INTRODUCTION TO MATHEMATICAL STRUCTURES AND PROOFS: SOLUTION MANUAL

by

LARRY J. GERSTEIN

Table of Contents

Solutions and Solution Sketches for Even-Numbered Exercises in

INTRODUCTION TO MATHEMATICAL STRUCTURES AND PROOFS

by

LARRY J. GERSTEIN

CHAPTER 1

§1.1

2.(a) Jones is lying if he somehow votes for both candidates (perhaps by first stealing a ballot) or doesn't vote at all. (In the words of the next section, here the "or" is *exclusive.*) Smith is lying only if he takes you to *neither* the movies nor dinner. (He is telling the truth if he takes you to one or both activities: his "or" is *inclusive.*)

(b) No. It suggests that there are two uses for "or" in ordinary speech.

4.(a) groan, grown, brown, blown, blows, blots, clots, cloth.

(b) We could show that "xylem" is false if we could show (by a search through the dictionary) that no other English word could be obtained by changing exactly one letter of "xylem."

§1.3

2. The conditional statement is true because its hypothesis ("today is Wednesday") is false.

4. If P and Q are both true (that is, it rains but we go on a picnic anyway) there is some ambiguity: it's not clear whether the given statement says that we *won't* go on a picnic if it rains.

6. Convenient abbreviations— W: Sunday's weather is nice; P: we will go on a picnic; F: we will go fishing; C: my car will need repair. A reasonable interpretation of the given statement can then be represented by $(W \wedge \sim C) \Longrightarrow (P \vee F)$. Then a truth table shows that your uncle lies only in the following situation: Sunday's weather is nice, the car does *not* need repair, and he takes you to neither a picnic nor a movie.

8. M: Claudia will run the marathon; T: Claudia has trained properly; I: Claudia is injury-free at race time.

(a) $(T \vee I) \Longrightarrow M$

(b) $M \Longrightarrow I$

(c) $M \Longleftrightarrow (T \wedge I)$

10. (b) Insert ((before the given expression.

(d) Insert) after the leftmost Q. (There are other possibilities too.)

Expressions (a), (c), and (e) are ok.

12. $0, 1, 10, 11, 100, 101, 110, 111, 1000, 1001, 1010, 1011, \ldots.., 10001$.

14. There are four variables, hence there are $2^4 = 16$ rows.

16. When P_1 is false there are 2^{n-1} possibilities for the truth values of the other variables, hence 2^{n-1} rows in the table. Similarly, there are 2^{n-2} rows in which P_1 is false while P_2 is true.

18. Expressions (a), (b), and (d) are tautologies. Expression (c) becomes a false proposition in the case when P is a false proposition and Q is a true proposition.

§1.4

2.(i) If some dogs bark then all cats meow.

(ii) If no dogs bark then some cat does not meow.

(iii) All cats meow and no dogs bark.

4. Suppose m and n are both even; say $m = 2r$ and $n = 2s$. Then $m + n = 2r + 2s = 2(r + s)$, which is even. If m and n are both odd, say $m = 2r + 1$ and $n = 2s + 1$, then $m + n = (2r + 1) + (2s + 1) = 2(r + s + 1)$, which is even. Finally, if m is even and n is odd, say $m = 2r$ and $n = 2s + 1$, then $m + n = 2r + 2s + 1 = 2(r + s) + 1$, which is odd.

6. A direct proof corresponds to moving in a direction that seems likely to lead to the top of the mountain, perhaps modifying the direction from time to time depending on the terrain, but continuing a forward motion until ending up on top. The analogy between mountain climbing and indirect proof technique is somewhat weaker. But, for the sake of discussion, it might correspond to assuming that the mountain is unclimbable, then finding a contradiction, perhaps by looking through binoculars and seeing happy hikers frolicking about on the top.

§1.5

2. S is a contradiction if $\sim S$ is a tautology.

4.(d) From §1.3 we know that $P \implies Q$ is an abbreviation for $\sim(P \wedge \sim Q)$. From this observation and parts (a), (b), (c) of the present exercise, we get that $P \implies Q$ can be represented by

$$((P \uparrow (Q \uparrow Q)) \uparrow (P \uparrow (Q \uparrow Q))) \uparrow ((P \uparrow (Q \uparrow Q)) \uparrow (P \uparrow (Q \uparrow Q)))$$

6. The expression $S_1 \iff S_2$ is a sentential form; accordingly, when the variables in S_1 and S_2 are replaced by propositions, the resulting composite proposition may be true or false. But $S_1 \equiv S_2$ is not a sentential form; instead, it is the assertion that whenever the variables in the two sentential forms S_1 and S_2 are replaced by propositions, the two resulting propositions will have the same truth value.

8. (a) Suppose S_1 logically implies S_2. Then whenever the variables in S_1 and S_2 are replaced by propositions, yielding respective propositions P_1 and P_2, the proposition $P_1 \implies P_2$ will be true; that is, P_1 will materially imply P_2.

(b) To say that two sentential forms are logically equivalent amounts to saying that each logically implies the other; that is, we say $S_1 \equiv S_2$ when both $S_1 \models S_2$ and $S_2 \models S_1$ are true.

§1.6

2. The given circuit can be represented by the sentential form

$$((\sim P \vee \sim Q) \wedge (\sim P)) \vee ((\sim P \vee \sim Q) \wedge R).$$

By using the distributive laws (1.34), this form can be shown to be logically equivalent to the form $\sim P \vee (\sim Q \wedge R)$. From this a simpler circuit follows.

CHAPTER 2

§2.1

2.(a) $A = \{ x \mid x \in \mathbb{Z}, x \geq 0, \text{ and } x \text{ even } \}$

(b) $B = \{ x \mid x = n^2 + 1 \text{ for some } n \in \mathbb{Z}\}$

(c) $C = \{ x \mid x = 4n + 1 \text{ for some } n \in \mathbb{Z}, \text{ with } n \geq 0\}$

(d) $D = \{ x \mid x = \frac{1}{n} \text{ for some } n \in \mathbb{N}\}$

(e) $E = \{ x \mid x = \text{lemon or } x \in \mathbb{N}\}$

4. (a) Not well-defined. "Large" is vague.

(b) This is well-defined. Either an integer is a multiple of 7 or it isn't. There is no ambiguity.

(c) This is a well-defined set, because π has a unique decimal expansion.

6. Not necessarily. For example, suppose $a = c = 1$ and $b = d = 2$.

8. (a) We have $A \notin A$ and $A \in \{A\}$. So the sets A and $\{A\}$ don't have the same members, hence are not equal.

(b) (We will argue by contradiction.) Each of the two sets in braces is a set with only one member, so the two sets would be equal if and only if the one member of the left set were equal to the one member of the right set. That is, if the given sets were equal, then we would also have equality after the outer pair of braces were peeled off the set on each side of the equation. After reasoning in this way n times, we would get the equality $A = \{A\}$, which we know to be false by part (a).

§2.3

2. (a) false; (b) true

4. (a) $(\exists p)(p \text{ prime and } p < 17)$

(b) $(\forall x \in \mathbb{R})(\exists p)(p \text{ prime and } p > x)$

(c) $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(y^5 = x)$

(d) $(\forall P, Q \in \Pi)(\exists! L)(L \text{ is a line and } P, Q \in L)$

6. $(p \in \mathbb{N}) \wedge p > 1 \wedge \big({\sim}(\exists a, b \in \mathbb{N})(a, b > 1 \wedge p = ab)\big)$

8. Let L and M denote the sets of liars and men, respectively. One interpretation (and probably the intended one) of the given statement is that at least one man is not a liar, represented symbolically by $(\exists x)(x \in M \wedge x \notin L)$. Another possible interpretation is that *no* men are liars, which can be represented by $\sim(\exists x)(x \in L \wedge x \in M)$. [Note: Once union and complements of sets have been introduced in §2.5, these statements will be representable by $M - L \neq \emptyset$ and $L \cap M = \emptyset$, respectively.]

§2.4

2. No, because a statement of the form $A \subset A$ would mean that some element x would satisfy both $x \in A$ and $x \notin A$, an absurdity.

4. (a) Argue by contradiction. If $B \subset A$, then some element x is in A but not in B, contradicting the hypothesis.

(b) Again argue by contradiction. If $A \neq \emptyset$ then A contains an element, which contradicts the hypothesis.

6. Because $A \subset B$ we know $A \subseteq B$ (from the definition of $\subset$), so $A \subseteq B$ by Theorem 2.15. The condition $A \subset B$ also says that there is an element x such that $x \in B$ but $x \notin A$. Then $x \in C$, because $B \subseteq C$, and so $A \neq C$. The conclusion follows.

8. "$\Longrightarrow$": Assume $A \subseteq B$, and suppose $X \subseteq A$. Then $X \subseteq B$ by Theorem 2.15. "$\Longleftarrow$" Assume every subset of A is a subset of B. But A is a subset of itself. Therefore $A \subseteq B$ by the hypothesis.

10. The objects on both sides of the equation under consideration are one-element sets. If they were equal, then we would have $\{\{5\}\} = \{5\}$, which in turn would yield $\{5\} = 5$, an impossibility because $5 \notin 5$. Therefore the given sets are *not* equal.

§2.5

2. $A' = \{\, x \mid x \leq 0 \text{ or } x \geq 6 \,\}$ $\quad C' = \{\, x \mid x \text{ is odd} \,\}$ $\quad (A \cap C)' = \{\, x \mid x \neq 2 \text{ and } x \neq 4 \,\}$

4. (i) $x \in A \cap B' \Longrightarrow x \in B' \Longrightarrow x \notin B \Longrightarrow x \notin A \cap B \Longrightarrow x \in (A \cap B)'$
The subsequent parts of Exercise 4 should be deleted. In particular, part (ii) is redundant in view of part (i), and part (iii) is wrong in view of part (i).

6. Let $A = \{1, 2, 3\}$, $\quad B = \{2, 4\}$, $\quad C = \{3, 4\}$. Then

$$A - (B - C) = A - \{2\} = \{1, 3\}, \quad \text{while} \quad (A - B) - C = \{1, 3\} - \{3, 4\} = \{1\}.$$

8. (c) and (e) are very much like (a), which is proved in the text. Here is a proof of (g):

$$x \in (A \cup B)' \iff x \notin A \cup B \iff {\sim}(x \in A \vee x \in B) \iff x \notin A \wedge x \notin B \iff x \in A' \cap B'$$

Note: In this argument in place of something of the form $x \notin S$, where S is a set, you may prefer $x \in U - S$, where U is taken as the underlying universal set. My preference is to assume that all elements under discussion are understood to lie in a fixed universal set, so that explicit mention of membership in the universal set can be omitted.

10. (a) Use the fact that $A - A = \emptyset$.

(b) Use the fact that $\emptyset - A = \emptyset$

(c) Outline: $((A - B) \cup (B - A)) - (A - B) = (B - A) - (A - B) = B - A$

(d) We're given that $(A - B) \cup (B - A) = \emptyset$, so $A - B = \emptyset$. Now if $x \in A$ then also $x \in B$ (otherwise we'd have $x \in A - B$, contradictiong the fact that $A - B = \emptyset$.) Therefore $A \subseteq B$. Inclusion "$\supseteq$" is similar.

(e) The Venn diagram suggests that both sides are equal to

$$(A \cup B \cup C) - ((A \cap B) \cup (A \cap C) \cup (B \cup C)).$$

Tediously verifying that will do the job.

§**2.6**

2. (a) The set of living people born on a Sunday, Monday, or Tuesday in January.

(b) $\emptyset$

(c) The set of living people born on a Friday in January through April.

(d) The set of living people born on a Friday or Saturday.

(e) The set of all living people.

(f) The set of living people born in May through December.

4. (b) (by contradiction) If we had $x \in B_1 \cap B_2 \cap B_3$, then $x \in B_1 \cap B_2$, contradicting the hypothesis that $B_1 \cap B_2 = \emptyset$.

6. (a) $\mathbb{N}$ (b) $\{0\}$ (c) the set of all integers except 1 and -1 (d) $\{0\}$ (e) $\{\, x \in \mathbb{Z} \mid x = 0 \text{ or } |x| \geq 6 \,\}$ (f) M_5

8. (a) $\{\, I_x \,\}_{x \in \mathbb{R}}$, where $I_x = [x, x+1]$.

(b) $\{ C_y \}_{y \in \mathbb{R}}$, where C_y is the circle of radius 1 centered at $(0, y)$.

(c) $\{ C_P \}_{P \in \Pi}$, where C_P is the circle of radius 1 centered at P.

(d)$\{ L_b \}_{b \in \mathbb{R}}$, where L_b is the line with slope 6 and y-intercept b.

(e) $\{ L_m \}_{m \in \mathbb{R}}$, where L_m is the line with slope m and y-intercept 5.

§2.7

2. (a) $\{\emptyset, \{2\}\}$

(b) $\{\emptyset, \{\emptyset\}, \{\{2\}\}, \{\{\emptyset, \{2\}\}\}\}$

(c) $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{2\}\}\}, \{\{\{\emptyset, \{2\}\}\}\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\{2,\}\}\}, \{\emptyset, \{\{\emptyset, \{2\}\}\}\},$
$\{\{\emptyset\}, \{\{2\}\}\}, \{\{\emptyset\}, \{\{\emptyset, \{2\}\}\}\}, \{\{\{2\}\}, \{\{\emptyset, \{2\}\}\}\}, \{\emptyset, \{\emptyset\}, \{\{2\}\}\},$
$\{\emptyset, \{\emptyset\}, \{\{\emptyset, \{2\}\}\}\}, \{\emptyset, \{\{2\}\}, \{\{\emptyset, \{2\}\}\}\}, \{\{\emptyset\}, \{\{2\}\}, \{\{\emptyset, \{2\}\}\}\}, P(P(\{2\}))\}$

4. Inclusion "$\supseteq$" follows from Theorem 2.36. Now suppose $x \in A - B$ and $y \in B - A$. Then $\{x, y\} \in P(A \cup B)$, but $\{x, y\} \notin P(A) \cup P(B)$. Inclusion "$\supset$" follows.

6. (a) $\emptyset$ is in every power set. In the notation of the present problem, we always have $\emptyset \in P(B)$.

(b) Again use the fact that $\emptyset$ is in every power set.

(c) Let $X \in P(A - B)$. [We must show that $X \in S = (P(A) - P(B)) \cup \{\emptyset\}$.] Then $X \subseteq A - B \subseteq A$, so $X \subseteq A$, giving $X \in P(A)$. If $X = \emptyset$ then $X \in S$ and we're done. Now suppose $X \neq \emptyset$, say $x \in X$. Then (since $X \subseteq A - B$) we have $x \notin B$. Therefore $X \not\subseteq B$; i.e., $X \notin P(B)$. Therefore $X \in (P(A) - P(B)) \subseteq S$, and again we're done.

8. An element $X \in P(A \cup \{x\})$ is a subset of $A \cup \{x\}$. Such an X is either a subset of A or has the form $S \cup \{x\}$ for some $S \subseteq A$.

§2.8

2. "$\subseteq$": Let $w \in \{1, 2\} \times S$. Then $w = (a, s)$, where $a \in \{1, 2\}$ and $s \in S$. Therefore $w = (1, s)$ for some $s \in S$ or $w = (2, s)$ for some $s \in S$, and so $w \in (\{1\} \times S) \cup (\{2\} \times S)$.
"$\supseteq$": Let $w \in (\{1\} \times S) \cup (\{2\} \times S)$. Then either $w \in \{1\} \times S$ or $w \in \{2\} \times S$. In the first case $w = (1, s)$ for some $s \in S$; in the second case $w = (2, s)$ for some $s \in S$. In both cases $w \in \{1, 2\} \times S$.

4. (a) This is the solid rectangle of height 2 whose base is the line segment from the point $(-2, 3)$ to the point $(1, 3)$.

(b) This is the set of all points whose coordinates are both integers.

(c) These are the points with integer x-coordinates.

(d) These are the points whose y-coordinates are positive integers.

(e) These are the points with x-coordinate in the interval $[1, 2]$.

(f) These are the points with positive integer x-coordinate and y-coordinate in the interval $[1, 2]$.

6. (a) If $(a_1, a_2, a_3) = (b_1, b_2, b_3)$, then $((a_1, a_2), a_3) = ((b_1, b_2), b_3)$. Therefore $(a_1, a_2) = (b_1, b_2)$ and $a_3 = b_3$. It follows that $a_i = b_i$ for $i = 1, 2, 3$.

(b) Define $(a_1, a_2, a_3, a_4) = ((a_1, a_2, a_3), a_4)$. The required proof is essentially the same as the argument in part (a).

8. We are given that $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. First suppose $a = b$. Then $\{\{a\}, \{a, b\}\} = \{\{a\}\} = \{\{c\}, \{c, d\}\}$. So $\{c, d\} = \{c\} = \{a\}$, and therefore $a = b = c = d$, which finishes the result in this case.

Now suppose $a \neq b$. Then $\{a\} \neq \{a, b\}$, and so $\{c\} \neq \{c, d\}$. We know that $\{c, d\} \neq \{a\}$, since $\{a\}$ has only one element. Therefore, from the hypothesis we have $\{c, d\} = \{a, b\}$ and also $\{a\} = \{c\}$. Hence $a = c$, so $\{c, d\} = \{a, d\} = \{a, b\}$. Therefore $b = d$.

§2.9

2. $\Pi_1 = \{\{1,2\}, \{3,4,5\}\}, \Pi_2 = \{\{1,3\}, \{2,4,5\}\}, \Pi_3 = \{\{1,4\}, \{2,3,5\}\}, \Pi_4 = \{\{1,5\}, \{2,3,4\}\}, \Pi_5 = \{\{4,5\}, \{1,2,3\}\}, \Pi_6 = \{\{3,5\}, \{1,2,4\}\}, \Pi_7 = \{\{3,4\}, \{1,2,5\}\}, \Pi_8 = \{\{2,5\}, \{1,3,4\}\}, \Pi_9 = \{\{2,4\}, \{1,3,5\}\}, \Pi_{10} = \{\{2,3\}, \{1,4,5\}\}$

4. If $x \in S$ then either $x \in A$ or $x \notin A$; accordingly, $x \in A \cup (S - A)$, and therefore $S = A \cup (S - A)$. Moreover, $A \cap (X - A) = \emptyset$, and the result follows.

6. (a) $R = \{(1, 2), (2, 3)\}$; (b) $R = \{(1, 1), (2, 2), (3, 3), (1, 2)\}$

8. $R \cup \{(2, 1), (3, 1), (3, 2)\}$

10. (a) No. Conceivably there are cities A and B such that there is a one-way road directly from A to B, but no direct road from B to A.

(b) In every case in which one can drive from a city A to a city B, either directly or by passing through other cities, to achieve transitive closure one would need to be sure that there is a direct road from A to B.

12. (a) Supplement $G(R)$ as needed so that in every case in which there is a directed edge between two vertices there is also a directed edge in the opposite direction between the same two vertices.

(b) Supplement $G(R)$ as needed so that there is a loop at each vertex (i. e., a directed edge from the arc to itself).

(c) Supplement $G(R)$ as needed so that in each case in which one can get from a vertex p to a vertex $q \neq p$ by following a sequence of directed edges in $G(R)$ there will be a directed edge from p to q in the new graph.

(d) Reverse the direction of the arrow on each directed edge in $G(R)$.

14. For each $x \in S$ the ordered pair (x, x) belongs to R (since R is reflexive), and switching the coordinates of such an ordered pair leaves it unchanged. Therefore R^{-1} is reflexive. Now suppose $(x, y) \in R^{-1}$. Then $(y, x) \in R$. Because R is symmetric, the ordered pair (x, y) is also in R, and therefore $(y, x) \in R^{-1}$. Therefore R^{-1} is symmetric. Finally, we must show that R^{-1} is transitive. So suppose $(x, y), (y, z) \in R^{-1}$. Then $(z, y), (y, x) \in R$; therefore, since R is transitive, we have $(z, x) \in R$, and hence $(x, z) \in R^{-1}$. Thus R^{-1} is transitive, as desired.

16. (a) Let $x, y \in A$, with $x \neq y$. Then $\{x\}, \{y\} \in P(A)$. Since $\{x\} \not\subseteq \{y\}$ and $\{y\} \not\subseteq \{x\}$, it follows that "$\subseteq$" is not a total ordering. The divisibility relation is not a total ordering because $2 \nmid 3$ and $3 \nmid 2$.

(b) Word w_1 precedes another word w_2 if in spelling out the words (from left to right, in our usual way), in the first instance in which the letters disagree the letter in w_1 precedes the corresponding letter in w_2 in the alphabet. If no disagreement occurs, it is because one word is a prefix of the other; in that case list the shorter word first.

18. For each $x, y \in S$ the conditional statement $(x, y) \in \emptyset \Longleftrightarrow (y, x) \in \emptyset$ is true, because component statements are false. Therefore $\emptyset$ is symmetric. The proof of transitivity is similar. Finally, if $x \in S$ (and there is such an x because $S \neq \emptyset$) then $(x, x) \notin \emptyset$, so $\emptyset$ is not reflexive.

20. (a) not transitive

(b) Each block in the partition consists of all the cars of a given color. (So there is a red block, a green block, and so on.)

(c) not symmetric

(d) Each block has the form $\{x, -x\}$ for some $x \in \mathbb{R}$.

(e) not transitive

(f) The blocks are the horizontal lines.

22. If the L_i are the blocks, two points in the plane are related if and only if they have the same x-coordinate. If the C_r are the blocks, two points in the plane are related

if and only if they are the same distance from the origin.

§2.10

2. The case $n = 1$ is clear. (That is, $P(1)$ is true.) Now suppose the result holds when $n = k$. (That is, $P(k)$ is true. We must show $P(k+1) : 1^3 + \cdots + (k+1)^3 = (\frac{(k+1)(k+2)}{2})^2$. We have

$$\begin{aligned}
1^3 + \cdots + (k+1)^3 &= (1^3 + \cdots + k^3) + (k+1)^3 \\
&= \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3, \text{ by the induction hypothesis} \\
&= \frac{k^4 + 2k^3 + k^2 + 4(k^3 + 3k^2 + 3k + 1)}{4} \\
&= \frac{k^4 + 6k^3 + 13k^2 + 12k + 4}{4} \\
&= \left(\frac{k^2 + 3k + 2}{2}\right)^2 = \left(\frac{(k+1)(k+2)}{2}\right)^2
\end{aligned}$$

This finishes the proof.

[Note: While this proof is correct, someone in the act of proving the result probably proceeds through the next to last line as above, but then takes the expression $(\frac{(k+1)(k+2)}{2})^2$, which is, after all, the desired final object one is seeking, and expands it to see that it is actually equal to what has already been obtained.]

4. The case $n = 0$ is trivial. Now take the equation $k^4 - 4k^2 = 3t$ as the induction hypothesis. Then

$$\begin{aligned}
(k+1)^4 - 4(k+1)^2 &= k^4 + 4k^3 + 6k^2 + 4k + 1 - 4k^2 - 8k - 4 \\
&= (k^4 - 4k^2) + 4k^3 + 6k^2 - 4k - 3 \\
&= 3t - 3 + 2k(2k-1)(k+2)
\end{aligned}$$

Now k has one of the forms $3s, 3s+1$, or $3s+2$ for some integer s, and in each of these cases it can be checked that $k(2k-1)(k+2)$ is a multiple of 3. The result follows.

6. The case $n = 2$ is easily checked. Now take as the induction hypothesis the statement $P(k) : \frac{1}{1\cdot 2} + \cdots + \frac{1}{(k-1)k} = 1 - \frac{1}{k}$. Then

$$\begin{aligned}
\frac{1}{1\cdot 2} + \cdots + \frac{1}{((k+1)-1))(k+1)} &= \frac{1}{1\cdot 2} + \cdots + \frac{1}{(k-1)k} + \frac{1}{k(k+1)} \\
&= (1 - \frac{1}{k}) + \frac{1}{k(k+1)} \text{ by the induction hypothesis} \\
&= 1 - \frac{k+1}{k(k+1)} + \frac{1}{k(k+1)} = 1 - \frac{k}{k(k+1)} = 1 - \frac{1}{k+1}
\end{aligned}$$

which completes the induction argument.

8. The induction step of the proof is not complete, because truth of $P(1)$ does not lead to truth of $P(2)$. (That is, the argument given in the book does not show that in any set of *two* horses both horses must have the same color.

10. Define $E(n)$ for each $n \geq 1$ as follows: Set $E(1) = a_1$, and then for $k \geq 1$ define $E(k+1) = a_{k+1}^{E(k)}$.

12. $\sum_1^5 a_i = 3^{-1} + 3^0 + 3^1 + 3^2 + 3^3 = 40\frac{1}{3}$, $\prod_1^5 a_i = 3^5 = 243$.

14. The product $100! = 1 \cdot 2 \cdots 5 \cdots 10 \cdots 100$ has twenty factors that are multiples of 5; of those, $25, 50, 75$, and 100 are multiples of 5^2. Altogether that gives twenty-four 5s. They pair up with 2s in the product to give twenty-four factors of 10. Therefore 100! has twenty-four 0s on its right end.

CHAPTER 3

§3.1

2. (a) $A = \{1, 3, 8, 9, \pi\}$, $B = \mathbb{R}$ (Or B can be taken to be any set containing the set $\{1, 2, 5, -4\}$.)

(b) $f(8) = 5$, $f^{-1}(2) = 3$.

4. (a) $\operatorname{dom} f = \mathbb{R}$, $\operatorname{dom} g = \mathbb{R} - \{5\}$; therefore $f \neq g$.

(b) $\operatorname{dom} f = \{\, x \in \mathbb{R} \mid x \geq 0 \,\}$, $\operatorname{dom} g = \mathbb{R}$; therefore $f \neq g$.

(c) $f = g$ and $\operatorname{dom} f = \mathbb{R}$.

(d) Both functions have domain $\mathbb{R}$. But $f \neq g$, because $f(\pi) = \pi^2$, $g(\pi) = 0$.

6. (b) The equivalence class of x is the set of all cars whose color is the same as x's.

(c) The equivalence class of x is $\{x, -x\}$.

(d) Same answer as (c).

(e) The equivalence class of (x, y) is $\{(x, y), (y, x)\}$.

(f) Suppose $x + y = c$. Then the equivalence class of (x, y) is the line whose equation is $x + y = c$; that is, the line with slope -1 and y-intercept c.

(g) The equivalence class of the point $P = (x, y)$ is the circle of radius $\sqrt{x^2 + y^2}$ centered at the origin.

8. (a) This is the set of all states that the machine can reach from the state q_0 by receiving just one symbol from Σ.

(b) This is the set of all states that the machine can enter upon receiving the input symbol σ_0.

(c) $\delta(\delta(q_0, \sigma_1), \sigma_2)$

(d) $\delta(\cdots \delta(\delta(q_0, \sigma_1), \sigma_2) \cdots), \sigma_n)$

10. (a)

$$f(x) = \begin{cases} [x] & \text{if } x < [x] + \frac{1}{2} \\ [x] + 1 & \text{if } [x] + \frac{1}{2} \leq x \end{cases}$$

(b)

$$f(x) = \begin{cases} x & \text{if } x \in \mathbb{Z} \\ [x] + 1 & \text{if } x \notin \mathbb{Z} \end{cases}$$

§3.2

2. Note that the solutions to (a)–(c) given here are just one set of possibilities out of many.

(a) For $n \in N$, define $f(n) = n$'s youngest living aunt.

(b) No. If n and n' are brothers then $f(n) = f(n')$.

(c) No. An aunt with a younger sister will not be in the image.

(d) If there are at least as many elements in A as in N we can do it. For example, order the members of these sets by weight (using as many decimal places as needed in order to distinguish one person's weight from another's). Take the lightest $n \in N$ to the lightest $a \in A$, and so on.

(e) We need at least as many elements in N as in A. Proceed as in (d); once every member of A is in the function's image, the remaining elements of N can be paired with any elements of A; for instance, they can all be paired with the lightest element of A.

4. (a) $2^3 = 8$ (b) 0 (c) 6 (d) $8 - 2 = 6$ [Here we have subtracted the number of nonsurjections from the number of functions.] (e) 0 (f) For (a), n^m; for (b), there are $n(n-1)\cdots(n-(m-1))$ injections, provided that $m \leq n$, otherwise 0.

6. (a) $A = \{1,2\}, C = \{1\}, B = \{5\}, f(1) = f(2) = 5$.

(b) $A = \{1,2\}, C = \{1\}, B = \{1,2\}, f(1) = 1, f(2) = 2$.

(c) $A = \{1,2\} = B, C = \{1\}, f(1) = 1, f(2) = 2$.

(d) impossible

8. (a) Take $5, 3, 1, 4, 2$ as the representatives of the respective sets.

(b) No representative set is possible. Setting aside the second and third listed sets, the four distinct representatives of the remaining sets (in the notation of the discussion preceding Example 3.13, these are M_1, M_4, M_5, M_6) would have to come from the set $\{1, 4, 6\}$, an impossibility.

10. Let $P = (1,1), Q = (2,2)$. Then $f(P) = f(Q)$, since both points are on the same line through the origin. Let S denote the set of all points on the upper half of the unit circle, omitting only the point $(-1, 0)$. That is, take $S = \{\,(x,y) \mid x^2 + y^2 = 1, y \geq 0, x > 1\,\}$.

12. We are given that the result holds when $n = 1$ and $n = 2$. Now suppose it holds when $n = k$. We have $(a_1, \cdots, a_{k+1}) = (b_1, \cdots, b_{k+1}) \iff ((a_1, \cdots, a_k), a_{k+1}) = ((b_1, \cdots, b_k), b_{k+1})$. But, from the case $n = 2$ (ordered pairs) this gives $a_{k+1} = b_{k+1}$ and $(a_1, \cdots, a_k) = (b_1, \cdots, b_k)$, from which the result follows by the induction hypothesis.

14.

$$\frac{1+\frac{5}{1}}{2}=3,\ \frac{3+\frac{5}{3}}{2}=2.35,\ \frac{2.35+\frac{5}{2.35}}{2}=2.24,\ \frac{2.24+\frac{5}{2.24}}{2}=2.236,\ \frac{2.236+\frac{5}{2.236}}{2}\approx 2.23607$$

Finally, $\frac{2.23607+\frac{5}{2.23607}}{2} \approx 2.23607$. Therefore, $\sqrt{5} \approx 2.23607$.

16. (a) $a_1 = 1, \quad a_{k+1} = a_k + 2$.

(b) $a_1 = a_2 = 1$, and

$$a_{k+1} = \begin{cases} a_k + 2 & \text{if } a_k = a_{k-1} \\ a_k & \text{otherwise} \end{cases}$$

(c) $a_1 = 1, \quad a_{k+1} = a_k + k$

(d) $a_1 = a_2 = 1, \quad a_{k+1} = a_{k-1} + a_k$

18. The mapping is given by $n \longmapsto 10^{n-1} + 1$.

20. Define $a_1 = (1, -1)$, and if $a_k = (a, b)$ define

$$a_{k+1} = \begin{cases} (a-1, b-1) \text{ if } a > 1 \\ (1+|b|, -1) \text{ if } a = 1 \end{cases}$$

§3.3

2. (a) Let $g(x) = x^2 + \cos x, h(x) = x^3$. Then $f = h \circ g$.

(b) Let $g(x) = x^5 - 7x, h(x) = x + 1$. Then $f = h \circ g$.

(c) Let $g(x) = x(10)^x, h(x) = x^2$. Then $f = h \circ g$.

(d) Let $g(x) = \frac{1}{x\sqrt{x-1}}, h(x) = 5x$. Then $f = h \circ g$.

4. For all $x \in S$, we have $f(x) = a$ and $g(x) = b$, with $a, b \in S$ and $a \neq b$. Then $(f \circ g)(x) = f(g(x)) = f(b) = a$for all $x \in S$, while $(g \circ f)(x) = g(f(x)) = g(a) = b$.

6. Both of the given composite functions have the action

$$x \longmapsto \sin\left(\left(\frac{\sqrt{3x}-5}{\sqrt[4]{3x}+1}\right)^3\right)$$

8. (a) Let $A = C = \{1, 2\}, B = \{1, 2, 3\}$, and define f and g by $f(1) = g(1) = 1, f(2) = g(2) = 2, g(3) = 2$.

(b) The solution given here for part (a) works.

10. (a) Left cancellation does not generally hold when f is not injective. For example, if $g, h \colon A \to B$ are different functions, C is a set with one element, and $f \colon B \to C$ the only possible function (so f is surjective), then left cancellation fails. On the other hand, we claim that right cancellation holds whenever f is surjective, and this is proved as follows. We're given a surjective function $f \colon A \to B$ and functions $r, s \colon B \to C$, with $r \circ f = s \circ f$. Let $b \in B$. [We must show that $r(b) = s(b)$.] Since f is surjective, we can write $b = f(a)$ for some $a \in A$. Then $(r \circ f)(a) = (s \circ f)(a)$ (because $r \circ f = s \circ f$ by hypothesis). Therefore $r(f(a)) = s(f(a))$; that is, $r(b) = s(b)$, proving the claim.

(b) Now suppose f is injective, but not surjective. We claim that left cancellation works. We are given functions $g, h \colon A \to B, f \colon B \to C$, with $f \circ g = f \circ h$ and f injective. Then for each $a \in A$ we have $f(g(a)) = f(h(a))$, and hence $g(a) = h(a)$ (by injectivity of f.) Therefore $g = h$, proving the claim. On the other hand, now suppose we have $f \colon A \to B$, and $r, s \colon B \to C$. If r and s agree on $f(A)$ but disagree on some element of $B - f(A)$, this provides an example of failure of right cancellation. [Note: Since we are assuming that f is not surjective, we know that $B - f(A) \neq \emptyset$.]

12. dom $f = \{\, x \in \mathbb{R} \mid x \geq 0 \,\}$, range $f = \{\, x \in \mathbb{R} \mid x \geq 3 \,\}$, $f^{-1}(x) = (x-3)^4$.

14. (a) Let $x \in A \cup C$. If $x \in A$ then $\exists! y \in B$ with $(x, y) \in f$; if If $x \in C$ then $\exists! y \in D$ with $(x, y) \in g$. Because $A \cap C = \emptyset$, exactly one of the two cases applies to x. Therefore $\exists! y \in B \cup D$ with $(x, y) \in f \cup g$.

(b) Let $A = B = C = \{1\}$, $D = \{2\}$, $f = \{(1,1)\}$, $g = \{(1,2)\}$.

(c) Let $A = \{1,2\}$, $C = \{2,3\}$, $B = D = \{1,2\}$, $f = \{(1,1),(2,2)\}$, $g = \{(2,2),(3,1)\}$.

(d) Let $y \in B \cup D$. If $y \in B$, choose $x \in A$ with $f(x) = y$. Similarly, if $y \in D$, choose $x \in C$ with $g(x) = y$. [Note: If $y \in B \cap D$ then the same element x is chosen in both cases because $f \cup g$ is given to be a function.] Then $(f \cup g)(x) = y$.

(e) $f(x_1) = f(x_2) \iff (f \cup g)(x_1) = (f \cup g)(x_2) \iff x_1 = x_2$ (since $f \cup g$ is injective.

(f) Let $y \in B \cup D$. We must check that $(f \cup g)^{-1}(y) = (f^{-1} \cup g^{-1})(y)$. Suppose $y \in B$. Then, since $(f \cup g)$ is a bijection, $\exists! x \in A \cup B$ such that $(f \cup g)(x) = y$. Say $x \in A$. So $y = (f \cup g)(x) = f(x)$. Therefore $x = f^{-1}(y) = (f \cup g)^{-1}(y)$. Similarly, if $y \in D$ then $g^{-1}(y) = (f \cup g)^{-1}(y)$. The result follows.

(g) Let $A = B = \{1,2\}$, $C = D = \{3,4\}$, and f, g the associated identity functions.

(h) Let $A = B = D = \{1,2\}$, $C = \{3,4\}$, $f(1) = g(3) = 1$, $f(2) = g(4) = 2$.

CHAPTER 4

§4.1

2. If L has equation $y = mx + b$, with $m \neq 0$, then the mapping $\mathbb{R} \mapsto L$ given by $x \mapsto mx + b$ is easily shown to be a bijection. If L has equation $y = b$, then the mapping $\mathbb{R} \mapsto L$ given by $x \mapsto (x, b)$ does the job. Finally, if L, M are lines then by Theorem 4.2 we have $L \approx \mathbb{R} \approx M$ and hence $L \approx M$.

4. (a) The mapping $A \times B \mapsto B \times A$ given by $(a, b) \mapsto (b, a)$ is easily shown to be a bijection.

(b) There are bijections $f\colon A \to C$ and $g\colon B \to D$; then the mapping $A \times B \mapsto C \times D$ given by $(a, b) \mapsto (f(a), g(b))$ does the job.

(c) Consider the mapping $(A \times B) \times C \mapsto A \times (B \times C)$ given by $((a, b), c)) \mapsto (a, (b, c))$.

(d) Use the mapping $(w, a) \mapsto a$.

6. Define $f\colon [-2, 8] \to [3, 5]$ by $f(x) = \frac{x+17}{5}$.

8. Let M be the collection of m-element subsets of A, and let C be the collection of $n - m$-element subsets of A. Define $f\colon M \to C$ by $f(X) = X'$, where X' denotes the complement of X in A. The fact that $X' \in C$ follows from Theorem 4.14. The function f is surjective, since if $Y \in C$ then $Y' \in M$ and $f(Y') = (Y')' = Y$. Injectivity follows from the fact that if $X' = X_1'$ then $(X')' = (X_1')'$, and therefore $X = X_1$.

10. Among the people in the study, let L be the set of lunch eaters, F the set of flossers, and P the set of subscribers to the paper. We are given that $\sharp(L \cap F) = 52, \sharp(L \cap P) = 15$, and $\sharp(L \cap F \cap P) = 10$. By making a Venn diagram and labeling the appropriate sections with this data, we get the following results: (a) 14 (b) 12 (c) 10

12. (a) There are bijections $f\colon A \to A_1$ and $g\colon B \to B_1$, hence a bijection $A \cup B \to A_1 \cup B_1$ given by

$$x \mapsto \begin{cases} f(x) & \text{if } x \in A \\ g(x) & \text{if } x \in B \end{cases}$$

(b) Use the fact that $A \cup (B \cup C) = (A \cup B) \cup C$.

14. (a) Use Exercise 4(a) in this section.

(b) This is a consequence of Theorem 2.45(a).

16. (a) Either list them directly (count from 0 to 7 in binary) or argue that there

are two possibilities for each digit and three such decisions to be made, hence $2^3 = 8$ possibilities in all, by the product rule.

(b) Follow the given hint.

18. (a) There are $7 \times 5 = 35$ mens shirts and $8 \times 4 = 32$ womens shirts, for a grand total of 67.

(b) By using both the product rule (4.22) and addition rule (Theorem 4.14), we deduce that there are $35 + 35 \cdot 26^2 + 35 \cdot 26^3$ possibilities in all.

(c) $32 + 8 = 40$

20. (a) $100^2 = 10,000$

(b) First decide which tank is to provide the first selection (and hence, automatically, which is to provide the second selection). Then make the selections. By the product rule there are $2 \times 100^2 = 20,000$ possibilities.

22. (a) Let $A_1, \cdots, A_n$ denote the equivalence classes, and suppose (to the contrary of the desired conclusion) that $\sharp A_i = m_i \in \mathbb{N}$, for $1 \leq i \leq n$. By Corollary 4.15 we would then have $\sharp S = \sharp(\cup_{i=1}^{n} A_i) = m_1 + \cdots m_n \in \mathbb{N}$, contrary to the hypothesis that S is infinite.

(b) No. For example, define $x \sim y$ to mean that $x = y$. Then the equivalence classes are the one-element sets $\{x\}$ for $x \in S$. But there are infinitely many of these. [In fact the collection of such sets can be put into one-to-one correspondence with S via $\{x\} \longleftrightarrow x$.]

§4.2

2. Let $A = [0,1], B = [0,2], f\colon A \to B$ the identity map, $g\colon B \to A$ given by $x \mapsto \frac{x}{4}$. Then f and g are injections, but neither is a bijection.

4. (a) First we check injectivity. We have $h(x) = h(0) = \frac{1}{2} \iff x = 0$. If x does not have form $\frac{1}{n}$ for some integer n then neither does $h(x) = x$. Finally, if $h(\frac{1}{n}) = h(x)$, then from what has already been said x has form $\frac{1}{m}$ for some m; but then $\frac{1}{n+2} = h(\frac{1}{n}) = h(\frac{1}{m}) = \frac{1}{m+2}$, hence $n = m$, and therefore $x = \frac{1}{n}$. Thus h is injective. Surjectivity follows from the fact that an element $x \in (0,1)$ either has form $\frac{1}{m}$ for some $m \in \mathbb{N} - \{1\}$ or does not. Every such $\frac{1}{m}$ is in $\mathrm{im} h$, as indicated in the definition, and $h(x) = x$ in all other cases. Therefore h is surjective.

(b) Each element of the form $\frac{1}{n}$ in $(0,1)$ moves to the next such element, freeing the location of $\frac{1}{2}$ for zero. Also see the quote from "Alice's Adventures in Wonderland" at the start of the chapter.

6. Because $\sharp A \leq \sharp B$, there is an injection $f\colon A \to B$ (from Definition 4.27). Now

define $F: P(A) \to P(B)$ by

$$F(X) = \{ f(x) \mid x \in X \}$$

for each $X \in P(A)$. Then $F(X) \subseteq B$; that is, $F(X) \in P(B)$. To see that F is injective, let $X, Y \in P(A)$ with $X \neq Y$; so one of X, Y contains an element not in the other. Say $a \in X - Y$. Then $f(a) \in F(X)$, while $f(a) \notin F(Y)$ (because $a \notin Y$ and f is injective). Therefore $F(X) \neq F(Y)$, which proves that F is injective.

8. (a) Suppose $\sharp A = n$. So there is a bijection $f: \mathbb{N}_n \to A$. We know from Chapter 2 that $\sharp P(A) = 2^n$, so there is a bijection $g: P(A) \to \mathbb{N}_{2^n}$. By Cantor's theorem there is an injection (but no bijection) $h: A \to P(A)$, giving this diagram:

$$\mathbb{N}_n \xrightarrow{f} A \xrightarrow{h} P(A) \xrightarrow{g} \mathbb{N}_{2^n}$$

hence an injection $\mathbb{N}_n \to \mathbb{N}_{2^n}$. If there were also a bijection $j: \mathbb{N}_n \to \mathbb{N}_{2^n}$, then $f \circ j^{-1} \circ g$ would be an injection from $P(A)$ to A, so the Schroder-Bernstein theorem would give $A \approx P(A)$, contradicting Cantor's theorem. Therefore $\sharp\mathbb{N}_n < \sharp\mathbb{N}_{2^n}$, and hence $n < 2^n$.

(b) The result is clear for $n = 0, 1$. Now suppose the result is true for $n = k$; that is, $k < 2^k$. Then $k + 1 < 2^k + 1 < 2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$, which completes the induction.

§4.3

2. For each $n \in \mathbb{N}$, the person in room n should move to room $2n$. This clears out the odd-numbered rooms and makes space for the new guests. More specifically, if the new guests are $g_1, g_2, \cdots$, then g_i should go into room $2i - 1$.

4. True, since every subset of a countable set is countable. (Theorem 4.36)

6. We are given that A_1 is countable; and $A_1 \cup A_2$ is countable by Theorem 4.37. Now suppose the result holds when $n = k$; that is, $\cup_{i=1}^{k} A_i$ is countable. Then $\cup_{i=1}^{k+1} A_i = (\cup_{i=1}^{k} A_i) \cup A_{k+1}$ is countable by the induction hypothesis and the case $n = 2$.

8. Let $A_1, A_2, \cdots$ be a countably infinite collection of countable sets. Define $B_1 = A_1$, and for $n \geq 0$ put $B_n = A_n - \cup_{i<n} A_i$. Then the B_n are countable sets (being subsets of countable sets) and $\cup_{n \in \mathbb{N}} B_n = \cup_{n \in \mathbb{N}} A_n$. Notice that the sets $B_1, B_2, \cdots$ are pairwise disjoint. Summary so far: without loss of generality, we can assume that the original sets $A_1, A_2, \cdots$ are pairwise disjoint. It was shown in the text (Theorem 4.39) that $\mathbb{N} \times \mathbb{N}$ is countable. But

$$\mathbb{N} \times \mathbb{N} = (\{1\} \times \mathbb{N}) \cup (\{2\} \times \mathbb{N}) \cup (\{3\} \times \mathbb{N}) \cup \cdots$$

a union of countably many countably infinite sets. For each $i \in \mathbb{N}$, there is a bijection between A_i and a subset of $\{i\} \times \mathbb{N}$. This leads to a bijection between $\cup A_i$ and a subset of the countable set $\mathbb{N} \times \mathbb{N}$. Therefore $\cup A_i$ is countable, since a subset of a countable set is countable.

10. Consider an interval of length $L > 0$. Choose $n \in \mathbb{N}$ large enough so that $\frac{1}{n} < L$. Then at least one of the points $0, \pm\frac{1}{n}, \pm\frac{2}{n}, \pm\frac{3}{n}, \ldots$ is in the interval. Our conclusion: each of the given intervals contains a rational number. Moreover, different intervals contain different rationals, because the intervals are given to be pairwise disjoint. Thus the given family of intervals is in one-to-one correspondence with a subset of the rational numbers, and the family is therefore countable (by Theorems 4.40 and 4.36).

12. (a) The "total" of the interval lengths is $\sum_{n=1}^{\infty} \frac{1}{2^n} = 1$. That is the "geometric size" of $\mathbb{Q}$ is at most 1.

(b) This time the interval lengths "add" to $\sum_{n=1}^{\infty} \frac{\epsilon}{2^n} = \epsilon(\sum_{n=1}^{\infty} \frac{1}{2^n}) = \epsilon$. So the total lengths of these intervals containing $\mathbb{Q}$ is ϵ. Since ϵ can be taken as small as we like, we conclude that the total length of $\mathbb{Q}$ is less than any particular positive number. That is, in a sense $\mathbb{Q}$ has zero size. (In the terminology of advanced analysis courses, $\mathbb{Q}$ is a set "of measure zero.")

(c) Because one is not adding in the usual sense, but rather taking the limit of a certain sequence of sums (called the associated "partial sums.")

14. Every such circle passes through a point $(x, 0)$ on the positive x-axis, and different circles pass through different points. Therefore there is a one-to-one correspondence between the given set of circles and the set of positive real numbers; so this set of circles is uncountably infinite. On the other hand, the set $\mathbb{Q} \times \mathbb{Q}$ is countable (by Theorems 4.40 and 4.39(b)), so there cannot be a point from $\mathbb{Q} \times \mathbb{Q}$ on each of the circles.

§4.4 THERE ARE NO EXERCISES IN THIS SECTION.

§4.5

2. The list starts with the empty word, then the 26 words of length 1, then the 26^2 words of length 2. Then come the 3×26^2 three-letter words starting with a, b, or c. Among the three-letter words starting with d, there are 14×26 words starting with da through dn. Finally, dog is the 7th three-letter word starting with do. So dog's position on the list is number $1 + 26 + 26^2 + (3 \times 26^2) + (14 \times 26) + 7 = 3102$.

4. The accepted language $L(M)$ is $\emptyset$, the empty language. There is no way to get from the initial state to the final state by following a sequence of arcs. In general, if the the state graph is not connected, and the component of the state graph containing the initial state does not contain a final state, then without looking further at the graph (and struggling to construct a path from the initial state to a final state) we know that no words can be accepted, and so the associated language is $\emptyset$.

6. We have defined $\delta(q, \epsilon) = q \quad \forall q \in S$. Therefore the empty string ϵ is accepted if and only if $q_0 \in F$.

CHAPTER 5

§5.1

THERE ARE NO EXERCISES IN THIS SECTION.

§5.2

2. A four-digit number must have its left-digit (the thousands digit) nonzero.

(a) $9 \times 10^3 = 9000$

(b) $4 \times 5^3 = 500$

(c) $9 \times 9 \times 8 \times 7 = 4536$

(d) $9^4 = 6561$

(e) We will count digits from the right. (That is, view the units digit as the first digit, the tens digit as the second digit, and so on.) There are several cases to count separately.

(i) There are 9^2 numbers in which the 1st and 3rd digits are both 0.

(ii) There are $8 \times 9 \times 8$ numbers in which the 1st digit is 0 and the 3rd digit is not 0.

(iii) There are $8 \times 9 \times 4$ numbers in which the 1st and 3rd digits are equal and not 0.

(iv) There are $9 \times 8 \times 4$ numbers in which the 1st digit is not 0 and the 3rd digit is 0.

(v) There are $8 \times 8 \times 8 \times 4$ numbers in which the 1st and 3rd digits are not equal and not 0.

The total of all these is 3281.

4. There are $2^3 = 8$ subsets of the jams (that is, 8 jam combinations), including the possibility of no jam. Let's refer to the potentially lethal cheese as the bad cheese, the others as good. First we count the possibilities that don't use the bad cheese: there are 5 cracker possibilities, 6 cheese possibilities (either a good cheese or no cheese), and 8 jam possibilities; by the product rule this gives $5 \times 6 \times 8 = 240$ snacks. Next consider the nonlethal possibilities that use the bad cheese: there are 5 cracker possibilities and 4 jam possibilities (no jam or one of the three jams), which yields $5 \times 4 = 20$. The grand total: 260.

§5.3

2. The mapping on the left is not one-to-one; the other has domain the set $\{1, 2, 3, 4, 5\}$, whereas 6 is in its range.

4. (a)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}$$

(b)

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

6. This follows from Theorem 3.24, the associative law for function composition. (Multiplication of permutations is composition of functions that happen to be permutations, i.e., bijections of a set to itself.)

8. (a)

$$\sigma^0 = e \quad \text{(the identity permutation)} \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}, \quad \sigma^1 = \sigma, \quad \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix},$$

$$\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix}, \quad \sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}, \quad \sigma^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 5 & 1 & 3 & 2 \end{pmatrix}, \quad \sigma^6 = e$$

Every permutation of the form σ^n for some $n \geq 7$ can be expressed as $(\sigma^6)^t\sigma^k = \sigma^k$ for some $k \leq 5$. Thus the permutations listed above are all the permutations that are powers of σ.

(b) We have $268 = 6 \cdot 44 + 4$, therefore $\sigma^{268} = (\sigma^6)^{44} \cdot \sigma^4 = \sigma^4$

10. The diagram, when read from left to right in our customary reading style, indicates the order in which things happen. That is, we follow the action of the indicated function composition by picking an element $a \in A$, applying f, then applying g, and so on, eventually getting $h(g(f(x)))$. In the expression $h(g(f(x)))$ the functions are listed in the *opposite* order from that in the diagram, so that we have to "back up from right to left starting at x to get the correct order of events. If functions were written on the right, then we would instead get the expression $(((x)f)g)h$, in which the functions appear from left to right in the order in which they are applied.

12. $4! \times 6! = 17280$. This is because such a permutation can be thought of as a product $\alpha\beta$, where α is a permutation of $\{1, 2, 3, 4\}$ and β is a permutation of $\{5, 6, 7, 8, 9, 10\}$. There are $4!$ possibilities for α and $6!$ possibilities for β.

14. There are seven letters to be arranged from left to right in seven positions. First choose the three positions that will get as. There are 35 ways to do this. Then there are $4!$ ways to distribute the remaining four letters in the remaining four positions. By the product rule there are therefore $35 \times 4! = 840$ possible words.

16. View the women as w_1, w_2, w_3, w_4, the men as m_1, m_2, m_3, m_4. In this problem it is only *relative* position that matters. That is, we usually imagine that one person, say

w_1, goes out and stands on the floor, and then we count the number of possibilities for the other peoples locations in view of the requirements of the problem.

(a) Answer: 6. After w_1 is in position, imagine that the woman who will be the first woman to w_1s right goes to the floor, then the woman to her right, and so on. There are $3! = 6$ possiblities for this positioning of the women. Once the women are in place, the positions of the men are automatic under the conditions of the problem.

(b) Answer: 144. After w_1 is in position, there are 4 possibilities for the man on her right, then three possibilities for the woman on his right, and so on.

(c) Answer: $7! = 5040$. After w_1 is in position, there are 7 possibilities for the person on her right, then 6 possibilities for the person on his or her right, and so on.

(d) Answer: $7! - 2 \cdot 6! = 4000$. Let's first count the number of UNacceptable configurations. First imagine the two hate-filled men standing as a unit in one position. By the reasoning of part (c) there are 6! ways to then position the other people in the circle. Having done this,we still have to decide which of the two men is to the left of the other, and there are two possibilities for that choice. Thus in all there are $2 \cdot 6!$ unacceptable configurations. But from part (c) there are 7! total (acceptable and unacceptable) ways to arrange the people. The result follows.

§5.4

2. A symmetry of the circle is either a rotation about the center of the circle or a reflection through a diameter of the circle (more precisely, through a line on which a diameter lies). One can see this informally by considering distinct points A, B close to each other on the circle; what happens to these points will determine the symmetry. Suppose these points have images A', B', respectively. A rotation will achieve this if the image points have the same orientation with respect to each other as the originals; otherwise a suitable reflection will do the job. The symmetry set is uncountable. For example, there is a rotation of each angle of α radians with $0 \leq \alpha < 2\pi$.

4. Write $d(P,Q)$ for the distance between P and Q. To say that s is a symmetry means that $d(s(P), s(Q)) = d(P,Q)$.

(a)

$$\begin{aligned} d((s_2 \circ s_1)(P), (s_2 \circ s_1)(Q)) = d(s_2(s_1(P)), s_2(s_1(Q))) &= d(s_1(P)), s_1(Q)) \quad \text{because } s_2 \text{ is a symmet} \\ &= d(P,Q) \quad \text{because } s_1 \text{ is a symmetry} \end{aligned}$$

(b) First note that s^{-1} exists because s is a bijection. For points P, Q in the plane we must show that $d(s^{-1}(P), s^{-1}(Q)) = d(P,Q)$. Because s is surjective we can write

$P = s(A), Q = s(B)$ for some A, B in the plane. Then

$$\begin{aligned} d(s^{-1}(P), s^{-1}(Q)) &= d(s^{-1}(s(A)), s^{-1}(s(B))) \\ &= d(A, B) \\ &= d(s(A), s(B)) \quad \text{because } s \text{ is a symmetry} \\ &= d(P, Q) \end{aligned}$$

6. (a) Let P be one of the vertices. Under the action of a symmetry σ, the vertex P must go to a vertex; so there are 4 possibilities for $\sigma(P)$. Then the vertices of the triangular base opposite P must go to the vertices of the base opposite $\sigma(P)$. By Example 5.14, there are 6 possible ways that can happen. So altogether there are 24 symmetries, by the product rule.

(b) The vertex at the top must remain fixed. The square at the bottom must go to itself, and, by the discussion preceding Example 5.17, there are 8 possibilities for that. Thus there are 8 symmetries of the pyramid.

(c) The two vertices not on the square must either remain fixed or switch with each other. Then there are 8 symmetries of the square. This gives $2 \times 8 = 16$ symmetries of the octahedron.

(d) Let P be one of the vertices. Under the action of a symmetry P must go to one of the 8 vertices of the cube. The 4 vertices that are directly connected to P by an edge are the vertices of a square that must be taken to itself; there are 8 possibilites for that. (The remaining vertex not yet discussed, namely, the one diagonally opposite P in the cube, must go to the vertex diagonally opposite the image of P.) This gives a total of $8 \times 8 = 64$ symmetries of the cube.

(e) We are given that the solid is not a cube. There are several cases, of which we discuss just one here. Suppose one dimension is strictly larger than the other two. View that larger dimension as the length of the solid. Then either each end of the solid goes to itself under the action of a symmetry, or else the ends interchange. Once that has been decided, one needs to count the symmetries of an end. The result will vary depending on whether the end is square or not. (A square has 8 symmetries, a nonsquare rectangle has 4 symmetries.)

(f) There are uncountably many symmetries. A point P can be rotated to any point Q on the sphere. Then, viewing P as a pole (as on the Earth), the equator must go to the equator regarding Q as a pole. Refer to the solution to Exercise 2 for discussion of the symmetries of an equator.

8. The product $s_6 \circ s_3 \circ s_5$ is associated with the permutation $\sigma_6\sigma_3\sigma_5$,which is

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

But applying that permutation two times gives the identity, hence applying it any odd number of times is like applying it once. Our conclusion: when the given symmetry is applied 787 times, vertices 2 and 3 interchange, while vertex 1 remains fixed.

§5.5

2. (a)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$$

(b)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \end{pmatrix}$$

(c)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}$$

(d)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix}$$

(e)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$$

4. There are four components. One has only vertices 1 and 5, another has successive vertices $2, 3, 7, 4, 11$, another has successive vertices $6, 10, 8$, and the last has only vertex 9.

6. From 5.19 we have $(\sigma^s)^1 = \sigma^s$, which in turn is equal to $\sigma^{s \cdot 1}$, proving the result when $t = 1$. Now suppose $(\sigma^s) = \sigma^{st}$ for some k. Then

$$\begin{aligned} \sigma^{s(k+1)} &= \sigma^{sk+s} \\ &= \sigma sk\sigma^s \quad \text{by Theorem 5.22a} \\ &= (\sigma^s)^k\sigma^s \quad \text{by the induction hypothesis} \\ &= (\sigma^s)^k(\sigma^s)^1 \quad \text{by the case } t = 1 \\ &= (\sigma^s)^{k+1} \quad \text{by Theorem 5.22(a)} \end{aligned}$$

This completes the induction argument.

8. (a) $\quad (a_1\, a_2\, \cdots\, a_{2s})^2 = (a_1\, a_3\, \cdots\, a_{2s-1})(a_2\, a_4\, \cdots\, a_{2s})$

(b) $\quad (a_1\, a_2\, \cdots\, a_{2s+1})^2 = (a_1\, a_3\, a_5\, \cdots\, a_{2s+1} a_2\, a_4\, a_6\, \cdots\, a_{2s})$

10. (a) Actually, this is just an instance of Corollary 3.29 (Cancellation Laws). The key here is that if $\alpha = \sigma^{-1}$ then $\sigma\alpha = \alpha\sigma = e$. So if α, β are inverses for σ, then $\sigma\alpha = \sigma\beta = e$.

Multiply this equation by α on the left, and then apply the associative law to get that $\alpha = \beta$.

(b) Use the fact that $(\sigma^{-1})^{-1} = \sigma$ for all $\sigma \in S_n$.

12. (a) Reflexivity: $\sigma^0(x) = x$ and therefore $x \sim x$ for all $x \in \mathbb{N}$. Symmetry: If $x \sim y$, say $\sigma^k(x) = y$, then $\sigma^{-k}(y) = x$ and so $y \sim x$. Transitivity: If $x \sim y$ and $y \sim z$, say $\sigma^k(x) = y$ and $\sigma^t(y) = z$, then $\sigma^{k+t}(x) = z$, hence $x \sim z$.

(b) The equivalence classes are the orbits of the cycles appearing in the factorization of σ into disjoint cycles.

14. There are $\binom{n}{k}$ ways to choose the elements to be involved in the cycle. In writing the cycle in our standard notation, we can pick one of these k elements at random to appear on the left end of the expression. (This choice has no effect on the final cycle.) Then the cycle is determined by the sequence of length $k-1$ appearing to its right, and there are $(k-1)!$ ways to arrange that. By the product rule, the answer is $\binom{n}{k} \times (k-1)! = \frac{n!}{(n-k)!k}$.

§5.6

2. In each case we first express the given permutation as a product of disjoint cycles. [Remark: Experience shows that students have particular trouble doing this with part (b).]

(a) The given permutation is equal to $(1\ 3)(2\ 5\ 4\ 6)$, hence has order 4.

(b) The given permutation is equal to $(1\ 6)(5\ 8)$, hence has order 2.

(c) The given permutation is equal to $(1\ 7\ 11)(2\ 4\ 8\ 3\ 12)(6\ 7)$, hence has order 60.

4. In brief, first note that $(a_1\ a_2\ \cdots\ a_n)^{-1} = (a_n\ a_{n-1}\ \cdots\ a_1)$, thus the inverse of an n-cycle is an n-cycle. In general, if $\sigma = \gamma_1 \cdots \gamma_t$, a product of disjoint cycles, then $\sigma^{-1} = \gamma_t^{-1} \cdots \gamma_1^{-1}$, a product of cycles of the same length as those in the factorization of σ, and the result follows.

6. Consider $\sigma = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9\ 10)$. This has order 30. If a cycle of length ≥ 6 occurred, a quick check shows that the permutation would have order at most 21. A product of two 5-cycles has order 5, and if only cycles of length ≤ 4 occur, the order can be at most 12.

8. The associated permutation factors into $(1\ 6\ 4\ 7\ 3)(2\ 8\ 5)$.

(a) No. Each of tires 2, 8, and 5 will be in service (i.e., in the role of non-spare) only $\frac{2}{3}$ of the time, while each of the other tires will be in service $\frac{4}{5}$ of the time.

(b) 15

10. Factor a and b into primes. Then the lcm of a and b is the integer m whose prime

factors are those appearing in the factorization of at least one of a, b. The exponent of such a prime in the factorization of m is the larger of the exponents to which it occurs in a and b.

§5.7

2. (a) The orbits are two-element sets.

(b) The cycles in the disjoint cycle factorization are unique. So if the permutation is to factor into disjoint transpositions, the cycles in the factorization of σ into disjoint cycles must all be transpositions.

4. In all cases the reversals are these: 1 and 2 reverse, 1 and 5 reverse, 2 and 5 reverse, 3 and 4 reverse, 3 and 5 reverse, 4 and 5 reverse. In particular, none of these elements reverse with any integer ≥ 6.

6. (a) The result is clear when $n = 2$. Assume were done when $n = k$, and suppose $n = k+1$. If $\sigma(k+1) = k+1$, then σ restricts to a permutation of $\mathbb{N}_k$, so it can be expressed in the desired form using transpositions of the form $(1\ a)$, with $a \leq k$. On the other hand, if $\sigma(k+1) = x$ with $x \leq k$, then $(x \quad k+1)\sigma$ fixes $k+1$, hence is a product of transpositions from $\{(1\ 2), \ldots, (1\ k)$. So σ can be expressed as $(x \quad k+1)$ times that product. We will therefore be done if we can show that every transposition can be expessed as a product of transpositions of the form $(1\ y)$. In fact, the formula $(a\ b) = (1\ b)(1\ a)(1\ b)$ does the job.

For another argument, just combine Theorem 5.48 (every permutation is a product of transpositions) with the factorization for $(a\ b)$ given above.

(b) Pick one of the end seats in a theater row. Every rearrangement of the people in that row of seats can be made by a sequence of switches with the person in the end seat (Of course that person is changing from moment to moment.)

8. The result comes by considering a transposition $(a\ b)$, with $a < b$. We have

$$(a\ b) = (a \quad a+1)(a+1 \quad a+2)\cdots(b-2 \quad b-1)(b-1 \quad b)(b-2 \quad b-1)\cdots$$
$$\cdots(a+2 \quad a+3)(a+1 \quad a+2)(a \quad a+1)$$

10. If σ is even (hence a product of an even number of transpositions), then clearly $f(\sigma)$ is odd. The fact that f is injective follows from the cancellation law Corollary 3.29). Finally, if λ is odd then $\tau\lambda$ is even, and $f(\tau\lambda) = \lambda$.

12. This happens when n is odd. (This follows from formula 5.49.)

14. No. The product of two odd permutations is a product of an even number of transpositions, hence an even permutation.

§5.8

2. (a) $\binom{13}{9} = 715$

(b)$\binom{12}{8} = 495$

4. Equality holds (at 0) when $0 \le n \le 3$. If $4 \le n \le 5$, then $\binom{n}{4} > 0$ while $\binom{n}{6} = 0$. Now suppose $n \ge 6$. If $\binom{n}{4} = \binom{n}{6}$, then

$$\frac{n!}{4!\,(n-4)(n-5)(n-6)!} = \frac{n!}{6!\,(n-6)!}$$

Cancellation of $n!$ and $(n-6)!$ from both sides yields $n^2 - 9n + 20 = 30$, and solving this for n yields $n = 10$ as the only possibility. (Note: -1 is also a solution to the quadratic equation, but we have assumed $n \ge 6$.) Indeed, $\binom{10}{4} = \binom{10}{6} = 210$. Summary: The equation $\binom{n}{4} = \binom{n}{6}$ holds when $0 \le n \le 3$ and when $n = 10$.

6. Let $f\colon A_1 \to A_2$ be a bijection, and let S_1, S_2 be the collections of k-subsets of A_1, A_2, respectively. Define $F\colon S_1 \to S_2$ by $F(X_1) = \{\, f(x) \mid x \in X_1 \,\}$. Check that F is a bijection from S_1 to S_2, using the fact that f is a bijection.

8. When we apply the binomial theorem to the given expression, y^3 appears in the term $-\binom{6}{3}(2x)^3(5y)^3 = -20000x^3y^3$, so the answer is $-20000x^3$.

10. (b) Choosing a set of k_1 elements and a set of k_2 elements from a set of n elements can be done by first choosing k_1 elements and then choosing k_2 elements from the remaining elements; by the product formula, there are $\binom{n}{k_1}\binom{n-k_1}{k_2}$ ways to do this. It can also be done by first choosing $k_1 + k_2$ elements and then choosing k_1 elements from those; and there are $\binom{n}{k_1+k_2}\binom{k_1+k_2}{k_1}$ ways to do this. Since the same things has been achieved by both methods, the number of ways to do it must be the same in both cases. This gives the desired equation.

12. (a) $\binom{15}{4}\binom{10}{4}$

(b) $\sum_{n=5}^{8} \binom{10}{n}\binom{15}{8-n}$

(c) $\sum_{n=2}^{8} \binom{10}{n}\binom{15}{8-n}$

14. Call the given set S. First consider the number of ordered triples (A, B, C) in which A, B are 10-element subsets of S and C is a 5-element subset of S, and $A \cup B \cup C = S$. There are $\binom{25}{10}$ possibilities for A, then $\binom{15}{10}$ possibilities for B, and then C consists of the remaining elements. By the product rule, there are $\binom{25}{10}\binom{15}{10}$ possibilities for (A, B, C). But for our present purpose, once a triple (A, B, C) has been selected we don't also need

(B, A, C) (that is, the order in which A and B are chosen doesn't matter). Reasoning as in the solution of Example 5.12, we see that our present answer is $\frac{\binom{25}{10}\binom{15}{10}}{2}$.

16. Corollary 4.16 gives the equation $\sharp(A_1 \cup A_2) = \sharp A_1 + \sharp A_2 - \sharp(A_1 \cap A_2)$. Now divide everything by $\sharp A$ to get the result.

18. (a) 40^{10}

(b) $\binom{10}{7}$

(c) $\binom{40}{7}\binom{10}{7} \cdot 7!$

(d) $\binom{40}{10}$

(e) $\frac{10!}{2!\,3!\,5!}$

(f) $\frac{15!}{5!}$

(g) We follow the suggestion given in the book. The result will be a string of 29 symbols, of which 20 will be x's and 9 will be vertical lines. (Notice: to separate 10 columns from each other, only 9 lines are needed.) The location of the 9 separating lines will determine the distribution of the burgers. Therefore, the answer is $\binom{29}{9}$.

20. Both sides represent the number of sequences of a set of n distinct elements. Multinomial coefficients are concerned with the arrangements of objects, usually grouped into different types, with objects of the same type indistinguishable. In the present exercise, there is only one object of each type. In other words distinct objects are distinguishable from each other.

22. (a) There are 9 positions to be filled with letters. There are $\binom{9}{2}$ ways to choose the positions of the two m's. Then there are 7! ways to distribute the remaining letters. The answer: $\binom{9}{2} \cdot 7!$

(b) First choose the positions to be filled by vowels (once those positions are chosen we know which vowel goes where, because we are preserving their original order), then the positions to be filled by m's, then the positions of the remaining letters. The result: $\binom{9}{4}\binom{5}{2}3!$

24. $\frac{9!}{4!\,2!\,3!}$

CHAPTER 6

§6.1

2. Concatenation involving the empty word is given in the text. Now suppose w_1, w_2 are words of positive length n_1, n_2, respectively. Define $w_1 w_2 \colon \mathbb{N}_{n_1+n_2} \to \Sigma$ by

$$i \longmapsto \begin{cases} w_1(i) & \text{for } 1 \le i \le n_1 \\ w_2(i - n_1) & \text{for } n_1 < i \le n_1 + n_2 \end{cases}$$

4. (a) By assuming the given equation to be true we deduce that $c = 0$. Conversely, if $c = 0$ then the equation holds for all a, b.

(b) For the given equation to make sense, we must have b and c nonzero. Both sides are equal to 0 if $a = 0$. Now suppose $a \neq 0$. Then the given equation yields $c = \pm 1$. Conversely, if $c = \pm 1$ then the given equation holds for all a, b (as long as $b \neq 0$).

6. The set S must contain $a - a = 0$ for $a \in \mathbb{N}$, and it must also contain every number $0 - a = -a$ fora $\in \mathbb{N}$. Thus $\mathbb{Z} \subseteq S$. But subtraction is an operation on $\mathbb{Z}$. Therefore $S = \mathbb{Z}$.

8. There must be an element $e \in S$ with the property that the row of the table in which e appears in the left margin duplicates the listing of the elements of S appearing at the top of the table; and the column of the table above which e appears in the margin above the table duplicates the listing of the elements of S appearing at the left of the table.

10. (a) Define an operation $*$ on the two-element set $\{a, b\}$ by $a * a = a, a * b = b, b * a = a, b * b = a$. Then a is a left identity but not a right identity.

(b) We have $\rho = \lambda\rho = \lambda$. (The left equality follows from the fact that λ is a left identity, the right equality is because ρ is a right identity.) Thus ρ is an identity.

12. Both equations are instances of the associative law. For example, the first equality follows by viewing $a * b, c, d$,respectively, as the three elements written as a, b, c in the associative law given in Definition 6.1.

14. We must fill in a little table with e, a, b down the left margin and across the top from left to right. Since e is given to be the identity, there are only four spaces remaining to be filled inside the table. Note that if $a * x = a * y$ then "$*$ing" the elements in this equation on the left by the inverse of a would give $x = y$ (using the associative law). Therefore no element can appear more than once in any horizontal row inside the table. Similarly, no element can appear more than once in any vertical column inside the table. If $a * a = e$ then we would have $a * b = b$, (in order to have no repetition in the row)

which would put two b's in the last column, which is not allowed. Therefore we must have $a * a = b$, and now we can complete each row and column in only one way in accordance with the "no repetition" rules just observed.

§**6.2**

2. (a) ....another, then the result is the additive inverse of the product of the two integers.

4. First note that $(b+c)+((-b)+(-c)) = (b+(-b))+(c+(-c)) = 0+0 = 0$. Therefore $(-b)+(-c) = -(b+c)$. Now we can prove the stated result: $a-(b+c) = a+(-(b+c)) = a+((-b)+(-c)) = (a+(-b))+(-c) = (a-b)-c$.

6. $ab = ac \Longrightarrow \frac{1}{a}(ab) = \frac{1}{a}(ac) \Longrightarrow (\frac{1}{a}(a)b = (\frac{1}{a}a)c) \Longrightarrow b = c$

8. We claim that $|a|$ is the maximum of a and $-a$. If $a < 0$ then $-a > 0$ by the trichotomy law, and in fact $|a| = -a > 0 > a$, which verifies the claim in this case. Similarly, if $a \geq 0$ then $-a \leq 0$ by the trichotomy law, and $|a| = a \geq -a$. This proves the claim, and the solution to the exercise follows immediately from this.

10. Since $a = (a-b)+b$, the triangle inequality gives $|a| \leq |a-b| + |b|$. Therefore $|a| - |b| \leq |a-b|$. Similarly, $|b|-|a| \leq |b-a| = |(-1)(a-b)| = |a-b|$. But $\big||a|-|b|\big| = \pm(|a|-|b|)$. The result follows.

§**6.3**

2. (a) True. We have $0 = 8 \cdot 0$

(b) True. The hypothesis gives $b = ax$ and $c = by$ for some integers x, y, from which we get $c = by = (ax)y = a(xy)$. The conclusion follows.

(c) True. We have $b = ax$, and so $bc = (ax)c = a(xc)$, which gives the result. [Note that not all of the hypothesis was needed.]

(d) True. From $b = ax$ we get $b = (-a)(-x)$.

(e) False. Let $a = 6, \quad b = 4, \quad c = 9$.

(f) True. If $a = 0$, then the statement $a|b$ gives $b = 0$, so the result holds in this case. Now suppose $a \neq 0$. The hypothesis gives $b = ax$ and $a = by$ for some integers x, y. Then $a = by = (ax)y = a(xy)$. Therefore $xy = 1$. But x and y are integers, so the only possibilities are $x = y = 1$ or $x = y = -1$.

4. If the smallest prime divisor p satisfies $p > \sqrt{|n|}$, then there is a prime $q \geq p$ such

that $|n| = pqa$ for some integer a. But this would give $|n| > (\sqrt{|n|})^2 = |n|$, an absurdity.

6. Because $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$, the conjecture is false.

8. Suppose $\{n, n+2, n+4\}$ is a prime triple, with $n > 3$. From the division algorithm, we know that either $n = 3k+1$ or $n = 3k+2$ for some integer k. But in the first case we would have $n+2 = 3(k+1)$, and in the second case $n+1 = 3(k+1)$. In neither case do we have a prime triple. Contradiction!

10.(a) 8 (b) 231 (c) 17 (d) 1

12. Let $d = (a, a+b)$. From the definition of (a,b) and the hypothesis, it will suffice to show that $d|a$ and $d|b$. [Reasoning: this will show that $d|(a,b)$, from the definition of greatest common divisor. But d is a positive integer, and $(a,b) = 1$ by hypothesis. So $d = 1$ is the only possibility.] We have $d|a$ and $d|(a+b)$, and therefore $d|((a+b)-a)$; that is, $d|b$.

14. (a) $8 = 56 \cdot 2 + 104 \cdot (-1)$

(b) $231 = 3003 \cdot 1 + 462 \cdot (-6)$

(c) $26 = -182 \cdot (-5) + 442 \cdot (-2)$

(d) $1 = 922 \cdot 1043 + 2161 \cdot (-445)$

16. $748 = 2^2 \cdot 11 \cdot 17$, so 748 has divisors

$$\pm1, \pm2, \pm4, \pm11, \pm22, \pm44, \pm17, \pm34, \pm68, \pm187, \pm374, \pm748$$

Also, $1258 = 2 \cdot 17 \cdot 37$ has divisors

$$\pm1, \pm2, \pm17, \pm37, \pm34, \pm74, \pm629, \pm1258$$

The common divisors are $\pm1, \pm2, \pm4, \pm17, \pm34$, and the greatest common divisor is 34.

18. Consider the standard factorization $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$. If we had $k|\alpha_i$ for all i, then n would be a kth power of an integer, contrary to hypothesis. So without loss of generality we can assume α_1 is not divisible by k. If $\sqrt[k]{n} \in \mathbb{Q}$, then $\sqrt[k]{n} = \frac{a}{b}$, for some $a, b \in \mathbb{Z}$. But then $b\sqrt[k]{n} = a$, and so $b^k n = a^k$. But in the standard factorization of a^k the exponent of every prime is a multiple of k, whereas the exponent of p_1 in the standard factorization of $b^k n$ is not a multiple of k. This is a contradiction of the uniqueness of the standard factorization. So our assumption that $\sqrt[k]{n} \in \mathbb{Q}$ must be wrong.

20. (a) Every prime appearing in the standard factorization of d appears to a power less than or equal to the power to which it appears in the standard factorization of n.

(b) If n has standard factorization $p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ and $d|n$, then $d = p_1^{\beta_1} \cdots p_t^{\beta_t}$, with $0 \le \beta_i \le \alpha_i$, for $1 \le i \le t$. Thus there are $\alpha_i + 1$ possibilities for each β_i, so by the product rule there are $\prod_{i=1}^{t}(\alpha_i + 1)$ possiblities for d.

22. Consider the sequence $n! + 2, n! + 3, \cdots, n! + n$. Every term of this sequence is composite, since $n! + k$ is divisible by k when $2 \le k \le n$. Thus we have produced a sequence of $n-1$ consecutive composite numbers. Given any integer M, choosing $n \ge M+2$ produces a sequence of more than M consecutive composite numbers.

§6.4

2. This is true for all $a, b \in \mathbb{Z}$.

4. We must prove that $6|(n^3 - n)$ for all $n \in \mathbb{Z}$, and for this it suffices to show that $2|(n^3 - n)$ and $3|(n^3 - n)$. We have $n^3 - n = n(n+1)(n-1)$. Either n or $n+1$ is even, so we have $2|(n^3 - n)$. If n is not a multiple of 3, then (from the division algorithm) n has one of the forms $3k+1, 3k+2$ for some integer k. In the first case $3|(n-1)$, and in the second case $3|(n+1)$. Thus in all cases $3|(n^3 - n)$.

6. The hypothesis is equivalent to the statement that $a = b + mk$ for some integer k. If $m|b$, say $b = mt$, then $a = m(t+k)$. And if $m|a$, say $a = ns$, then $b = m(s-k)$. Were done.

8. We have $6538 = 24 \cdot 272 + 10$. So 6538 hours is 10 hours more than 272 complete days. Therefore the time will be 6PM.

10. (a) The assumption $ka \equiv kb$ is equivalent to the statement $m|k(a-b)$. Suppose m has standard factorization $p_1^{\alpha_1} \cdots p_t^{\alpha_t}$. The factorization of $k(a-b)$ into primes can be achieved by juxtaposing the standard factorizations of k and $a-b$. Each p_i occurs at least to the power α_i in this factorization, since $m|k(a-b)$. But no p_i occurs in the factorization of m, since we are given that $(k,m) = 1$. Therefore, each p_i occurs at least to the power α_i in the standard factorization of $a-b$. Therefore $m|(a-b)$, which gives $a \equiv b \pmod{m}$.

(b) Yes. For example, $3 \cdot 2 \equiv 3 \cdot 4 \pmod 6$, yet $2 \not\equiv 4 \pmod 6$.

12. (a) Claim: $n \equiv 0$ or $4 \pmod 8$. We have $n = 2k$, so $n^2 = 4k^2$. If k is odd, then $n \equiv 4 \pmod 8$. If k is even then $n^2 \equiv 0 \pmod 8$.

(b) Claim: $n^2 \equiv 1 \pmod 8$. We are given that $n = 2k+1$ for some $k \in \mathbb{Z}$, so $n^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$. But the product $k(k+1)$ is even, and so $8|4k(k+1)$. This proves the claim.

14. The statements and proofs of Theorem 6.45 and Corollary 6.46 survive unscathed when 9 is replaced by 3. Thus an integer is divisible by 3 if and only if the sum of its digits

is divisible by 3. Thus $3|n$ in our present context.

16. The largest power of 7 not exceeding 35481 is $7^5 = 16807$. Division gives $35471 = 2 \cdot 7^5 + 1867$. So the leading digit in base 7 is 2. Continuing in this way, we get $1867 = 5 \cdot 7^3 + 152$, and so on. We eventually get $35481 = 2 \cdot 7^5 + 5 \cdot 7^3 + 3 \cdot 7^2 + 5$, which gives the base 7 representation 205305.

18. 123456789123456789

20. Repeated application of Theorem 6.45 shows these three congruences modulo 9:

$$a \equiv D(a), \quad b \equiv D(b), \quad a + b \equiv D(a+b)$$

From the first two congruences we get

$$a + b \equiv D(a) + D(b) \equiv D(D(a) + D(b)) \pmod 9$$

Therefore

$$D(a+b) \equiv a + b \equiv D(D(a) + D(b)) \pmod 9$$

But $D(a+b)$ and $D(D(a)+D(b))$ are both one-digit numbers, and two one-digit numbers are congruent modulo 9 if and only if they are equal. This finishes the proof.

§**6.5**

2. (a) From the division algorithm, every integer n can be written $n = mq + r$ for unique integers q, r such that $0 \leq r \leq m - 1$. Then $n \equiv r \pmod m$. Uniqueness follows from the fact that no two of $0, \cdots, m-1$ are congruent modulo m.

(b) From part (a) we know that there are exactly m congruence classes modulo m. By the pigeonhole principle, any set with more than m elements would contain two elements from the same congruence class. And a set with fewer than m elements would not include elements congruent to each of the m integers $0, \cdots, m-1$, which we already know to be in different congruence classes.

4 (a) Since $(a, m) = 1$, by Corollary 6.21 there are integers x, y such that $ax + my = 1$. But then $ax \equiv 1 \pmod m$.

(b) Euler's theorem gives $a^{\varphi(m)} \equiv 1 \pmod m$. Therefore $a(a^{\varphi(m)-1}) \equiv 1 \pmod m$, so $x = a^{\varphi(m)-1}$ is a solution.

(c) Choose $y \in \mathbb{Z}$ such that $ay \equiv 1 \pmod m$. Then $a(by) \equiv b \pmod m$.

(d) We have $ax_1 \equiv 1 \equiv ax_2 \pmod m$. The result now follows from the cancellation law (6.51(ii)).

6. (a) $12^{16} \equiv 1 \pmod{17}$.

(b) We have $482 = 16 \cdot 30 + 2$, therefore $12^{482} = (12^{16})^{30} \cdot 12^2 \equiv 12^2 \equiv 8 \pmod{17}$.

8. (a) By Fermat's theorem, if $p \not| a$ then $a^{p-1} \equiv 1 \pmod{p}$. Upon multilplying this congruence by a we get $a^p \equiv a \pmod{p}$. This latter congruence also holds when $p|a$, since then both sides of the congruence are divisible by a. So the congruence holds in all cases.

(b) From the binomial theorem, we have

$$(a+b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k + b^p$$

We claim that when $1 \leq k \leq p-1$, the binomial coefficient $\binom{p}{k}$ is divisible by p. To see this, write $\binom{p}{k} = \frac{p!}{k!\,(p-k)!}$ and observe that while the numerator of this fraction is divisible by p, all the factors of the denominator are smaller than p, hence (because p is prime) are relatively prime to p; so, after cancelling the factors of the denominator with factors of the numerator, a factor of p (and perhaps other factors as well) survives on top. Thus the integer $\binom{p}{k}$ is divisible by p; that is, $\binom{p}{k} \equiv 0 \pmod{p}$ for $1 \leq k \leq p-1$. When this is applied to the above binomial expansion, we get $(a+b)^p \equiv a^p + b^p \pmod{p}$, which was to be proved.

10. We have

$$10^{(\log_{10} 2)(\log_2 3)} = 2^{\log_2 3} = 3 = 10^{\log_{10} 3}$$

Therefore $(\log_{10} 2)(\log_2 3) = \log_{10} 3$. It follows that

$$\log_2 3 = \frac{\log_{10} 3}{\log_{10} 2}$$

§**6.6**

2. $\varphi(600) = \varphi(2^3 \cdot 3 \cdot 5^2) = 160$. So 160 of the integers from 1 to 600 *are* relatively prime to 600. The other 440 are not.

4. Let n have standard factorization $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. If n is odd then

$$\varphi(2n) = 2n(1-\frac{1}{2}) \prod_{i=1}^{r} (1 - \frac{1}{p_i}) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i}) = \varphi(n).$$

But if n is even then some p_i is equal to 2, and then

$$\varphi(2n) = 2n \prod_{i=1}^{r} (1 - \frac{1}{p_i}) = 2\varphi(n).$$

Therefore $\varphi(n) = \varphi(2n)$ if and only if n is odd.

6. From the hypothesis, there are standard factorizations of the form

$$m = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \quad \text{and} \quad n = p_1^{\beta_1} \cdots p_r^{\beta_r} p_{r+1}^{\beta_{r+1}} \cdots p_s^{\beta_s}$$

Then $\varphi(m) = m \prod_{i=1}^{r}(1 - \frac{1}{p_i})$, and

$$\varphi(mn) = mn \prod_{i=1}^{s}(1 - \frac{1}{p_i}) = \varphi(m) \cdot n \prod_{i=r+1}^{s}(1 - \frac{1}{p_i})$$

8. (a) Claim: If $n \in \mathbb{N}$ has standard factorization $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, then

$$f(n) = \prod_{i=1}^{r} f(p_i^{\alpha_i})$$

The proof is by induction on r. If $r = 1$ this is clear. Now suppose the result is true when $r = k$, and consider a number n of the form $n = p_1^{\alpha_1} \cdots p_{k+1}^{\alpha_{k+1}}$ Then

$$f(n) = f(p_1^{\alpha_1} \cdots p_{k+1}^{\alpha_{k+1}}) = f\left((p_1^{\alpha_1} \cdots p_k^{\alpha_k}) \cdot p_{k+1}^{\alpha_{k+1}}\right) = f(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) f(p_{k+1}^{\alpha_{k+1}})$$

because $(p_1^{\alpha_1} \cdots p_k^{\alpha_k}, p_{k+1}^{\alpha_{k+1}}) = 1$ and f is multiplicative. The result now follows from the induction hypothesis.

(b)

$$\sum_{d|n} f(d) = \sum_{(\beta_1,\ldots,\beta_r)} f(p_1^{\beta_1} \cdots p_r^{\beta_r}),$$

(where the sum is over all integer r-tuples $(\beta_1, \ldots, \beta_r)$ such that $0 \leq \beta_i \leq \alpha_i$ for $1 \leq i \leq r$)

$$= \sum_{(\beta_1,\ldots,\beta_r)} \left(\prod_{i=1}^{r} f(p_i^{\beta_i})\right)$$

$$= \prod_{i=1}^{r}(1 + f(p_i) + f(p_i^2) + \cdots + f(p_i^{\alpha_i}))$$

$$= \prod_{i=1}^{r}(\sum_{\beta_i=0}^{\alpha_i} f(p_i^{\beta_i}))$$

(c)

$$\sum_{d|12} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12$$

(d)

$$\begin{aligned}\sum_{d|n}\varphi(d) &= \prod_{i=1}^{r}\Big(\sum_{\beta_i=0}^{\alpha_i}\varphi(p_i^{\beta_i})\Big)\\ &= \prod_{i=1}^{r}\big(1+\varphi(p_i)+\varphi(p_i^2)+\cdots+\varphi(p_i^{\alpha_i})\big)\\ &= \prod_{i=1}^{r}\big(1+(p_i-1)+\cdots+(p_i^{\alpha_i}-p_i^{\alpha_i-1})\big)\\ &= \prod_{i=1}^{r}p_i^{\alpha_i}\\ &= n\end{aligned}$$

10. (a) We follow the suggestion in the book, with $S = S_6$, the symmetric group on six elements. In the notation of the suggestion (and of the inclusion-exclusion principle), we have $|S| = 6!$, $|A_i| = 5!$, $|A_{i_1} \cap A_{i_2}| = 4!$ (if $i_1 \neq i_2$), and so on. Notice that there are $6 = \binom{6}{1}$ sets A_i, $\binom{6}{2}$ sets $A_{i_1} \cap A_{i_2}$, etc. Then the desired quantity is $|A_1' \cap \cdots \cap A_6'|$, and by the inclusion-exclusion principle this is equal to

$$6! - \binom{6}{1}5! + \binom{6}{2}4! - \binom{6}{3}3! + \binom{6}{4}2! - \binom{6}{5}1! + 1 = 265.$$

(b) Reason as in part (a), writing out each binomial coefficient $\binom{n}{k}$ as $\frac{n!}{k!\,(n-k)!}$, and then factoring out $n!$ from the resulting alternating sum. This gives the number of derangements of $\{1, \ldots, n\}$ as

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

Springer
http://www.springer.com/978-1-4614-4264-6

Introduction to Mathematical Structures and Proofs
Gerstein, L.
2012, XIII, 401 p., Hardcover
ISBN: 978-1-4614-4264-6