The Elements of Advanced Mathematics

Fourth Edition

Steven G. Krantz

Chapter 1

Basic Logic

Exercises

1. Construct truth tables for each of the following sentences:

(a) $(\mathbf{S} \wedge \mathbf{T}) \vee \sim (\mathbf{S} \vee \mathbf{T})$

(b) $(\mathbf{S} \vee \mathbf{T}) \Rightarrow (\mathbf{S} \wedge \mathbf{T})$

(c) $(\sim \mathbf{S} \vee \mathbf{T}) \Longrightarrow \sim (\mathbf{S} \wedge \sim \mathbf{T})$

(d) $\mathbf{S} \Rightarrow \big(\mathbf{S} \Rightarrow \big(\mathbf{S} \Rightarrow (\mathbf{S} \Rightarrow \mathbf{T})\big)\big)$

(e) $\mathbf{S} \Rightarrow \big(\sim \mathbf{S} \Rightarrow \big(\mathbf{S} \Rightarrow (\sim \mathbf{S} \Rightarrow \mathbf{T})\big)\big)$

(f) $\big[\mathbf{S} \wedge \big(\mathbf{S} \wedge (\mathbf{S} \wedge \mathbf{T}) \wedge \mathbf{T}\big)\big] \vee \mathbf{T}$

(g) $\mathbf{S} \wedge (\mathbf{T} \vee \sim \mathbf{S})$

(h) $(\mathbf{S} \wedge \sim \mathbf{T}) \Rightarrow (\mathbf{T} \wedge \sim \mathbf{S})$

2. Let

$$\begin{aligned} \mathbf{S} &= \text{All fish have eyelids.} \\ \mathbf{T} &= \text{There is no justice in the world.} \\ \mathbf{U} &= \text{I believe everything that I read.} \\ \mathbf{V} &= \text{The moon's a balloon.} \end{aligned}$$

Express each of the following sentences using the letters $\mathbf{S}, \mathbf{T}, \mathbf{U}, \mathbf{V}$ and the connectives $\vee, \wedge, \sim, \Rightarrow, \Leftrightarrow$. *Do not use quantifiers.*

(a) If fish have eyelids then there is at least some justice in the world.

(b) If I believe everything that I read then either the moon's a balloon or at least some fish have no eyelids.

(c) If either the moon is not a balloon or if there is some justice in the world then I doubt some of the things that I read.

(d) For fish to have eyelids it is necessary for the moon to be a balloon.

(e) If fish have eyelids then there is at least some justice in the world.

(f) For there to be any justice in the world it suffices for fish to have eyelids.

(g) It is not the case that either some fish have no eyelids or that I disbelieve some of what I read.

(h) In order for the moon to be a balloon it is necessary and sufficient for at least some fish to have no eyelids and for there to be some justice in the world.

(i) If the moon is not a balloon and if I do not believe all that I read then at least some fish do not have eyelids.

(j) If I do not believe some of what I read then some fish do not have eyelids.

(k) For me to disbelieve at least some of what I read it is sufficient for there to be at least some justice in the world.

3. Let

$$\begin{aligned} \mathbf{S} &= \text{All politicians are honest.} \\ \mathbf{T} &= \text{Some men are fools.} \\ \mathbf{U} &= \text{I don't have two brain cells to rub together.} \\ \mathbf{W} &= \text{The pie is in the sky.} \end{aligned}$$

Translate each of the following into English sentences:

(a) $(\mathbf{S}\wedge\sim\mathbf{T})\Rightarrow\sim\mathbf{U}$

(b) $\mathbf{W}\vee(\mathbf{T}\wedge\sim\mathbf{U})$

(c) $\mathbf{W}\Rightarrow(\mathbf{S}\Rightarrow\mathbf{T})$

(d) $\mathbf{S}\Rightarrow(\mathbf{S}\vee\mathbf{U})$

(e) $(\mathbf{W}\wedge\mathbf{U})\Longrightarrow(\mathbf{W}\vee\mathbf{U})$

(f) $\big[\sim(\mathbf{W}\wedge\sim\mathbf{T})\big]\vee\big[\sim\mathbf{U}\wedge\mathbf{S}\big]$

(g) $\mathbf{W}\vee(\sim\mathbf{S}\Rightarrow\mathbf{T})$

(h) $\mathbf{S}\Longrightarrow(\mathbf{W}\Rightarrow\mathbf{U})$

(i) $\mathbf{U}\Longrightarrow(\mathbf{W}\Longrightarrow\mathbf{U})$

(j) $\mathbf{U}\Rightarrow(\mathbf{U}\Rightarrow\mathbf{W})$

4. State the converse and the contrapositive of each of the following sentences. Be sure to label each.

(a) In order for it to rain it is necessary that there be clouds.

(b) In order for it to rain it is sufficient that there be clouds.

(c) If life is a bowl of cherries, then I am not in the pits.

(d) If I am not a fool, then mares eat oats.

(e) A sufficient condition for the liquidity of water is that the temperature exceed 32° Fahrenheit.

(f) A necessary condition for peace in the world is that all people disarm.

(g) What's good for the goose is good for the gander.

(h) If wishes were horses, then beggars would ride.

(i) If my grandmother had wheels, she'd be a garbage truck.

(j) If he won't play ball, then he's benched.

(k) If the Donald won't buy it, then it's not worth a dime.

(l) If Melania wants it, then the Donald will buy it.

5. Assume that the universe is the ordinary system $\mathbb{R}$ of real numbers. Which of the following sentences is true? Which is false? Give reasons for your answers.

(a) If π is rational, then the area of a circle is $E = mc^2$.

(b) If $2 + 2 = 4$, then $3/5$ is a rational number.

(c) If $2 + 2 = 5$, then $2 + 3 = 6$.

(d) If both $2 + 3 = 5$ and $2 \cdot 3 = 5$, then the world is flat.

(e) If it is not the case that $3^2 = 9$, then $4^2 = 16$.

(f) If it is not the case that $3^2 = 9$, then $4^2 = 17$.

(g) If it is not the case that $3^2 = 8$, then $4^2 = 16$.

(h) If it is not the case that $3^2 = 8$, then $4^2 = 17$.

(i) If both $3 \cdot 2 = 6$ and $4 + 4 = 8$, then $5 \cdot 5 = 20$.

(j) If both $3 \cdot 2 = 6$ and $4 + 4 = 7$, then $5 \cdot 5 = 20$.

6. For each of the following statements, formulate a logically equivalent one using only $\mathbf{S}$, $\mathbf{T}$, $\sim$, and $\vee$. (Of course you may use as many parentheses as you need.) *Use a truth table or other means to explain why the statements are logically equivalent.*

(a) $\mathbf{S} \Rightarrow \sim \mathbf{T}$

(b) $\sim \mathbf{S} \wedge \sim \mathbf{T}$

(c) $\mathbf{S} \Longrightarrow \sim \mathbf{T}$

(d) $\mathbf{S} \wedge (\mathbf{T} \vee \sim \mathbf{S})$

(e) $(\mathbf{S} \vee \mathbf{T}) \Rightarrow (\mathbf{S} \wedge \mathbf{T})$

(f) $(\mathbf{S} \wedge \mathbf{T}) \Rightarrow (\mathbf{S} \vee \mathbf{T})$

(g) $(\mathbf{S} \Rightarrow \mathbf{T}) \vee (\mathbf{T} \Rightarrow \mathbf{S})$

(h) $[\sim (\mathbf{S} \vee \mathbf{T})] \Rightarrow \mathbf{S}$

7. Redo Exercise 6, this time finding logically equivalent statements that use only $\mathbf{S}$, $\mathbf{T}$, $\sim$, and $\wedge$. *Give reasons for your answers.*

8. Is it possible to find a statement that is logically equivalent to $\mathbf{S} \Rightarrow \mathbf{T}$ but that uses only $\wedge$ and $\vee$ (and not $\sim$)? Why or why not?

9. Translate each of the following statements into symbols, connectives, and quantifiers. Your answers should contain no words. State carefully what each of your symbols stands for. [Note: Each statement is true, but you are not required to verify the truth of the statements.]

(a) The number 5 has a positive square root.

(b) There is a quadratic polynomial equation with real coefficients that has no real root.

(c) The sum of two perfect cubes is never itself a perfect cube.

(d) If $x \cdot y \neq 0$, then $x^2 + y^2 > 0$.

(e) Every positive real number has two distinct real fourth roots.

(f) If z and w are complex numbers, then $z \cdot w$ is also a complex number.

(g) The sum of two irrational numbers need not be irrational.

(h) The product of two irrational numbers need not be irrational.

(i) The sum of two rational numbers is always rational.

(j) The square of a rational number is always rational.

(k) The square root of a rational number need not be rational.

10. In each of the following statements, you should treat the real number system $\mathbb{R}$ as your universe. Translate each statement into an English sentence. Your answers should contain no symbols—only words. [Note: Each statement is true, but you are not required to verify the truth of the statements.]

(a) $\exists x, (x \in \mathbb{R} \wedge x > 0 \wedge \sim \exists y, y > 0 \wedge y^2 = x)$

(b) $\exists x \forall y, (y > x) \Rightarrow (y > 5)$

(c) $\exists x \in \mathbb{R} \exists y \in \mathbb{R}, x^2 + y^2 < 2xy$

(d) $\exists x, x > 0 \wedge x^3 < x^2$

(e) $\sim \exists x, (x \in \mathbb{R} \wedge x > 1 \wedge x > x^2)$

(f) $\exists x, \sim \big(x^2 > 0 \Rightarrow x > 0\big)$

(g) $\exists x, (x \in \mathbb{R} \wedge \sim \exists y, y^3 = x + 1)$

(h) $\exists y \forall x, x^2 + y^4 > 2$

11. Use our standard quantifiers $\forall$ and $\exists$ to translate the sentence "There are exactly five solutions to the equation $P(m) = 0$" into symbols. Now translate the sentence "The equation $Q(m) = 0$ is satisfied by all but four integers."

* **12.** An island is populated by truth-tellers and liars. You cannot tell which is which just by looking at them. You meet an inhabitant of the island. What single question (with a yes/no answer) can you ask him/her that will enable you to ascertain whether this person is a truth-teller or a liar?

13. For each of the following statements, formulate an English sentence that is its negation:

(a) The set S contains at least two integers.

(b) Mares eat oats and does eat oats.

(c) I'm rough and I'm tough and I breathe fire.

(d) This town is not big enough for both of us.

(e) I will marry Fred and disappoint Irving.

(f) I cannot marry either Selma or Flo.

(g) I will pay my taxes and avoid going to jail.

(h) If I am a good boy, then I will do fine.

(i) I love everyone and everyone loves me.

(j) If you study hard, then you will do well in school.

(k) If you get caught, then you will go to jail.

(l) If you work hard, then you will succeed.

(m) If you make more than $100,000, then you pay no income tax.

14. Which of these pairs of statements is logically equivalent? Why?

(a)	$A \vee \sim B$	$\sim A \Rightarrow B$
(b)	$A \wedge \sim B$	$\sim A \Rightarrow \sim B$
(c)	$A \vee (\sim A \wedge B)$	$\sim [\sim A \wedge (A \vee \sim B)]$
(d)	$B \Rightarrow \sim A$	$A \Rightarrow (A \vee B)$
(e)	$A \Leftrightarrow \sim B$	$A \Rightarrow (\sim B \vee \sim A)$
(f)	$\sim (A \vee \sim B)$	$B \wedge \sim A$
(g)	$\sim (A \Rightarrow \sim B)$	$B \Rightarrow A$

15. Formulate, as an English sentence (without symbols), the negation of each of the statements in Exercise 10.

16. Give a logical demonstration (i.e., a "proof") that any statement in sentential logic can be formulated using just $\sim$ and $\wedge$. That is, given any statement P there is a logically equivalent statement P' such that P' uses only the connectives $\sim$ and $\wedge$.

17. Give a logical demonstration (i.e., a "proof") that any statement in sentential logic can be formulated using just $\sim$ and $\vee$. That is, given any statement P there is a logically equivalent statement P' such that P' uses only the connectives $\sim$ and $\vee$.

18. Give a logical demonstration (i.e., a "proof") that any statement in sentential logic can be formulated using just $\sim$ and $\Rightarrow$. That is, given any statement P there is a logically equivalent statement P' such that P' uses only the connectives $\sim$ and $\Rightarrow$.

19. Use a truth table to show that *not every* logical statement can be formulated using $\vee$ and $\wedge$.

* **20.** There is actually a single logical connective—different from the ones that we have studied in the present chapter—with the property that every statement in sentential logic can be formulated *using that one connective only*. Endeavor to define such a connective.

21. You are given atomic sentences A, B, C. Also you are given the connectives $\vee$, $\wedge$, and $\sim$ (one of each). Using as many parentheses as you like, how many different compound sentences can you form using these components?

22. Explain why $\forall$ is logically equivalent to $\sim \exists \sim$.

23. Explain why $\exists$ is logically equivalent to $\sim \forall \sim$.

24. Explain why $\forall\exists$ and $\exists\forall$ are *not* the same.

Chapter 2

Methods of Proof

Exercises

1. Prove that the product of two odd natural numbers must be odd.

2. Prove that if n is an even natural number and if m is *any* natural number, then $n \cdot m$ must be even.

3. Prove that the sum of the squares of the first n natural numbers is equal to

$$\frac{2n^3 + 3n^2 + n}{6}.$$

4. Prove that the sum of the first k even natural numbers is $k^2 + k$.

5. Prove—*not* by mathematical induction—that the sum of the first k odd natural numbers is k^2.

6. Prove that if n red letters and n blue letters are distributed among n mailboxes, then either some mailbox contains at least two red letters or some mailbox contains at least two blue letters or else some mailbox contains at least one red and one blue letter.

7. Prove that, if m is a power of 3 and n is a power of 3, then $m + n$ is never a power of 3.

8. What is special about the number 3 in Exercise 7? What other natural numbers can be used in its place?

9. Imitate the proof of Pythagoras's theorem to show that the number 5 does not have a rational square root.

10. Prove that if n is a natural number and if n has a rational square root, then in fact the square root of n is an integer.

11. Complete this sketch to obtain an alternative proof that the number 2 does not have a rational square root:

(a) Take it for granted that it is known that each positive integer has one and only one factorization into prime factors (a prime number is a positive integer, greater than 1, that can be divided evenly only by 1 and itself).

(b) Seeking a contradiction, suppose that $\alpha = p/q$ is a rational square root of 2 (we need *not* assume that the rational fraction p/q is reduced to lowest terms).

(c) Then $2 = p^2/q^2$ or $2q^2 = p^2$.

(d) Count the number of prime factors on either side of the last equation in part **(c)** to arrive at a contradiction.

12. Prove that if the natural number n is a perfect square, then $n + 1$ will never be a perfect square.

13. Prove that if the product of two integers is even, then one of them must be even.

14. Prove that if the product of two integers is odd, then both of them must be odd.

15. Prove that any integer can be written as the sum of at most two odd integers. Is the same true if "odd" is replaced by "even"?

* **16.** A popular recreational puzzle hypothesizes that you have nine pearls that are identical in appearance. Eight of these pearls have the same weight, but the ninth is either heavier or lighter—you do not know which. You have a balance scale (see Figure 2.3), and are allowed three weighings to find the odd pearl. How do you proceed?

Figure 2.1: A balance scale.

Now here is a bogus proof by mathematical induction that you can solve the problem in the first paragraph in three weighings not just for nine pearls but for *any number of pearls*. For convenience let us begin the mathematical induction with the case $n = 9$ pearls. By the result of the first paragraph, we can handle that case. Now, inductively, suppose that we have an algorithm for handling j pearls. We use this hypothesis to treat $(j + 1)$ pearls. From the $(j + 1)$ pearls, remove one and put it in your pocket. There remain j pearls. Apply the j-pearl algorithm to these remaining pearls. If you find the odd pearl, then you are done. If you do not find the odd pearl, then it is the one in your pocket. That completes the case $(j + 1)$ and the proof.

What is the flaw in this reasoning? [*Remark*: If you are fiendishly clever, then you can actually handle 12 pearls in the original problem—with just three weighings. However, this requires the consideration of 27 cases.]

In each of Exercises 17–26, either prove that the statement is true or give a counterexample. Remember that a counterexample to a "for all" statement consists of a single example; but a counterexample to a "there exists" statement consists in showing that something never occurs.

17. The sum of two perfect squares is a perfect square.

* **18.** Let n be a positive integer. In the list $n, n + 1, n + 2, \ldots, 2n + 2$ there must be a perfect square.

19. There is a positive integer that is the sum of all its divisors that are less than itself (including the divisor 1). Such a number is called a *perfect number*.

20. The difference of two perfect squares is never a prime (refer to Exercise 11 for the definition of "prime").

21. The sum of two perfect squares is never a prime.

22. For x a positive real number we have $1 + x^2 < (1 + x)^2$.

* **23.** For any positive real numbers $a_1, a_2, \ldots, a_n$ we have

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \leq \left(a_1 \cdot a_2 \cdots a_n\right)^{1/n}.$$

24. Between any two distinct real numbers there is a rational number.

25. Between any two distinct rational numbers there is an irrational number.

* **26.** Let m and n be two successive perfect cubes. Then between them must lie a perfect square.

27. Prove by mathematical induction that every natural number greater than 1 has a prime factor (refer to Exercise 11 for the definition of "prime").

* **28.** Prove by mathematical induction that the sum of the angles interior to a convex polygon with k sides is $(k - 2) \cdot 180^\circ$ (begin with $k = 3$ and you may assume that the result is known for triangles).

29. Prove that if k is a natural number that is greater than 2, then $2^k > 1 + 2k$.

* **30.** Prove that the method of complete mathematical induction is logically equivalent to the method of ordinary mathematical induction.

31. Give a formal discussion of why the mathematical induction process may be begun at any natural number—not just 1.

* **32.** Fix a number $q > 0$. Use mathematical induction on the positive integer n to prove the following formula of Ramanujan:

$$\begin{aligned} 1 + \frac{q}{1-q} + \frac{q^2}{(1-q)(1-q^2)} + \frac{q^3}{(1-q)(1-q^2)(1-q^3)} \\ + \cdots + \frac{q^n}{(1-q)(1-q^2)\cdots(1-q^n)} \\ = \quad \frac{1}{(1-q)(1-q^2)\cdots(1-q^n)} \end{aligned}$$

* **33.** Use mathematical induction on n to prove that the formula in Exercise 32 still holds if the sequence of exponents $1, 2, 3, \ldots, n$ is replaced by the sequence of square exponents $1, 4, 9, \ldots, n^2$.

34. Prove that, if n is an integer greater than 4, then $2^n > n^2 + 1$.

35. Prove the pigeonhole principle by mathematical induction.

36. Give a direct proof of the pigeonhole principle.

37. You write 27 letters to 27 different people. Then you address the 27 envelopes. You close your eyes and stuff one letter into each envelope. What is the probability that just one letter is in the wrong envelope?

* **38.** You have a finite collection of points in the plane, not all colinear. Prove that there is a line passing through just two of these points.

* **39.** A tangled up piece of string of length 1 lies in the plane. Prove that there is a rectangle containing the string that has area not exceeding $1/4$.

40. Formulate a statement, using only the quantifier $\exists$ and *not* the quantifier $\forall$, that expresses the thought that all boys under the age of 10 practice all pieces in their piano book every day.

* **41.** Let a be a nonzero real number. Prove by mathematical induction that, for any positive integer n,

$$\begin{pmatrix} a & 2 \\ 0 & a \end{pmatrix}^n = \begin{pmatrix} a^n & 2na^{n-1} \\ 0 & a^n \end{pmatrix}$$

42. Use mathematical induction to prove that every positive integer of the form $n^3 - n$ is divisible by 6.

* **43.** Use mathematical induction to prove the identity

$$\frac{2^2}{1 \cdot 3} \cdot \frac{3^2}{2 \cdot 4} \cdots \frac{n^2}{(n-1)(n+1)} = \frac{2n}{n+1}\,.$$

44. Use mathematical induction to prove that

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{1998}} \geq \sqrt{1998}\,.$$

[**Hint:** Formulate a statement that depends on n (instead of on 1998) and prove *that* by mathematical induction on n.]

Chapter 3

Set Theory

3.1 Undefinable Terms

Exercises

1. Let $S = \{1, 2, 3, 4, 5\}$, $T = \{3, 4, 5, 7, 8, 9\}$, $U = \{1, 2, 3, 4, 9\}$, $V = \{2, 4, 6, 8\}$. Calculate each of the following:

(a) $S \cap U$
(b) $(S \cap T) \cup U$
(c) $(S \cup U) \cap V$
(d) $(S \cup V) \setminus U$
(e) $(U \cup V \cup T) \setminus S$
(f) $(S \cup V) \setminus (T \cap U)$
(g) $(S \times V) \setminus (T \times U)$
(h) $(V \setminus T) \times (U \setminus S)$

2. Let S be any set and let $T = \emptyset$. What can you say about $S \times T$?

3. Prove the following formulas for arbitrary sets S, T, U, and V. [**Hint:** You may find Venn diagrams useful to guide your thinking, but a Venn diagram is *not* a proof.]

(a) $S \cap \big(T \cup U\big) = (S \cap T) \cup (S \cap U)$
(b) $S \cup \big(T \cap U\big) = (S \cup T) \cap (S \cup U)$
(c) $S \cap {}^cT = S \setminus T$
(d) $(S \setminus T) \cup (T \setminus S) = (S \cup T) \setminus (S \cap T)$
(e) $S \setminus (T \cup U) = (S \setminus T) \cap (S \setminus U)$
(f) $S \setminus (T \cap U) = (S \setminus T) \cup (S \setminus U)$
(g) $(S \setminus T) \times (U \setminus V) = (S \times U) \setminus \big[(S \times V) \cup (T \times U)\big]$
(h) $(S \cup T) \times V = (S \times V) \cup (T \times V)$

4. Let $S_\alpha \subset X$ be sets indexed over an arbitrary index set A, $\alpha \in A$. Prove each of the following identities:

(a) ${}^c\big(\cap_{\alpha\in A} S_\alpha\big) = \cup_{\alpha\in A} {}^cS_\alpha$
(b) ${}^c\big(\cup_{\alpha\in A} S_\alpha\big) = \cap_{\alpha\in A} {}^cS_\alpha$
(c) $T \cap \big(\cup_{\alpha\in A} S_\alpha\big) = \cup_{\alpha\in A}\big(T \cap S_\alpha\big)$
(d) $T \cup \big(\cap_{\alpha\in A} S_\alpha\big) = \cap_{\alpha\in A}\big(T \cup S_\alpha\big)$

5. Draw Venn diagrams to illustrate parts (a)– (f) of Exercise 3.3.

6. Suppose that $A \subset B \subset C$. What is $A \setminus B$? What is $A \setminus C$? What is $A \cup B$?

In Exercises 3.7–3.9, let $\mathbb{N}$ denote the natural numbers, $\mathbb{Z}$ the integers, $\mathbb{Q}$ the rational numbers, and $\mathbb{R}$ the real numbers.

7. Describe the set $\mathbb{Q} \setminus \mathbb{Z}$ in words. Describe $\mathbb{R} \setminus \mathbb{Q}$.

8. Describe $\mathbb{Q} \times \mathbb{R}$ in words. Describe $\mathbb{Q} \times \mathbb{Z}$.

9. Describe $(\mathbb{Q} \times \mathbb{R}) \setminus (\mathbb{Z} \times \mathbb{Q})$ in words.

10. Give an explicit description of the power set of $S = \{a, b, 1, 2\}$ (that is, write out all the elements).

11. Let the set S have k elements. Give a direct proof (different from the one in the text) of the assertion that the number of elements of the power set of S is 2^k. That is, devise an explicit scheme for counting the subsets.

12. Calculate the power set of the power set of $T = \{1, 2\}$.

13. TRUE or FALSE: If $S_1, S_2, \ldots$ are sets of integers and if $\cup_{j=1}^{\infty} S_j = \mathbb{Z}$, then one of the sets S_j must have infinitely many elements. Give a proof of your answer.

14. TRUE or FALSE: If $S_1, S_2, \ldots$ are sets of real numbers and if $\cup_{j=1}^{\infty} S_j = \mathbb{R}$, then one of the sets S_j must have infinitely many elements. Give a proof of your answer.

15. Prove that $S \subset T$ if and only if $\mathcal{P}(S) \subset \mathcal{P}(T)$.

16. Prove that $S = T$ if and only if $\mathcal{P}(S) = \mathcal{P}(T)$.

17. Prove that if $A \subset B$ and $B \subset C$ then $A \subset C$.

18. Let $S = \{a, b, c, d\}$, $T = \{1, 2, 3\}$, and $U = \{b, 2\}$. Which of the following statements is true?

(a) $\{a\} \in S$

(b) $a \in S$

(c) $\{a, c\} \subset S$

(d) $\emptyset \in S$

(e) $\{a\} \in \mathcal{P}(S)$

(f) $\big\{\{a\}, \{a, b\}\big\} \subset \mathcal{P}(S)$

(g) $\{a, c, 2, 3\} \subset S \cup T$

(h) $U \subset S \cup T$

(i) $b \in S \cap U$

(j) $\{b\} \subset S \cap U$

(k) $\{1, 3\} \in T$

(l) $\{1, 3\} \subset T$

(m) $\{1,3\} \in \mathcal{P}(T)$

(n) $\emptyset \in \mathcal{P}(S)$

(o) $\{\emptyset\} \in \mathcal{P}(S)$

(p) $\emptyset \subset \mathcal{P}(S)$

(q) $\{\emptyset\} \subset \mathcal{P}(S)$

19. Write out the power set of each set:

(a) $\big\{1, \emptyset, \{a,b\}\big\}$

(b) $\big\{\bullet, \triangle, \partial\big\}$

(c) $\Big\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\Big\}$

20. Prove by mathematical induction on k that, if the set S has k elements and the set T has ℓ elements, then $S \times T$ has $k \cdot \ell$ elements.

21. Prove or disprove each of the following statements:

(a) $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$

(b) $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$

(c) $\mathcal{P}(A \setminus B) = \mathcal{P}(A) \setminus \mathcal{P}(B)$

22. If $S \subset T_\alpha$ for every $\alpha \in A$ then prove that

$$S \subset \cap_{\alpha \in A} T_\alpha$$

23. If $S \supset T_\alpha$ for every $\alpha \in A$ then prove that

$$S \supset \cup_{\alpha \in A} T_\alpha$$

24. Let $\{A_j\}$ be sets. We say that the A_j are *disjoint* if $\cap_j A_j = \emptyset$. On the other hand, the A_j are *pairwise disjoint* if $A_j \cap A_k = \emptyset$ whenever $j \neq k$. Show that these two concepts are different for four sets.

25. Let S, T, U be finite sets. Verify that the sets $(S \times T) \times U$ and $S \times (T \times U)$ have the same number of elements.

26. Let S be an infinite set and suppose that $T \subset S$. Prove that either T is infinite or $S \setminus T$ is infinite.

27. Suppose that S is a set and that $S \times T$ is finite for every choice of finite set T. Prove that then S must be finite.

28. Suppose that S is a set and that $S \cup T$ is finite for every choice of finite set T. Prove that then S must be finite.

* **29.** Let $\mathcal{P}$ be the power set of $I = \{1, 2, 3, 4, 5\}$. Let $\mathcal{S}$ be a randomly chosen subset of $\mathcal{P}$. What is the probability that $\mathcal{S}$ is the power set of some subset of I?

Chapter 4

Relations and Functions

4.1 Relations

Exercises

1. Consider the relation on $\mathbb{Z}$ defined by $(m, n) \in \mathcal{R}$ if $m + n$ is even. Prove that this is an equivalence relation. What are the equivalence classes?

2. Consider the relation on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ defined by $(m, n)\mathcal{R}(m', n')$ provided that $m \cdot n' = m' \cdot n$. Prove that this is an equivalence relation. Can you describe the equivalence classes?

3. Consider the relation on $\mathbb{Z} \times \mathbb{Z}$ defined by $(m, n)\mathcal{R}(m', n')$ provided that $m + n' = m' + n$. Prove that this is an equivalence relation. Can you describe the equivalence classes? Can you pick a representative for each equivalence class that will help to exhibit what the equivalence relation is?

4. Consider the relation defined on the cartesian plane by $(x, y)\mathcal{R}(x', y')$ if $y = y'$. Prove that this is an equivalence relation. Can you describe the equivalence classes? Can you pick a representative for each equivalence class that will help to exhibit what the equivalence relation is?

5. Consider the relation defined on the cartesian plane by $(x, y)\mathcal{R}(x', y')$ if $y - y'$ is an integer and $x - x'$ is an integer. Prove that this is an equivalence relation. Can you describe the equivalence classes? Can you pick a representative for each equivalence class that will help to exhibit what the equivalence relation is?

6. Consider the relation defined on the collection of all circles in the Euclidean plane by $C_1 \mathcal{R} C_2$ if the circle C_1 and the circle C_2 have the same center. Prove that this is an equivalence relation. Can you describe the equivalence classes? Can you pick a representative for each equivalence class that will help to exhibit what the equivalence relation is?

7. Let S be the set of all living people. Let $x, y \in S$. Say that x is related to y if x and y have some blood relation in common. Is this an equivalence relation? Why or why not?

8. Consider the relation on $\mathbb{Q} \times (\mathbb{Q} \setminus \{0\})$ defined by $(m, n)\mathcal{R}(m', n')$ provided $m \cdot n' = m' \cdot n$. Prove that this is an equivalence relation. Can you describe the equivalence classes? Why is the outcome in this exercise different from that in Exercise 4.2?

9. Let $S = \{a, b, c, d\}$ and $T = \{1, 2, 3, 4, 5, 6, 7\}$. Which of the following relations on $S \times T$ is a function?

(a) $\big\{(\mathbf{a}, \mathbf{4}), (\mathbf{d}, \mathbf{3}), (\mathbf{c}, \mathbf{3}), (\mathbf{b}, \mathbf{2})\big\}$
(b) $\big\{(\mathbf{a}, \mathbf{5}), (\mathbf{c}, \mathbf{4}), (\mathbf{d}, \mathbf{3})\big\}$
(c) $\big\{(\mathbf{a}, \mathbf{1}), (\mathbf{b}, \mathbf{1}), (\mathbf{c}, \mathbf{1}), (\mathbf{d}, \mathbf{1})\big\}$
(d) $\big\{(\mathbf{a}, \mathbf{2}), (\mathbf{b}, \mathbf{2}), (\mathbf{c}, \mathbf{3}), (\mathbf{d}, \mathbf{3})\big\}$
(e) $\big\{(\mathbf{d}, \mathbf{1}), (\mathbf{c}, \mathbf{2}), (\mathbf{b}, \mathbf{3}), (\mathbf{a}, \mathbf{4})\big\}$
(f) $\big\{(\mathbf{d}, \mathbf{7}), (\mathbf{c}, \mathbf{6}), (\mathbf{c}, \mathbf{5}), (\mathbf{a}, \mathbf{4}), (\mathbf{b}, \mathbf{2})\big\}$
(g) $\big\{(\mathbf{a}, \mathbf{6}), (\mathbf{c}, \mathbf{9})\big\}$

10. Which of the following functions is one-to-one? Which is onto?

(a) $f : \mathbb{N} \to \mathbb{N}$ $\quad f(m) = m + 2$
(b) $g : \mathbb{Z} \to \mathbb{Z}$ $\quad g(m) = 2m - 7$
(c) $h : \mathbb{R} \to \mathbb{R}$ $\quad h(x) = x - x^3$
(d) $f : \mathbb{Q} \to \mathbb{Q}$ $\quad f(x) = x^2 + 4x$
(e) $g : \mathbb{N} \to \mathbb{N}$ $\quad g(n) = n(n + 1)$
(f) $h : \mathbb{R} \to \mathbb{R}$ $\quad h(n) = +\sqrt{n^2 + 1}$
(g) $f : \mathbb{Z} \to \mathbb{N}$ $\quad f(n) = n^2 + n + 1$

(h) $g : \mathbb{N} \to \mathbb{Z}$ $\qquad g(k) = k^3 + 2k$
(i) $h : \mathbb{N} \to \mathbb{Q}$ $\qquad h(t) = t/(t+1)$
(j) $f : \mathbb{Q} \to \mathbb{Q}$ $\qquad f(y) = y^2 - y$

11. Consider all ordered triples of positive integers. If $\alpha = (a, b, c)$ and $\alpha' = (a', b', c')$ are two such triples, then we say that $\alpha < \alpha'$ if either

(a) $a < a'$
(b) $a = a'$ and $b < b'$

or

(c) $a = a'$, $b = b'$, and $c < c'$.

Discuss, in the language of Section 4.2, what type of order relation this is. This ordering is called the *lexicographic ordering*. In view of the way that we order words in a dictionary, explain why the ordering just described deserves that name.

12. Explain how the ordering described in Exercise 5.11 can be generalized to ordered k-tuples $(a_1, \ldots, a_k)$ of positive integers.

13. Consider the set S of all infinite sequences $\{a_1, a_2, \ldots\}$ of real numbers. Say that two such sequences $\alpha = \{a_1, a_2, \ldots\}$ and $\alpha' = \{a'_1, a'_2, \ldots\}$ satisfy $\alpha \leq \alpha'$ if the terms of α are eventually less than or equal to the terms of α'. This means that there exists a $K > 0$ such that $a_j \leq a'_j$ for all $j \geq K$. Discuss, in the language of Section 4.2, what sort of order relation this is.

14. Consider a relation defined on all living people defined by $a\mathcal{R}b$ if a and b are of the same sex and a is strictly younger than b. Is this an equivalence relation? Does it fit one of the orderings described in Section 4.2?

15. Express parts **(b)**, **(c)**, **(d)** of Definition 4.4.1 using the language of ordered pairs. Imitate our discussion of part **(a)** in the text.

* **16.** Classify the Pythagorean triples. That is, find all triples m, n, p of positive integers such that $m^2 + n^2 = p^2$. [**Hint:** Consider m, n, p of the form $m = s^2 - t^2$, $n = 2st$, $p = s^2 + t^2$, for s, t positive integers with no common divisors.]

17. Give an example of a function $f : \mathbb{N} \to \mathbb{Z}$ that is onto.

18. Give an example of a function $f : \mathbb{Q} \to \mathbb{N}$ that is onto.

19. Prove that there is no function $g : \mathbb{N} \to \mathbb{R}$ that is onto.

20. What is the cardinality of each of the following sets?

(a) $\mathbb{N} \times \mathbb{Q}$

(b) $\mathbb{N} \times \mathbb{N}$

(c) $\mathbb{R} \times \mathbb{Q}$

(d) $\mathcal{P}(\mathbb{Q})$

(e) $\mathbb{C}$

(f) $\mathbb{R} \setminus \mathbb{N}$

(g) $\mathbb{Q} \setminus \mathbb{N}$

(h) The set of all decimal expansions, terminating or nonterminating, that include only the digits 3 and 7.

(i) The set of all *terminating* decimal expansions that include only the digits 3 and 7.

(j) The set of all solutions of all quadratic polynomials with integer coefficients.

(k) The set of all solutions of all quadratic polynomials with real coefficients.

(l) The set of all subsets of $\mathbb{N}$ that have at least three and not more than eight elements.

(m) The set of all subsets of $\mathbb{Z}$ with at least six elements.

* **21.** Let S and T be sets and let $f : S \to T$ and $g : T \to S$ be arbitrary functions. Prove that there is a subset $A \subset S$ and a subset $B \subset T$ such that $f(A) = B$ and $g(T \setminus B) = S \setminus A$.

* **22.** Find all functions $f : \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{0\}$ that are one-to-one and onto and such that $f^{-1}(x) = 1/f(x)$.

* **23.** Let $f : \mathbb{R} \to \mathbb{R}$ be a function with the property that every x in $\mathbb{R}$ is a local minimum. That is, for $x \in \mathbb{R}$ there is an $\epsilon_x > 0$ so that if $t \in (x - \epsilon_x, x + \epsilon_x)$, then $f(t) \geq f(x)$. Then prove that the image of f is countable.

24. Construct an onto function $f : \mathbb{R} \to \mathbb{R} \times \mathbb{R}$. Use this function to equip $\mathbb{R} \times \mathbb{R}$ with an ordering.

25. Find the domain and image of each of these relations:

(a) $\{(x, y) \in \mathbb{R} \times \mathbb{R} : x = \sqrt{y + 3}\}$
(b) $\{(x, y) \in \mathbb{Q} \times \mathbb{Q} : y = 1/(x^2 - 4)\}$
(c) $\big\{(\alpha, \beta) : \alpha \text{ is a person, } \beta \text{ is a person, and } \alpha \text{ is the father of } \beta\big\}$
(d) $\big\{(\alpha, \beta) : \alpha \text{ is a person, } \beta \text{ is a person, and } \alpha \text{ is a parent of } \beta\big\}$
(e) $\{(x, y) \in \mathbb{Q} \times \mathbb{Q} : x^2 + y^2 < 1\}$
(f) $\{(x, y) \in \mathbb{N} \times \mathbb{Q} : x \cdot y \text{ is an integer}\}$
(g) $\{(x, y) \in \mathbb{R} \times \mathbb{R} : x \cdot y \text{ is rational}\}$
(h) $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x - y = 2\}$

26. We have used the phrase "ordered pair" in this book without giving a precise definition of the phrase. As noted in the text, we *could* define the ordered pair (a, b) to be the set $\big\{\{a\}, \{a, b\}\big\}$. This is clearly distinct from the ordered pair (b, a), which would be $\big\{\{b\}, \{b, a\}\big\} = \big\{\{b\}, \{a, b\}\big\}$. Using this technical definition, *prove* that $(a, b) = (a', b')$ if and only if $a = a'$ and $b = b'$.

27. Give a rigorous definition of "ordered triple" based on the ideas in Exercise 4.26.

28. Declare two real numbers to be related if their difference is rational. Prove that this is an equivalence relation. How many elements are in each equivalence class? How many equivalence classes are there?

29. Formulate a notion of composition of two relations. Formulate a notion of the inverse of a relation. Now express the ideas of reflexivity, symmetry, and transitivity for a relation in the language of inverse and composition of relations.

30. Let $A = \{1, 2, 3\}$, $B = \{a, b, c\}$, $C = \{s, t, u\}$. Define functions

$$\begin{aligned} f &= \{(1, c), (2, c), (3, a)\} \\ g &= \{(a, t), (b, s), (c, u)\} \end{aligned}$$

What are the domain and image of f? What are the domain and image of g? Calculate $g \circ f$ and g^{-1}.

31. Give precise meaning to, and prove, the statement that the intersection of two functions is a function. Is it also the case that the union of two functions is a function?

32. Give an explicit example of a function $f : \mathbb{Q} \to \mathbb{Q}$ such that f is one-to-one and onto but such that $f(x) > x^3$ for every x.

33. Let $f : \mathbb{R} \to \mathbb{R}$ be a function. Suppose that, for every surjective function $g : \mathbb{R} \to \mathbb{Z}$, it holds that $g \circ f$ is surjective. Then prove that f is surjective.

34. Let X be a set such that there exists a surjective function $f : X \to \mathbb{Z}$. Then prove that X is infinite.

35. Let X be a set such that there exists a surjective function $f : X \to \mathbb{R}$. Then prove that X is uncountable.

36. Consider the following relation on $\mathbb{N}$: $(x, y) \in \mathcal{R}$ if $x < y + 2$. What sort of order relation is $\mathcal{R}$?

37. Consider the following relation on $\mathbb{N}$: $(x, y) \in \mathcal{R}$ if $x < y - 2$. What sort of order relation is $\mathcal{R}$?

38. Let S be the set of all living people. Tell which of the following are equivalence relations on S. Give detailed reasons for your answers.

(a) x is related to y if x and y are siblings

(b) x is related to y if y is presently a spouse of x

(c) x is related to y if y has at one time or another been a spouse of x

(d) x is related to y if y is a parent of x

(e) x is related to y if y is a child of x

(f) x is related to y if x hates y but y loves x

(g) x is related to y if x hates y and y hates x

(h) x is related to y if x and y have a common ancestor

39. Let S be the collection of all polynomials with real coefficients. Say that $p, q \in S$ are related if the number 0 is a root of $p - q$. Is this an equivalence relation on S?

40. Redo Example 4.5.10 by laying out the ordered pairs in a tableau (see below) and counting them along diagonals that proceed from the lower left to the upper right.

$$\begin{array}{cccc} (1,1) & (1,2) & (1,3) & (1,4) & \dots \\ (2,1) & (2,2) & (2,3) & (2,4) & \dots \\ (3,1) & (3,2) & (3,3) & (3,4) & \dots \\ & & \dots & & \end{array}$$

* **41.** In this exercise we indicate why any infinite set can be put into a set-theoretic isomorphism with a proper subset of itself. You should provide the details.

Let S be a set with infinitely many elements. By Proposition 4.5.24, there is a subset $T \subset S$ that is countable. Now we know that the set of natural numbers can be placed in one-to-one correspondence with a proper subset of itself, hence so can T be placed in one-to-one correspondence with a proper subset T' of itself. Let g denote the set-theoretic isomorphism of T with T'.

Now set $U = S \setminus T$. We may construct a set theoretic isomorphism of $S = U \cup T$ to $U \cup T'$ (a proper subset of S) by following these rules:

(a) Map each element of U to itself;

(b) Map each element $t \in T$ to $g(t) \in T'$.

42. TRUE or FALSE: If $S_1 \supset S_2 \supset \cdots$ are each uncountable sets then $\cap_j S_j$ is a nonempty, indeed an uncountable, set.

43. Let A and B be sets. Let us say that A and B are related if there exists a set theoretic isomorphism from A to B. Prove that this is an equivalence relation. Each equivalence class is called a *cardinal number*.

44. Say that two real numbers x and y are related if there is an integer k such that $k < x \leq k + 1$ and $k < y \leq k + 1$. Explain why this is an equivalence relation. Draw a figure that shows the equivalence classes in the real line.

45. Say that two real numbers are related if the first five digits of each of their decimal expansions (the five digits to the right of the decimal point) are equal. After giving a precise formulation of this relation, show that it is an equivalence relation. Give a verbal description of each equivalence class.

46. Give an explicit example of a function $f : \mathbb{Q} \to \mathbb{Q}$ such that f is one-to-one and onto but such that $f(x) \neq x$ for every x.

47. Write $\mathbb{N} \times \mathbb{N}$ as the countable union of finite sets. Conclude that $\mathbb{N} \times \mathbb{N}$ is countable.

48. Write $\mathbb{N} \times \mathbb{N}$ as the finite union of countable sets. Conclude that $\mathbb{N} \times \mathbb{N}$ is countable.

49. Let S and T be sets. We let T^S denote the set of all functions from S to T. For the specific example $S = \{1, 2, 3\}$ and $T = \{a, b\}$, write out the set T^S. Also write out the set S^T.

50. Refer to Exercise 4.49 for notation. Suppose that the set S has k elements and the set T has m elements, with k, m positive integers. What does the set S^T have to do with the number k^m?

51. Refer to Exercise 4.49 for notation. Let S be a finite set and let T be a set with three elements. Prove that there is a one-to-one correspondence between S^T and $S \times S \times S$.

52. Refer to Exercise 4.49 for notation. Let $S = \{1, 2\}$, $T = \{a, b, c\}$, and $U = \{\alpha, \beta\}$. Prove that there is a natural one-to-one correspondence between $(S^T)^U$ and $S^{T \times U}$.

53. Refer to Exercise 4.49 for notation. Let S be a set and let T be the empty set $\emptyset$. What can you say about S^T and T^S?

54. Exhibit a one-to-one correspondence of the set $\mathbb{R}$ of real numbers with a proper subset of $\mathbb{R}$. [**Hint:** Refer to Exercise 4.41.]

55. Write the set of all sequences of 0's and 1's using the notation introduced in Exercise 4.49.

56. Refer to Example 4.1.3. Let $S = \mathbb{N}$ and $T = \mathbb{N}$. Define a relation $\mathcal{R}$ on S and T by the condition $(s, t) \in \mathcal{R}$ if $s^2 + t^2$ is itself a perfect square. Show

that the domain of $\mathcal{R}$ has infinitely many elements (Exercise 4.16 above may be of some help). Show that the image of $\mathcal{R}$ has infinitely many elements.

Chapter 5

Axioms of Set Theory, Paradoxes, and Rigor

5.1 Axioms of Set Theory

Exercises

1. Let S, T, U be finite sets. Prove that

$$\text{card}\Big[\big[S^T\big]^U\Big] = \text{card}\big[S^{T\times U}\big].$$

2. Let S, T, U be finite sets. Assume that $T \cap U = \emptyset$.

Prove that

$$\text{card}\left[S^T \times S^U\right] = \text{card}\left[S^{T\cup U}\right].$$

* **3.** What does our definition of the product of sets $\{S_\alpha\}_{\alpha\in A}$ have to do with the Axiom of Choice? Discuss.

4. Give examples of sets S, T, U, V such that $S \in T$, $T \in U$, $U \in V$. Use the ideas from Section 5.1 for inspiration.

* **5.** Explain why the axioms of set theory, as presented in Section 5.1, disallow the construction of the set in Russell's paradox.

6. Give an explicit well ordering of the rational numbers. Do not use the result of Section 5.2 about the total ordering of countable sets to answer this question. [**Hint:** Refer to Exercises 4.11, 4.12 for the notion of lexicographic ordering.]

7. Let S and T be well ordered sets. Specify a well ordering of the set $S \times T$.

8. A set can be a subset of itself, but it cannot be an element of itself. Explain the difference, and why this situation is logically acceptable.

9. Prove that there is no infinite set that has cardinality smaller than $\mathbb{N}$. Do *not* use Proposition 4.5.24.

10. Suppose that we were to add an axiom to the set theory described in Section 5.1 that said "If S and T are sets, then so is $S \cap T$". This would be redundant (that is, it would not be independent of the other axioms). Explain why.

11. Suppose that we were to add an axiom to the set theory described in Section 5.1 that said "If S and T are sets, then so is $S \setminus T$". This would be redundant (that is, it would not be independent of the other axioms). Explain why.

12. Suppose that we were to add an axiom to the set theory described in Section 5.1 that said "If S and T are sets, then so is $S \times T$". This would be redundant (that is, it would not be independent of the other axioms). Explain why.

13. In some developments of set theory, there is an Axiom of Pairing that is formulated as follows: let x and y be objects (either sets or set elements); then

$$\exists A \, \forall z, z \in A \Leftrightarrow (z = x \vee z = y).$$

Prove that the Axiom of Pairing is a corollary of the Power Set Axiom and the Axiom Schema of Replacement.

* **14.** In some developments of set theory, there is an Axiom Schema of Separation that is formulated as follows: Let $P(x)$ be a property of x. Let z be a set. Then

$$\exists y \, \forall x, x \in y \Leftrightarrow \big(x \in z \wedge P(x)\big).$$

This axiom is important, for it specifies that a new set can only be defined as a subset of a known set. Prove that the Axiom Schema of Separation is a corollary of the Axiom Schema of Replacement.

* **15.** In some developments of set theory, there is a Union Axiom that is formulated as follows: Let A and B be sets; then

$$\exists C \, \forall x, x \in C \Leftrightarrow \big(x \in A \vee x \in B\big).$$

Prove that the Union Axiom is a corollary of the Axiom of Extensionality, the Axiom of Pairing (Exercise 5.13), and the Sum Axiom.

16. If A is a set and $A \subset A \times A$, then prove that $A = \emptyset$.

17. The mathematician/philosopher Bertrand Russell liked to say that if you need to choose one sock from each of infinitely many pairs of socks, then you will need to use the Axiom of Choice. But for shoes you do not. Explain what Russell meant by these statements.

18. Prove that if $A \times B = \emptyset$, then either $A = \emptyset$ or $B = \emptyset$.

* **19.** Let S and T be sets. Prove that not both $S \in T$ and $T \in S$.

20. If $S \times T = T \times S$, then what does that tell you about the sets S and T?

21. If A, B, C are sets and $A \subset B$, then prove that $A \times C \subset B \times C$.

22. If $A = \mathcal{P}(A)$, then what can you conclude about A?

23. Let X be a finite set. Explain why 2^X is an appropriate, and commonly used, notation for the power set of X.

24. A standard proof of the method of mathematical induction begins in this way. Suppose that $P(j)$ is a statement, that $P(1)$ is true, and that $P(j) \Rightarrow P(j+1)$ for each j. Seeking a contradiction, assume now that it is *not the case* that $P(n)$ is true for every n. Let S be the set of all positive integers k such that $P(k)$ is false. Since $\mathbb{N}$ is well ordered, the set S has a least element. Complete the proof.

25. Explain why the methodology of Exercise 5.24 will not work to prove mathematical induction on the rationals or mathematical induction on the reals.

26. Give three distinct examples of partial orderings that are not total orderings.

27. Give three distinct examples of total orderings that are not well orderings.

28. Identify the type of each of the following orderings $\triangle$:

(a) S and T are sets; $S \triangle T$ if $S \supset T$.

(b) m and n are integers; $m \triangle n$ if $m + n > 5$.

(c) x and y are real numbers; $x \triangle y$ if $x \cdot y > 0$.

(d) S and T are sets; $S \triangle T$ if $S \in T$.

(e) z and w are real numbers; $z \triangle w$ if $z - w$ is a positive real number.

29. Let S be the collection of all sets that can be described in fewer than 50 words. Is S an element of itself? Why or why not? What does this example have to do with Russell's paradox? Do the axioms of set theory forbid this set?

Chapter 6

Number Systems

6.1 The Natural Number System

Exercises

1. Let S be a set and let $p : S \times S \to S$ be a binary operation. If $T \subset S$, then we say that T is *closed* under p if $p : T \times T \to T$. [As an example, let $S = \mathbb{Z}$ and T be the even integers and p be ordinary addition.]

Now let $S = \mathbb{R}$. Under which arithmetic operations $+, -, \cdot, \div$ is the set $T = \mathbb{Q}$ closed? Under which arithmetic operations $+, -, \cdot, \div$ is the set $T = \mathbb{R} \setminus \mathbb{Q}$ closed?

2. Imitate the construction of equivalence classes of $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, using $\mathbb{Q} \times (\mathbb{Q} \setminus \{0\})$ instead, as in Section 6.3. What sort of number system results? [**Hint:** Pick a useful representative from each equivalence class.]

3. Imitate the construction of equivalence classes of $\mathbb{N} \times \mathbb{N}$, using $\mathbb{Z} \times \mathbb{Z}$ instead, as in Section 6.2. What sort of number system results? [**Hint:** Pick a useful representative from each equivalence class.]

4. Let q be a rational number. Construct a sequence $\{x_j\}$ of irrational numbers such that $x_j \to q$. This means that, for each $\varepsilon > 0$, there is a positive integer K such that if $j > K$, then $|x_j - q| < \varepsilon$.

5. The numbers $\pi \approx 3.14159\ldots$ and $e \approx 2.71828\ldots$ are both known to be irrational (these assertions are quite difficult to prove). It is unknown

whether $x = \pi + e$ or $y = \pi - e$ is irrational. However at least one of these two numbers *must* be irrational. Can you explain why?

6. Let S be a set of real numbers with the property that, whenever $x, y \in S$ and $x < t < y$, then $t \in S$. Can you give a simple description of the set S?

7. Let $a_1 < a_2 < \cdots$ be real numbers. Prove that either there is a real number α such that $a_j \to \alpha$ (refer to Exercise 6.4 for this notation) *or else* the sequence $\{a_j\}$ increases without bound.

8. Let $\{a_j\}_{j=1}^{\infty}$ be a set of real numbers. Let $M > 0$ and assume that $|a_j| \leq M$ for every j. Prove that there is a subsequence $\{a_{j_k}\}$ and a real number x such that for every $\varepsilon > 0$ there is a $K > 0$ such that $|a_{j_k} - x| < \varepsilon$ whenever $k > K$. Refer to Exercises 6.4 and 6.7 for related ideas.

9. Prove that subtraction is well defined in the integers.

10. Prove that multiplication is well defined in the integers.

11. Give a careful discussion of the failure of the operation of division in the integers.

* **12.** If x is a positive real number, then let (x) denote its fractional part. For instance, $(3.2) = .2$, $(4/3) = 1/3$, etc.

Now fix an irrational number λ between 0 and 1. Let $a_k = (k\lambda)$. Then each a_k an element of $I = \{t : 0 \leq t < 1\}$. Prove the following: if $\varepsilon > 0$ and $x \in I$ then there is an element a_k such that $|a_k - x| < \varepsilon$. This is a famous result of Herman Weyl.

* **13.** Consider all sequences $\{a_1, a_2, \dots\}$ of rational numbers that satisfy the following condition: If $\varepsilon > 0$, then there exists an integer $N > 0$ such that if $j, k > N$ then $|a_j - a_k| < \varepsilon$. Such a sequence is called a *Cauchy sequence*.

Say that two Cauchy sequences $\{a_j\}$ and $\{a_j^*\}$ are related if, for any $\varepsilon > 0$, there is a positive integer N such that $j, k > N$ implies $|a_j - a_k^*| < \varepsilon$. Show that this is an equivalence relation. Explain why the set of all equivalence classes is, in a natural way, a model for the real numbers.

14. Prove that addition and subtraction are well defined in the rational number system $\mathbb{Q}$.

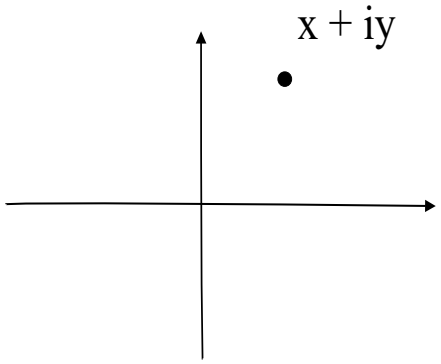

Figure 6.1: An Argand diagram.

15. Determine whether $\sqrt{2} + \sqrt{3}$ is rational or irrational.

* **16.** It is not necessary to discuss well definedness of addition and multiplication in the real number system. Explain why this is so.

17. It is not necessary to discuss well definedness of addition and multiplication in the complex number system. Explain why this is so.

18. Prove that every nonzero complex number $z \in \mathbb{C}$ has two distinct square roots in $\mathbb{C}$.

19. Prove that addition of integers is associative.

20. Assuming that it is known that addition of integers is both commutative and associative, prove then that addition of rational numbers is commutative and associative.

21. An Argand diagram is a device for sketching a complex number in the plane. If $x + iy$ is a complex number then we depict it in the cartesian plane as the point (x, y). See Figure 6.3. Sketch the complex numbers $3 - 2i$, $7 + 4i$, $e + \pi i$, $-6 - i$.

22. Consider the function $f(x) = 2^x$. What does it mean? When x is an integer the meaning is obvious. What about when x is a rational number? What can you say about $f(x)$ when x is an irrational number?

23. The complex number $1 = 1 + 0i$ has three cube roots. Use any means to find them, and sketch them on an Argand diagram (refer to Exercise 6.21 for terminology).

* **24.** Let θ be any real number. A famous formula of Euler asserts that

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

A rigorous verification of this formula requires a study of complex power series (see, for instance, [KRA1]). This exercise provides you with an intuitive argument that should make you comfortable with Euler's formula.

If z is *any* complex number, then define

$$e^z = \sum_{j=0}^{\infty} \frac{z^j}{j!}.$$

Notice that, when z happens to be a real number, then the formula is one that you learned in calculus. The new formula is a standard generalization of the calculus formula. Substitute in $i\theta$ for z and (manipulating the series just as though it were a polynomial) separate the right-hand side into its real and imaginary parts. The result is

$$e^{i\theta} = \left(1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} - + \cdots\right) + i\left(\theta - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} - + \cdots\right).$$

Finally, notice that the power series expansions in the parentheses on the right are those associated with the functions cosine and sine, respectively. This is Euler's formula.

25. Refer to Exercise 6.24. If $\xi = s + it$ is any complex number such that $s^2 + t^2 = 1$, then we may find an angle θ, $0 \leq \theta < 2\pi$, such that $\cos\theta = s$ and $\sin\theta = t$. See Figure 6.4. We conclude that

$$\xi = e^{i\theta}.$$

Explain this reasoning in detail.

26. If $z = x + iy \in \mathbb{C}$ is any nonzero complex number, then let

$$r^2 = |z|^2 = x^2 + y^2.$$

The number r is the distance of z to the origin in the Argand plane (Exercise 6.21). It is also the modulus of z. Set $\xi = z/r$. Show that $|\xi| = 1$. Now apply Exercise 6.25 to conclude that

$$z = r\, e^{i\theta},$$

some $0 \leq \theta < 2\pi$. This is called the *polar form* of the complex number z.

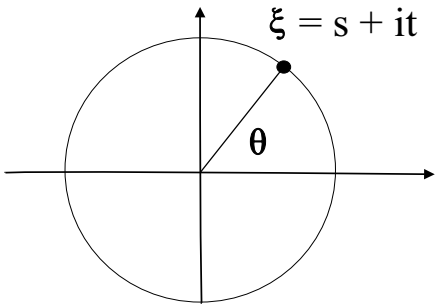

Figure 6.2: The angle associated to a complex number of modulus 1.

27. If $z = re^{i\theta}$ is a complex number in polar form, then $re^{i(\theta+2\pi)}$ is the same complex number (refer to Exercises 6.24, 6.25, 6.26). Explain.

28. Let z be any nonzero complex number, and let k be an integer exceeding 1. In this exercise we learn to find all the k^{th} roots of z. There will be k of them.

First we solve the equation

$$w^k = z = re^{i\theta},$$

where we have written z in the polar form $z = re^{i\theta}$ (refer to Exercises 6.24, 6.25, 6.26, 6.27). If $w = se^{i\psi}$, then we see that $s = r^{1/k}$ and that $\psi = \theta/k$.

But we may also solve the equation

$$w^k = z = r^{i(\theta+2\pi)}$$

to find a second k^{th} root with $s = r^{1/k}$ and $\psi = \theta/k + 2\pi/k$ (refer to Exercise 6.27).

Continue this procedure to find $(k-2)$ more k^{th} roots of z.

Apply the procedure developed here to find all sixth roots of 2. Sketch all six roots, together with the number $2 = 2 + 0i$, on an Argand diagram.

29. Apply the ideas developed in Exercise 6.28 to find all fourth roots of the complex number $1 + i$. Sketch all the roots, together with the number $1 + i$, on an Argand diagram.

30. Apply the ideas developed in Exercise 6.28 to find all sixth roots of the complex number $2 - 3i$. Sketch all the roots, together with the number $2 - 3i$, on an Argand diagram.

31. Apply the ideas developed in Exercise 6.28 to find all third roots of the complex number $-i$. Sketch all the roots, together with the number $-i$, on an Argand diagram.

32. The mapping

$$x + iy \mapsto x + yi + 0j + 0k$$

shows that the complex numbers form a natural algebraic sub-object inside the quaternions. Explain this statement.

33. Prove that the complex numbers cannot be made into an ordered field (as discussed in Section 6.7).

* **34.** Discuss the relationship between well ordering and the Axiom of Regularity (begin by considering the natural numbers).

35. Prove those parts of Theorem 6.3.6 that were not proved in the text.

36. Prove those parts of Theorem 6.3.9 that were not proved in the text.

37. Complete the calculation in the proof of Theorem 6.4.8.

38. Prove the generalization of Theorem 6.4.8 that is stated after the proof of that theorem.

39. Prove that addition and multiplication are commutative in the complex number system.

40. Prove that multiplication distributes over addition in the complex number system.

41. Exhibit two distinct ways in which the complex numbers may be viewed as a subfield of the quaternions.

42. In how many different ways can the real numbers be exhibited as a subfield of the quaternions?

43. Let z be an element of the quaternions. If $z = z_1 \cdot \mathbf{1} + z_2\mathbf{i} + z_3\mathbf{j} + z_4\mathbf{k}$, then define $\overline{z} = z_1 \cdot \mathbf{1} - z_2\mathbf{i} - z_3\mathbf{j} - z_4\mathbf{k}$. Calculate $z \cdot \overline{z}$. In what sense is this bar operation analogous to conjugation in the complex number system?

44. Let $\mathcal{M}_{n\times n}$ denote the set of $n \times n$ matrices with real entries, equipped with the usual matrix addition and multiplication. Explain why $\mathcal{M}_{n\times n}$ does not form a field when equipped with standard matrix addition and multiplication.

45. Let p be a polynomial and assume that $\alpha \in \mathbb{C}$ is a root of p. Prove that $(z - \alpha)$ evenly divides $p(z)$ with no remainder.

46. One of the most crucial properties of the complex number system is enunciated by the Fundamental Theorem of Algebra. This theorem states that if $p(z)$ is a polynomial of degree at least one, then p has a root in the complex number field. That is, there is a number $\alpha \in \mathbb{C}$ such that $p(\alpha) = 0$.

Assume the Fundamental Theorem of Algebra for the moment. Use the result of Exercise 6.45 to show that if $p(z)$ is a polynomial of degree $k \geq 1$, then p has k roots (possibly not all distinct).

* **47.** Here is a sketch of a proof of the Fundamental Theorem of Algebra (Exercise 6.46). Fill in as many details of the proof as you can. Do not be afraid to consult your instructor for help.

(a) Let $p(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_k z^k$ be the polynomial under consideration. We are assuming that $k \geq 1$.

(b) If $a_0 = 0$ then 0 is a root of the polynomial (why?). So we may as well only consider the case in which $a_0 \neq 0$.

(c) Fix a positive number R and let C_R denote the circle in the complex plane with center at the origin and radius R. Let us consider the image of C_R under the polynomial p (think of p as a mapping from $\mathbb{C}$ to $\mathbb{C}$).

(d) If R is very large then we can study the situation in part (c) by writing the polynomial as

$$p(z) = z^k \cdot \left(a_k + a_{k-1}\frac{1}{z} + \cdots + a_1 \frac{1}{z^{k-1}} + a_0 \frac{1}{z^k} \right).$$

When $z \in C_R$ and $R > 0$ is very large, then each of the terms in parentheses, except for the first, is very small. Thus, for such z, the expression $p(z)$ is approximately equal to $z^k \cdot a_k$. The image of C_R under this last expression is a large circle that surrounds the origin.

(e) If R is very small, then (returning to the original expression for $p(z)$) the quantity $p(z)$ approximately equals $a_0 \neq 0$—for the other terms in the polynomial will be small too. Thus the image of C_R under the mapping p will be some small curve near the point $a_0 \neq 0$. In particular, if R is small enough, then this small curve *will not* surround the origin.

(f) We see from parts (d) and (e) that when R is small, then the image of C_R under p is a curve that *does not* surround the origin; but if R is large, then the image of C_R under p is a curve that *does* surround the origin.

(g) It follows from continuity considerations that there must be an intermediate value of R (refer to part (f)) such that the image of C_R under p is a curve that passes through the origin. In other words, for that special value of R, there is a point z_0 on the curve C_R such that $p(z_0) = 0$. But then z_0 is the root that we seek.

48. The Division Algorithm states that, if p, q are positive integers with $p < q$, then we may write $q = p \cdot k + s$, where k is a positive integer and $s < p$. This is just the familiar algorithm of division that we learn in grade school: You can divide p into q as many times as it will go, and the remainder will be smaller than p. There is also a version of the division algorithm for division of polynomials. Formulate such a result.

Combine the Division Algorithm for polynomials with the Fundamental Theorem of Algebra to learn about the factorization of polynomials. Proceed as follows. Suppose that $p(z)$ is a polynomial of degree at least 1 and that r_1 is a root of p, as guaranteed by the Fundamental Theorem of Algebra. Divide $p(z)$ by $z - r_1$. Then there will be some quotient $p_1(z)$ and some remainder $s(z)$. Show that in fact s must be zero. So

$$p(z) = (z - r_1) \cdot p_1(z) \, .$$

Now if the degree of p_1 is at least one, then we may again apply the Fundamental Theorem of Algebra to find a root r_2. Divide $p_1(z)$ by $z - r_2$. The result, as before (using the division algorithm for polynomials) is that

$$p_1(z) = (z - r_2) \cdot p_2(z)$$

for some polynomial p_2, hence

$$p(z) = (z - r_1) \cdot (z - r_2) \cdot p_2(z) \, .$$

Continuing in this manner, we ultimately come up with a factorization

$$p(z) = c_0 \cdot (z - r_1) \cdot (z - r_2) \cdots (z - r_k) \, ,$$

where c_0 is a constant and k is the degree of the original polynomial p.

49. Prove parts (2), (3), (4) of Proposition 6.6.7.

50. Prove parts (1), (2), (3) of Proposition 6.6.8.

51. Refer to Exercise 6.48 for a discussion of the Division Algorithm. Use the Division Algorithm to generate a method for finding the greatest common divisor of two positive integers m and n.

* **52.** Prove that there is a real number $m > 0$ with the following property: Let $a_1, a_2, \ldots, a_k$ be complex numbers. Then there is a subcollection $a_{j_1}, a_{j_2}, \ldots, a_{j_p}$ such that

$$\left| a_{j_1} + a_{j_2} + \cdots + a_{j_p} \right| \geq m \cdot \left[|a_1| + |a_2| + \cdots |a_k| \right] \, .$$

[**Hint:** First consider the case $k = 2$.]

53. Refer to Exercises 6.24, 6.25, 6.26. Produce an explicit complex number z such that $e^z = i$. Produce an explicit complex number w such that $e^w = -i$.

Chapter 7

More on the Real Number System

Exercises

1. Let $0 < \eta < 1$. Modify the construction of the Cantor ternary function to obtain a set $C_\eta \subset [0,1]$ with the property that $[0,1] \setminus C_\eta$ is a union of intervals the sum of whose lengths is η.

2. Verify that if $x_1 < x_2$ are elements of the Cantor set, then there is a number t that is strictly between x_1 and x_2 and such that t does not lie in the Cantor set.

3. Prove that the collection of endpoints of the removed open intervals in the Cantor set construction is countable. Such points have addresses with only finitely many 1s. Thus most elements of the Cantor set are not endpoints, but are points with addresses that have infinitely many nonzero entries.

* **4.** A subset of $\mathbb{R}$ is said to be *perfect* if it is closed and bounded and every element of the set is a limit point of the set. Prove that the Cantor set is perfect. [*Remark:* It is an advanced theorem that a perfect set must perforce be uncountable. This gives another proof of the uncountability of the Cantor set.]

5. Let $S \subset \mathbb{R}$. A point $s \in S$ is said to be an *interior* point if there exists a number $\epsilon > 0$ such that $(s-\epsilon, s+\epsilon) \subset S$. The interior of S is just the collection of all interior points. Prove that the interior of S is an open set.

6. Let $S \subset \mathbb{R}$. A point $s \in \mathbb{R}$ is said to be a *boundary point* of S if, for each $\epsilon > 0$, we have both $(s-\epsilon, s+\epsilon) \cap S \neq \emptyset$ and $(s-\epsilon, s+\epsilon) \cap {}^cS \neq \emptyset$.

The boundary of S is just the collection of all boundary points. Prove that the boundary of S is closed.

7. Refer to the last two exercises for terminology. Let $S \subset \mathbb{R}$ be any closed subset. Prove that S is the union of its interior and its boundary.

8. Let $\{x_j\}$ be a sequence of real numbers. Prove that the sequence $\{x_j\}$ converges to α if and only if every subsequence has itself a subsequence that converges to α.

9. A set $S \subset \mathbb{R}$ is said to be *discrete* if, for each point $s \in S$, there is a number $\epsilon > 0$ such that $(s - \epsilon, s + \epsilon) \cap S = \{s\}$. Is the set $\mathbb{Q}$ of rational numbers discrete? Is the Cantor set discrete? Is the set $\mathbb{Z}$ of integers discrete? Define

$$T = \{1, 1/2, 1/3, \dots\}.$$

Is T discrete?

* **10.** Refer to Exercise 7.4 for the definition of perfect set. Prove that every compact set K is the union of a perfect set and a countable set. [**Hint:** Define x to be a *consolidation point* of K if each open interval about x contains uncountably many points of K. Let the perfect set consist of the set of consolidation points.]

11. Let $s_1 \leq s_2 \leq s_3 \cdots$ be real numbers. Prove that either the sequence $\{s_j\}$ converges or else it is unbounded.

12. A set $W \subset \mathbb{R}$ is said to be *dense* in $\mathbb{R}$ if, for each $x \in \mathbb{R}$ and each $\epsilon > 0$, the interval $(x - \epsilon, x + \epsilon)$ contains an element of W. Prove that the set of irrational numbers is dense in $\mathbb{R}$. Give an example of a sequence that is dense in $\mathbb{R}$.

13. Let $S \subset \mathbb{R}$ be any set. Let L be the set of limit points of S. Prove that L is closed.

14. Let $S \subset \mathbb{R}$ be any set. The *closure* of S is defined to be the union of S with all its limit points (see Exercise 7.13). Prove that the closure of S is a closed set. What is the closure of $\mathbb{Q}$? What is the closure of $\mathbb{Z}$?

15. Refer to Exercises 7.5, 7.6, and 7.14 for terminology. Let $S \subset \mathbb{R}$ be any closed set, let $\mathcal{O}$ be its interior, and let $\mathcal{C}$ be its closure. Prove that $\mathcal{C} \setminus \mathcal{O}$ is just the boundary of S.

16. Let $U \subset \mathbb{R}$ be any open set. Prove that U can be written as the countable disjoint union of open intervals. [**Hint:** The intervals will be the equivalence classes under a suitable equivalence relation.]

17. Refer to the last exercise. Let $E \subset \mathbb{R}$ be any closed set. Prove that there is a continuous function ϕ with domain $\mathbb{R}$ such that $\phi \geq 0$ and $Z = \{x \in \mathbb{R} : \phi(x) = 0\} = E$.

* **18.** Let $S \subset \mathbb{R}$ be any set. We say that S is *disconnected* if there are open sets U and V with $U \cap V = \emptyset$ such that $U \cap S \neq \emptyset$, $V \cap S \neq \emptyset$, and

$$S = [U \cap S] \cup [V \cap S] .$$

If S is not disconnected, then we say that S is *connected*. Prove that $\mathbb{R}$ is connected. Prove that any interval is connected. Prove that $\mathbb{Q}$ is disconnected. Prove that the Cantor set is disconnected.

19. Refer to Exercise 7.14 for terminology. Let $\{x_j\}$ be any sequence in $\mathbb{R}$. Let X be the closure of $\{x_j\}$. How many points can $X \setminus \{x_j\}$ have in it? One? Finitely many? Infinitely many? Uncountably many?

20. Refer to Exercise 7.5 for terminology. What is the interior of $\mathbb{Q}$? What is the interior of $\mathbb{R}$? What is the interior of the Cantor set?

21. Let $\mathcal{O}_1, \mathcal{O}_2, \ldots$ be open sets. Define $\mathcal{O} = \cup_j \mathcal{O}_j$. Is $\mathcal{O}$ open? Define $\mathcal{T} = \cap_j \mathcal{O}_j$. Is T open?

Let $\mathcal{E}_1, \mathcal{E}_2, \ldots$ be closed sets. Define $\mathcal{E} = \cup_j \mathcal{E}_j$. Is $\mathcal{E}$ closed? Define $\mathcal{F} = \cap_j \mathcal{E}_j$. Is $\mathcal{F}$ closed?

22. Refer to the last exercise. For the assertions that are false, show that if one restricts attention to finite collections of sets, then they become true.

23. Give a characterization of the open subsets of $\mathbb{R}$ using the language of sequences.

24. Give a characterization of the closed subsets of $\mathbb{R}$ using the language of neighborhoods.

25. Let S be an uncountable subset of $\mathbb{R}$. Show that S must have a limit point. That is, there is a point $s \in \mathbb{R}$ and a sequence $\{s_j\} \subset S$ with $s_j \neq s$ for all j such that $\lim_{j \to \infty} s_j = s$. Prove that if S has only countably many points, then the conclusion fails.

26. Let $\mathcal{O}$ be an open subset of $\mathbb{R}$. Prove that $\mathcal{O}$ can be written as the countable increasing union of closed sets.

27. Let E be a closed subset of $\mathbb{R}$. Prove that E can be written as the countable decreasing intersection of open sets.

28. Explain why the words "closed" and "open" may not be switched in Exercise 26. Explain why the words "closed" and "open" may not be switched in Exercise 27.

* **29.** Define "open set" in $\mathbb{R}^2$. Prove that the product of open sets in $\mathbb{R}^1$ is open.

* **30.** Define "closed set" in $\mathbb{R}^2$. Prove that the product of closed sets in $\mathbb{R}^1$ is closed.

Chapter 8

A Glimpse of Topology

Exercises

1. Let X be the interval $[1, 5]$ and define

$$\mathcal{U} = \{[1, 4], [3, 5], [3, 4], [1, 5], \emptyset\} \ .$$

Explain why $\mathcal{U}$ is a topology on X.

2. Let X be the real numbers. Let a subset of X be open if it consists of irrational numbers only, or if it is all of X, or if it is the empty set. Explain why these open sets form a topology on X.

3. Declare a collection of polynomials in the variable x with real coefficients to be open if the set of all their coefficients forms an open set in $\mathbb{R}$ according to Example 8.2.1. As an instance, the set of polynomials $a + bx + cx^2$ with $a, b, c \in (0, 1)$ is an open set of polynomials. Verify that these open sets form a topology on the collection of all real-coefficient polynomials of a single variable.

4. Declare a set in $\mathbb{Z}$ to be open if it is finite. Verify that these open sets do *not* form a topology. What happens if the word "finite" is replaced by "infinite"?

5. Let $X = \{a, b\}$ be a set with just two points. Describe all possible topologies on X.

6. Show that if a finite topological space is $\mathbf{T}_1$, then it must be discrete.

7. Let (X, d) be a metric space. This means that d measures distance in X. It has these properties:

(a) $d(x, y) \geq 0$ for all $x, y \in X$;

(b) $d(x, y) = 0$ if and only if $x = y$;

(c) $d(x, y) = d(y, x)$ for all $x, y \in X$;

(d) $d(x, y) \leq d(x, z) + d(z, y)$ for all $x, y, z \in X$.

Of course we can use d to define balls in X. These balls will generate a topology (by taking arbitary union and finite intersection).

Let $E \subset X$ be a closed set. Define

$$\rho(x) = \inf\{d(x, e) : e \in E\}.$$

This function ρ measures the *distance* of x to E. Show that ρ is continuous. Indeed it is Lipschitz continuous, which means that there is a positive constant A such that $|\rho(x) - \rho(y)| \leq Ad(x, y)$ for all $x, y \in X$.

8. Let $(X, \mathcal{U})$ be a topological space. A set $S \subset X$ is said to be *dense* if, for every point $x \in X$ and every neighborhood U of x, there is a point $s \in S$ that lies in U. Show that the polynomials are a dense subset of the continuous functions on $[0, 1]$ (equipped with the topology generated by sets of the form $\mathcal{E}_{g,\epsilon} \equiv \{f \text{ continuous on } [0, 1] : \max_{x\in[0,1]} |f(x) - g(x)| < \epsilon\}$). Show that the rational numbers $\mathbb{Q}$ are dense in the reals $\mathbb{R}$. Show that the integers $\mathbb{Z}$ are *not* dense in the reals $\mathbb{R}$.

9. Prove that a set E in a topological space X is open if and only if E contains none of its boundary points.

10. Prove that a set E in a topological space X is open if and only if E equals its interior.

11. Let (X, d) be a metric space (refer to Exercise 8.7 for terminology). Let $K \subset X$ be compact and $E \subset X$ be closed and disjoint from K. Show that there is a positive distance between K and E. That is to say, there is a number $\epsilon > 0$ such that if $k \in K$ and $e \in E$, then $d(k, e) > \epsilon$.

12. Show that the result of the last exercise is false if the two sets are assumed only to be closed.

13. Declare a set in $\mathbb{R}$ to be open if it is the empty set or if its complement is an interval $[a, b]$ or the empty set. Does this collection of sets form a topology?

14. Let X be the space of sequences $\{a_j\}$ of real numbers such that $\sum_j |a_j|^2$ is finite. Define a metric (refer to Exercise 8.7 for terminology) on this space by

$$d(\{a_j\}, \{b_j\}) = \left[\sum_j (a_j - b_j)^2\right]^{1/2}.$$

Show that this is a metric. Explain why the closed unit ball

$$B = \left\{\{a_j\} : \sum_j a_j^2 \leq 1\right\}$$

is not compact. It is nonetheless the case that B is closed and bounded.

* **15.** Give an example of a compact set in a non-Hausdorff space that is not closed.

16. Let X be the real numbers and declare that every singleton set $\{x\}$ is open. Generate a topology with these sets. Now describe all the open sets. Which sets are closed? Which sets are compact?

17. Let $f : X \to Y$ be a continuous mapping of topological spaces and let $K \subset Y$ be compact. Is it necessarily the case that $f^{-1}(K)$ is compact? Give a proof or a counterexample.

18. Let $X = \{A, B, C, D, E\}$. Describe two distinct topologies on X that are not homeomorphic. [Here two topologies $(X, \mathcal{U})$ and $(X, \mathcal{V})$ are *homeomorphic* if there is a one-to-one, onto, bicontinuous mapping $\Phi : (X, \mathcal{U}) \to (X, \mathcal{V})$.]

19. Think of the space in Exercise 8.14 as a vector space. Show that it does not have a basis consisting of finitely many elements.

20. Let B be the closed unit ball defined in Exercise 8.14. Calculate its interior.

21. Let the topological space X be $\mathbb{R}^2$ equipped with the usual Euclidean topology. Let S be the points that have both integer coordinates. Calculate the closure of S. Calculate the interior of S. Calculate the boundary of S.

22. Let the topological space X be the real line $\mathbb{R}$. An open set is any set whose complement is finite (together with the empty set and the whole space). Let $S = [0, 1]$. Calculate the closure of S. Calculate the interior of S. Calculate the boundary of S.

23. Put a topology on $\mathbb{R}^2$ with the property that the line $\{(x, 0) : x \in \mathbb{R}\}$ is dense in $\mathbb{R}^2$.

24. Define a new Cantor set with the property that the first set removed has length 3^{-10}, the next two sets removed have lengths 3^{-10^2}, the next four sets removed have lengths 3^{-10^4}, and so forth. The resulting set will still be nonempty, compact, and have uncountably many elements. Prove these statements. What will be the length of this new set?

* **25.** Prove that, in $\mathbb{R}^N$, any connected open set is path-connected. That is to say, prove that any two points can be connected by a continuous path.

26. Describe a topology on the real line which will make the interval $(0, 1)$ compact.

27. Describe a topology on $\mathbb{R}^2$ which will make all sets compact.

28. Give an example of a countable, connected Hausdorff space.

29. Let X be the metric space consisting of the continuous functions on the interval $[0, 1]$ equipped with the metric of uniform distance (refer to Exercise 8.8 for this metric). Let $S \subset X$ consist of those functions f that are continuously differentiable and satisfy $|f(x)| \leq 1$ and $|f'(x)| \leq 1$ for every x. Show that every sequence in S has a convergent subsequence.

30. Is the finite union of compact sets compact? How about the finite intersection of compact sets in a Hausdorff space?

31. The set $[0, 1] \subset \mathbb{R}$ is compact if $\mathbb{R}$ is equipped with the usual topology. We see that $\mathcal{W} = \{(1/j, 1 - 1/j)\}_{j=2}^{\infty} \cup \{(-1/4, 1/4), (5/6, 7/6)\}$ is an open cover of $[0, 1]$. Describe explicitly a finite subcover.

32. The following is a theorem of Lebesgue. Let $K \subset \mathbb{R}$ be a compact set and $\mathcal{W}$ an open cover of K. Then there is a $\delta > 0$ so that any ball with center in K and radius δ will be entirely contained in some element of the cover $\mathcal{W}$. Prove Lebesgue's theorem.

33. Let us work in the real numbers with the usual topology. Let E be the interval $[0, 1]$, and let F be the interval $[3, 4]$. Construct explicitly the function f specified by Urysohn's theorem.

34. Let E be any closed set in $\mathbb{R}$. Prove that there exists a continuous, real-valued function f such that

$$\{x \in \mathbb{R} : f(x) = 0\} = E\,.$$

35. Prove that the closure $\overline{S}$ of any set S in a topological space is in fact closed.

Chapter 9

Elementary Number Theory

EXERCISES

1. Calculate gcd$(455, 1235)$.

2. Use the sieve of Eratosthenes to make a list of all primes up to 100.

3. Prove that there are infinitely many primes of the form $6x - 1$.

* **4.** Let $\psi(x)$ be the number of primes of the form $4x - 1$ that are $\leq x$. Use a computer to make a conjectural guess about the limit as $x \to \infty$ of $\psi(x)/\pi(x)$.

5. Let a, b, c, n be integers. Prove that

(a) If $a|n$ and $b|n$ with gcd$(a, b) = 1$, then $ab|n$.

(b) If $a|bc$ and gcd$(a, b) = 1$, then $a|c$.

6. Let a, b, c, d, m be integers. Prove that

(a) If $a|b$ and $b|c$, then $a|c$.

(b) If $a|b$ and $c|d$, then $ac|bd$.

(c) If $m \neq 0$, then $a|b$ if and only if $ma|mb$.

(d) If $d|a$ and $a \neq 0$, then $|d| \leq |a|$.

7. For each of the following, apply the Division Algorithm to find q and r such that $a = bq + r$ and $0 \leq r < |b|$.

(a) $a = 300$, $b = 17$

(b) $a = 729$, $b = 31$

(c) $a = 300$, $b = -17$

(d) $a = 389$, $b = 4$

8. Suppose that a, b, n are positive integers. Prove that if $a^n | b^n$, then $a | b$.

9. Prove that, if a positive integer n is a perfect square, then n cannot be written in the form $4k + 3$ for k an integer. [**Hint:** Computer the remainder upon division by 4 of each of $(4m)^2$, $(4m + 1)^2$, $(4m + 2)^2$, $(4m + 3)^2$.]

10. Prove that no integer in the sequence

$$11\ ,\ 111\ ,\ 1111\ ,\ 11111\ ,\ 111111\ ,\ \ldots$$

is a perfect square. [**Hint:** $111 \cdots 111 = 111 \cdots 108 + 3 = 4k + 3$.]

11. Prove that, for any positive integer n, the set $[\mathbb{Z}/n\mathbb{Z}]^*$ (the integers modulo n which are relatively prime to n) with the binary operation of multiplication is a group.

12. Compute the following gcds.

(a) $\gcd(15, 5)$

(b) $\gcd(247, 299)$

(c) $\gcd(51, 897)$

(d) $\gcd(136, 304)$

13. Find $x, y \in \mathbb{Z}$ such that $121x + 55y = 11$.

14. Prove that, if a and b are integers and p is a prime, then $(a + b)^p = a^p + b^p \mod p$. [**Hint:** Of course you may assume that the binomial coefficient $\binom{n}{k}$ is an integer.]

15. Prove that if x, y is a solution of the equation $ax + by = d$ with $d = \gcd(a, b)$, then, for all $c \in \mathbb{Z}$,

$$x' = x + c \cdot \frac{b}{d} \quad , \quad y' = y - c \cdot \frac{a}{d} \qquad (*)$$

is also a solution of $ax + by = d$.

16. Refer to Exercise 15. Find the solution to $51x + 119y = 17$.

17. Prove that a number $n \in \mathbb{Z}$ is divisible by 3 if and only if the sum of the digits of n is divisible by 3.

* **18.** With reference to the Chinese Remainder Theorem, find a positive integer n that satisfies these congruences:

$$\begin{aligned} n &= 3 \mod 17 \\ n &= 2 \mod 23 \\ n &= 5 \mod 11 \\ n &= 19 \mod 37 \end{aligned}$$

* **19.** Let $f(x) = x^2 + ax + b$ be a quadratic polynomial with integer coefficients. For example, f could be $f(x) = x^2 - 7x + 5$. Formulate a conjecture about when the set

$$S = \{f(n) : n \in \mathbb{Z} \text{ and } f(n) \text{ is prime}\}$$

is infinite. Give numerical evidence (perhaps using a computer) to support your conjecture.

20. Find an integer n so that $37n = 1 \mod 101$.

21. Let p be a prime. Prove that $\mathbb{Z}/p\mathbb{Z}$ (the integers modulo p) is a field.

22. Show that, if n is a positive integer so that n and $n^2 + 2$ are prime then $n = 3$.

23. Let S be the set $\mathbb{Z}/5\mathbb{Z}$ (the integers modulo 5) with binary operation multiplication. Is this a group?

24. Find all four solutions of the equation

$$x^2 - 1 = 0 \mod 35\,.$$

25. Compute the last digit of 3^{45}.

* **26.** For $n \in \mathbb{N}$, let $\sigma(n)$ denote the sume of the divisors of n. For example, $\sigma(6) = 1 + 2 + 3 + 6 = 12$ and $\sigma(10) = 1 + 2 + 5 + 10 = 18$. Assume that $n = pqr$, with p, q, r distinct primes. Devise an algorithm that uses n, $\varphi(n)$, and $\sigma(n)$ to determine the prime factorization of n.

As an example of what we are asking, let $n = 105$. Then $p = 3$, $q = 5$, $r = 7$. So the input to the requested algorithm would be

$$n = 105 \ , \ \varphi(n) = 48 \ , \ \sigma(n) = 192 \, .$$

And the output would be $3, 5, 7$.

Chapter 10

Zero-Knowledge Proofs and Cryptography

Exercises

1. Perform an RSA encryption of the message

The Beatles forever.

using $n = 34161 = 177 \times 193$ and $e = 5^2 \times 7^2$.

2. Use the RSA method to *decrypt* the encoded message that you created in Exercise 12.1. Verify that the decrypted message is "The Beatles forever."

3. Devise a method for convincing a remote verifier that you can decrypt a certain message, without revealing to him/her what the decrypted message is.

4. Prove that the RSA encryption of the product of two messages is equal to the product of the encryptions of the individual messages. This fact can sometimes be used to speed up the breaking of RSA code.

5. Is there any value in performing RSA encryption twice? That is to say, take a message, RSA-encrypt it, and then RSA-encrypt that encrypted message.

6. The way we have described RSA encryption, it is entirely possible for someone to pretend to be you, encrypt a message, and send it to your collaborator. They would simply use the same encoding information (e and n) that

you use. What device could you use so that someone receiving an RSA-encrypted message that purports to be from you *really is* from you?

7. The ciphertext

> QBB JXU MEHBT YI Q IJQWU QDT QBB JXU CUD QDT MECUD CUHUBO FBQOUHI

has been generated by an advanced Caesar cipher with shift 16 (i.e., "A" is mapped to "Q", etc.). Decrypt it.

* **8.** The Greek Polybius ($\sim$200–118 B.C.E.) invented a monoalphabetic cipher that converts alphabetical characters into numerical characters. It is based on a checkerboard:

#	**1**	**2**	**3**	**4**	**5**
1	a	b	c	d	e
2	f	g	h	ij	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

We associate to each letter of the alphabet a two-digit number by looking at the row and column that it appears in. For example, k is associated to 25 and t is associated to 44.

Use the Polybius checkerboard to encrypt the message.

> God is in the details.

9. The Playfair Cipher replaces single letters with digraphs in an interesting manner. We begin with a keyword, say TURKEY. Then we create a 5×5 matrix by beginning with the key word and then filling in all the other letters in order (and we combine I and J). The result is

T	U	R	K	E
Y	A	B	C	D
F	G	H	I/J	L
M	N	O	P	Q
S	V	W	X	Z

The message is now broken up into pairs of letters (called *digraphs*), where an X is inserted between identical letters and also at the end of the message if necessary (to make an even number of letters).

Suppose that the message is

THE DAY IS SUNNY.

Then the digraph decomposition is

TH ED AY IS XS UN NY

Now all digraphs fall into one of three categories: **(i)** both letters in the same row, **(ii)** both letters in the same column, **(iii)** neither. We treat these as follows:

(a) If both letters are in the same row, then each is replaced by the letter to its right in the matrix. But if one of the letters occurs in the last position of the row, then it is replaced by the the letter at the beginning of the row. So, for example, BR becomes IU.

(b) If both letters are in the same column, then each is replaced by the letter beneath it in the matrix. But if one of the letters is at the bottom of the column, then it is replaced by the letter at the top of the column. So, for instance, RS becomes YL.

(c) If the letters in a digraph are neither in the same row nor in the same column, then we follow these rules:

(i) To encipher the first letter, look along its row until you reach the column containing the second letter. The letter at the intersection is the one that you use as the replacement.

(ii) To encipher the second letter, look along its row until you find the column containing the first letter; the letter at this intersection then is the replacement for the second letter.

Use this technique to encrypt the message enunciated above.

10. Does RSA encryption work if p and q are not prime?

11. Use the Division Algorithm to find the greatest common divisor of 248 and 164.

12. Use the Division Algorithm to find integers x and y so that

$$27x + 64y = 1\,.$$

13. Suppose you are person A, and you have chosen as your two primes $p = 97$ and $q = 173$, and you have chosen $e = 5$. Thus you told B that $n = 16781$ (which is just pq) and you told him that $e = 5$. He encodes a message (a number) for you and tells you that the encoding is 5347. Can you figure out the original message?

14. We know from the text that Fermat's little theorem says this:

> **Theorem:** If p is a prime integer and $1 \leq a < p$ is another integer, then
>
> $$a^{p-1} \equiv 1 \bmod p\,. \qquad (*)$$

If we are given a positive integer p, and we want to test whether p is prime, we can just pick an integer a from the interval $[1, p-1]$ at random and see whether $(*)$ holds. If the equality fails for some particular value of a, then we may definitely conclude that p is composite. If the equality holds for some particular value of a, then we can say that p is "probably" prime.

Test the integer 13 for primality, using $a = 4$ and $a = 5$.

15. Refer to Exercise 12.14 for terminology. Apply the Fermat test to the number 14 to test for primality. Use three different values for a.

16. The Chinese Remainder Theorem (see Exercises 12.19 and 12.20) says that there is an integer with residue 1 modulo 2, residue 2 modulo 3, and residue 3 modulo 5. Find it.

17. If p is a prime and q is a distinct prime, them $p^2 - q^2$ will never be prime. But $p^2 + q^2$ could be prime. Explain.

18. Do a `Google` search to learn what are the most commonly used letters in the roman alphabet in the English language. What are the most commonly used digraphs in the roman alphabet in the English language? How can one use this information in cryptography?

19. The most classical version of the Chinese remainder theorem says that, if $p_1, \ldots, p_k$ are distinct primes and $a_1, a_2, \ldots, a_k$ are positive integers, then there exists a solution x to the simultaneous equations

$$x = a_j \bmod p_j\,, \quad j = 1, \ldots, k\,.$$

Find a constructive proof of this result.

20. A version of the Chinese Remainder Theorem says this:

> Let p and q be two numbers (not necessarily primes), but which are relatively prime. Then, if $a = b \bmod p$ and $a = b \bmod q$, we may conclude that $a = b \bmod pq$.

Prove this theorem.

Chapter 11

Examples of Axiomatic Theories

11.1 Group Theory

Exercises

1. If G and H are groups, then describe how to put a group structure on $G \times H$. If G and H are abelian then is $G \times H$ abelian?

2. The groups $G = \mathbb{Z}_4$ and $H = \mathbb{Z}_2 \times \mathbb{Z}_2$ are both groups of order 4. But they are not the same group. That is, they are not isomorphic. Give a proof of this last statement.

3. Describe all possible groups of order 2.

4. Describe all possible groups of order 3.

5. Describe all possible groups of order 4.

6. Independent of having a model for non-Euclidean geometry, we could consider a (theoretical) geometry based on Euclid's axioms **P1**–**P4** and a fifth axiom that says:

> **Q5** There exists a line ℓ and a point P not on the line such that at least two distinct lines parallel to ℓ pass through P.

Show that, in this geometry, there is a triangle the sum of whose angles is less than 180°.

7. Notice that **Q5** in the last exercise is precisely the negation of the parallel postulate **P5** in the text. But we might ask if it then follows logically that for *every* line m and *every* point S not on m there are at least two distinct lines through S that are parallel to m. Prove that this is so.

8. Refer to Exercises 11.6 and 11.7. Prove that non-Euclidean geometry contains no rectangles.

9. Let G be a group and H a subgroup. We say that H is *normal* if, whenever $g \in G$ and $h \in H$, then $g^{-1}hg \in H$. Prove that, when H is a normal subgroup, then the collection of cosets G/H forms a group. Your group operation should be as follows: if xH and yH are cosets, then their product is defined to be xyH. You must prove that this is well defined and gives an associative binary operation on G/H. You must also show that there is a group identity and that every element has an inverse.

10. Let S be a set and let $\bullet$ be an operation on that set. Thus if s, t are elements of S, then $s \bullet t$ is another element of S. Let $T \subset S$. We say that the operation $\bullet$ is *closed* on T if $s \bullet t$ lies in T whenever $s, t \in T$.

Let S be the integers and let $T = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$. Is T closed under addition? Is T closed under multiplication?

Let S be the integers and let $T = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$. Is T closed under addition? Is T closed under multiplication?

11. In view of what you learned in Chapter 5 and Section 11.2, discuss the validity of the following statement: "If Euclidean geometry is consistent, then hyperbolic geometry is consistent."

12. A group G is called *cyclic* if there is an element $x \in G$ such that every element of G has the form x^k for some fixed element $x \in G$. Here $x^k \equiv x \cdot x \cdots x$, the product of k copies of x, when k is a positive integer; $x^k \equiv (x^{-1})^{|k|}$ when k is a negative integer; and $x^0 = e$. Give an example of a cyclic group with infinitely many elements (that is, a cyclic group of infinite order). Give an example of a cyclic group with finitely many elements (that is, a cyclic group of finite order).

13. Refer to Exercise 11.9 and 11.12 for terminology. If G is a cyclic group and H is a subgroup, then prove that G/H is a cyclic group.

14. Let $G = \mathbb{Z}_6 \times \mathbb{Z}_9$. Identify all the subgroups that have order a power of 3.

* **15.** Construct a hyperbolic trigonometry based on the hyperbolic geometry of the unit circle.

16. As noted in the text, the stereographic projection can be used to give an isomorphism between the Poincaré version of non-Euclidean geometry and the Beltrami–Klein version. Discuss Axioms **P1**–**P5** as well as **Q5** (Exercise 11.6 above) for the Beltrami–Klein model.

17. The complex function

$$\phi(z) = i\frac{1-z}{1+z}$$

maps the unit disc (the interior of the unit circle C) one-to-one and onto the upper half plane $U \equiv \{x + iy : y > 0\}$. This mapping is infinitesimally angle preserving (or *conformal*). Thus it induces a non-Euclidean geometry on the upper half plane. Describe this geometry. What are the points? What are the lines? What is the notion of distance?

18. In calculus we learn to calculate the length of a curve $\gamma(t), 0 \leq t \leq 1$, according to the formula

$$\ell(\gamma) = \int_0^1 |\gamma'(t)|\, dt.$$

Here $|\gamma'(t)|$ is the standard Euclidean length of the tangent vector $\gamma'(t)$.

Riemann's approach to non-Euclidean geometry was to allow the method of measuring the length of a tangent vector to vary from point to point. After all, $\gamma'(t_1)$ is a tangent vector to the curve *at the point* $\gamma(t_1)$ and $\gamma'(t_2)$ is a tangent vector to the curve *at the point* $\gamma(t_2)$, and it is plausible that length could be measured differently at these two points.

Now if $\gamma(t), 0 \leq t \leq 1$, is a curve in the unit disc, let us define the *Poincaré length* of the tangent vector $\gamma'(t)$ to be

$$\|\gamma'(t)\|_{\mathcal{P},\gamma(t)} = \frac{2|\gamma'(t)|}{1-|\gamma(t)|^2}.$$

As before, $|\quad|$ denotes Euclidean length. Notice that we are dilating our method of measuring length according to how close the point is to the boundary.

Fix $0 < r < 1$. Use the Poincaré length of a tangent vector to calculate the length of the curve $\gamma(t) = rt, 0 \leq t \leq 1$. Compare your result with the calculation of the Poincaré distance of 0 to $(r, 0)$ that was given in the text.

19. Refer to Exercise 11.18 for terminology. Consider geometry on the Euclidean plane. Suppose that $\gamma(t) = (\gamma_1(t), \gamma_2(t)), 0 \leq t \leq 1$, is a curve. Define the length of a tangent vector $\gamma'(t)$ at $\gamma(t)$ to be

$$\|\gamma'(t)\|_{\gamma(t)} = \max\{|\gamma_{\mathbf{1}}'(\mathbf{t})|, |\gamma_{\mathbf{2}}'(\mathbf{t})|\}.$$

In this geometry, what is the distance from $(0, 0)$ to $(1, 1)$? What is the curve of least length connecting these two points?

20. The Euclidean space $\mathbb{R}^3$ can be equipped with a group structure according to the law $(x, y, z)+(x', y', z') = (x+x', y+y', z+z')$. In this structure, the element $(0, 0, 0)$ is the identity and the inverse of (x, y, z) is $(-x, -y, -z)$. However, this is not the only group structure on $\mathbb{R}^3$. Devise another group structure that is noncommutative. (**Hint:** The group law will be expressed as quadratic polynomials in the coordinates. Consider a subgroup of the 3×3 matrices under matrix multiplication.)

21. Consider the group of all 2×2 matrices with entries that are elements of $\mathbb{Z}_3$. How many elements does this group have? Give an example of a subgroup of order 9. Give an example of a subgroup of order 27. Give an example of a subgroup of order 3.

* **22.** Give an example of a group G of finite order m and an integer k that divides m such that G does *not* have a subgroup of order k. [**Hint:** The group must be non-abelian. This problem is tricky. The least k, m that will work are 6 and 12.]

23. Let G and H be isomorphic groups. Call the isomorphism ϕ. Suppose that $g \in G$ and that $g^k = e_G$ for some positive integer k. Prove that $\phi(g)$ has the property that $[\phi(g)]^k = e_H$.

24. Refer to Exercise 11.9 for terminology. Let G and H be isomorphic groups, with isomorphism ϕ. Let K be a normal subgroup of G. Prove that the image of K under ϕ is a normal subgroup of H.

25. Let a be a complex number of modulus less than 1. Define $\phi_a(z) = (z - a)/(1 - \overline{a}z)$. Prove that ϕ_a maps the interior of the unit circle to the interior of the unit circle. Indeed, ϕ_a maps the unit circle itself to the unit circle. Prove that ϕ_a maps lines in Poincaré geometry to lines in Poincaré geometry. In particular, a circular arc inside the unit circle that is perpendicular to the unit circle is mapped by ϕ_a either to another such circular arc, or to a diameter of the circle.

26. Let p and q be points on the unit sphere. Describe an algorithm for finding the great circle that passes through p and q. Under what circumstances can you be sure that this circle is unique?

27. Refer to Exercise 11.25 for terminology. For $0 < \theta \leq 2\pi$, define a map

$$\rho_\theta(z) = e^{i\theta} \cdot z \, .$$

Then ρ_θ is the rotation of the unit disc in the complex plane through an angle of θ. Prove this statement, and prove that ρ_θ is one-to-one and onto from the disc to itself.

Prove that the collection of all maps of the form

$$\rho_\theta \circ \phi_a$$

forms a group. This object is known as the "group of conformal self-maps of the unit disc."

28. Refer to Exercises 11.25 and 11.27 for terminology. Prove that, if there are two points p, q in the disc such that a mapping $\tau = \rho_\theta \circ \phi_a$ satisfies $\tau(p) = p$ and $\tau(q) = q$, then in fact $\tau(z) \equiv z$ for all $z \in D$.

29. In the standard geometry of the Euclidean plane, the curves of shortest distance are straight lines: the least distance between two planar points is realized by the straight Euclidean line between those points. The Poincaré lines play the same role in the Poincaré geometry of the unit disc.

Conversely, in classical Euclidean geometry, we know that two planar points uniquely determine a straight line. What is the correct analogue of "two" for the Poincaré lines in the disc?

30. Let ℓ be a Poincaré line in the unit disc and p a point that is not on that line. Is there a unique Poincaré line m through p that is perpendicular to ℓ?