Abstract Algebra

Solutions Manual (PRETEXT SAMPLE ONLY)

Abstract Algebra

Solutions Manual (PRETEXT SAMPLE ONLY)

Thomas W. Judson
Stephen F. Austin State University

Sage Exercises for Abstract Algebra

Robert A. Beezer
University of Puget Sound

January 2, 2025

Edition: Annual Edition 2015

Website: abstract.pugetsound.edu[1]

[1] abstract.pugetsound.edu

Preface to the Solutions Manual

This contains the publicly available hints and answers for the PreTeXt sample book. Statements of the exercises are not reproduced.

See the text itself for much more information about the book.

Contents

1 Preliminaries

1.4 Exercises

Warm-up

This is a meaningless subdivision of the exercises for the sake of testing output.

1.4.1. Suppose that

$$
\begin{aligned}
A &= \{x : x \in \mathbb{N} \text{ and } x \text{ is even}\}, \\
B &= \{x : x \in \mathbb{N} \text{ and } x \text{ is prime}\}, \\
C &= \{x : x \in \mathbb{N} \text{ and } x \text{ is a multiple of } 5\}.
\end{aligned}
$$

Describe each of the following sets.

(a) $A \cap B$

(b) $B \cap C$

(c) $A \cup B$

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

1.4.2. If $A = \{a, b, c\}$, $B = \{1, 2, 3\}$, $C = \{x\}$, and $D = \emptyset$, list all of the elements in each of the following sets.

(a) $A \times B$

(b) $B \times A$

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

(d) $A \times D$

Hint. (a) $A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3), (c, 1), (c, 2), (c, 3)\}$; (d) $A \times D = \emptyset$.

1.4.3. Find an example of two nonempty sets A and B for which $A \times B = B \times A$ is true.

1.4.4. Prove $A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$.

1.4.5. Prove $A \cup B = B \cup A$ and $A \cap B = B \cap A$.

1.4.6. Prove $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Hint. If $x \in A \cup (B \cap C)$, then either $x \in A$ or $x \in B \cap C$. Thus, $x \in A \cup B$ and $A \cup C$. Hence, $x \in (A \cup B) \cap (A \cup C)$. Therefore, $A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C)$. Conversely, if $x \in (A \cup B) \cap (A \cup C)$, then $x \in A \cup B$ and $A \cup C$. Thus, $x \in A$ or x is in both B and C. So $x \in A \cup (B \cap C)$ and therefore $(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$. Hence, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

1.4.7. Prove $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

1.4.8. Prove $A \subset B$ if and only if $A \cap B = A$.

1.4.9. Prove $(A \cap B)' = A' \cup B'$.

1.4.10. Prove $A \cup B = (A \cap B) \cup (A \setminus B) \cup (B \setminus A)$.

Hint. $(A \cap B) \cup (A \setminus B) \cup (B \setminus A) = (A \cap B) \cup (A \cap B') \cup (B \cap A') = [A \cap (B \cup B')] \cup (B \cap A') = A \cup (B \cap A') = (A \cup B) \cap (A \cup A') = A \cup B$.

1.4.11. Prove $(A \cup B) \times C = (A \times C) \cup (B \times C)$.

1.4.12. Prove $(A \cap B) \setminus B = \emptyset$.

1.4.13. Prove $(A \cup B) \setminus B = A \setminus B$.

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

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

More Exercises

This is a meaningless subdivision of the exercises for the sake of testing output.

1.4.15. Prove $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.

1.4.16. Prove $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.

1.4.17. Which of the following relations $f : \mathbb{Q} \to \mathbb{Q}$ define a mapping? In each case, supply a reason why f is or is not a mapping.

(a) $f(p/q) = \dfrac{p+1}{p-2}$

(b) $f(p/q) = \dfrac{3p}{3q}$

(c) $f(p/q) = \dfrac{p+q}{q^2}$

(d) $f(p/q) = \dfrac{3p^2}{7q^2} - \dfrac{p}{q}$

1.4.18. Determine which of the following functions are one-to-one and which are onto. If the function is not onto, determine its range.

(a) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = e^x$

(b) $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = n^2 + 3$

(c) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = \sin x$

(d) $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x^2$

Hint. (a) f is one-to-one but not onto. $f(\mathbb{R}) = \{x \in \mathbb{R} : x > 0\}$. (c) f is neither one-to-one nor onto. $f(\mathbb{R}) = \{x : -1 \le x \le 1\}$.

1.4.19. Let $f : A \to B$ and $g : B \to C$ be invertible mappings; that is, mappings such that f^{-1} and g^{-1} exist. Show that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

1.4.20.

(a) Define a function $f : \mathbb{N} \to \mathbb{N}$ that is one-to-one but not onto.

(b) Define a function $f : \mathbb{N} \to \mathbb{N}$ that is onto but not one-to-one.

Hint. (a) $f(n) = n + 1$.

1.4.21. Prove the relation defined on $\mathbb{R}^2$ by $(x_1, y_1) \sim (x_2, y_2)$ if $x_1^2 + y_1^2 = x_2^2 + y_2^2$ is an equivalence relation.

1.4.22. Let $f : A \to B$ and $g : B \to C$ be maps.

(a) If f and g are both one-to-one functions, show that $g \circ f$ is one-to-one.

(b) If $g \circ f$ is onto, show that g is onto.

(c) If $g \circ f$ is one-to-one, show that f is one-to-one.

(d) If $g \circ f$ is one-to-one and f is onto, show that g is one-to-one.

(e) If $g \circ f$ is onto and g is one-to-one, show that f is onto.

Hint. (a) Let $x, y \in A$. Then $g(f(x)) = (g \circ f)(x) = (g \circ f)(y) = g(f(y))$. Thus, $f(x) = f(y)$ and $x = y$, so $g \circ f$ is one-to-one. (b) Let $c \in C$, then $c = (g \circ f)(x) = g(f(x))$ for some $x \in A$. Since $f(x) \in B$, g is onto.

1.4.23. Define a function on the real numbers by

$$f(x) = \frac{x+1}{x-1}.$$

What are the domain and range of f? What is the inverse of f? Compute $f \circ f^{-1}$ and $f^{-1} \circ f$.

1.4.24. Let $f : X \to Y$ be a map with $A_1, A_2 \subset X$ and $B_1, B_2 \subset Y$.

(a) Prove $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

(b) Prove $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$. Give an example in which equality fails.

(c) Prove $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$, where

$$f^{-1}(B) = \{x \in X : f(x) \in B\}.$$

(d) Prove $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.

(e) Prove $f^{-1}(Y \setminus B_1) = X \setminus f^{-1}(B_1)$.

Hint. (a) Let $y \in f(A_1 \cup A_2)$. Then there exists an $x \in A_1 \cup A_2$ such that $f(x) = y$. Hence, $y \in f(A_1)$ or $f(A_2)$. Therefore, $y \in f(A_1) \cup f(A_2)$. Consequently, $f(A_1 \cup A_2) \subset f(A_1) \cup f(A_2)$. Conversely, if $y \in f(A_1) \cup f(A_2)$, then $y \in f(A_1)$ or $f(A_2)$. Hence, there exists an $x \in A_1$ or there exists an $x \in A_2$ such that $f(x) = y$. Thus, there exists an $x \in A_1 \cup A_2$ such that $f(x) = y$. Therefore, $f(A_1) \cup f(A_2) \subset f(A_1 \cup A_2)$, and $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

1.4.25. Determine whether or not the following relations are equivalence relations on the given set. If the relation is an equivalence relation, describe the partition given by it. If the relation is not an equivalence relation, state why it fails to be one.

(a) $x \sim y$ in $\mathbb{R}$ if $x \geq y$

(b) $m \sim n$ in $\mathbb{Z}$ if $mn > 0$

(c) $x \sim y$ in $\mathbb{R}$ if $|x - y| \leq 4$

(d) $m \sim n$ in $\mathbb{Z}$ if $m \equiv n \pmod 6$

1.4.26. Define a relation $\sim$ on $\mathbb{R}^2$ by stating that $(a, b) \sim (c, d)$ if and only if $a^2 + b^2 \leq c^2 + d^2$. Show that $\sim$ is reflexive and transitive but not symmetric.

1.4.27. Show that an $m \times n$ matrix gives rise to a well-defined map from $\mathbb{R}^n$ to $\mathbb{R}^m$.

1.4.28. Find the error in the following argument by providing a counterexample. "The reflexive property is redundant in the axioms for an equivalence relation. If $x \sim y$, then $y \sim x$ by the symmetric property. Using the transitive property, we can deduce that $x \sim x$."

Hint. Let $X = \mathbb{N} \cup \{\sqrt{2}\}$ and define $x \sim y$ if $x + y \in \mathbb{N}$.

1.4.29. Projective Real Line. Define a relation on $\mathbb{R}^2 \setminus \{(0,0)\}$ by letting $(x_1, y_1) \sim (x_2, y_2)$ if there exists a nonzero real number λ such that $(x_1, y_1) = (\lambda x_2, \lambda y_2)$. Prove that $\sim$ defines an equivalence relation on $\mathbb{R}^2 \setminus (0,0)$. What are the corresponding equivalence classes? This equivalence relation defines the projective line, denoted by $\mathbb{P}(\mathbb{R})$, which is very important in geometry.

1.5 Sage Exercises

1.5.1. This exercise is just about making sure you know how to use Sage. Login to a Sage Notebook server and create a new worksheet. Do some non-trivial computation, maybe a pretty plot or some gruesome numerical computation to an insane precision. Create an interesting list and experiment with it some. Maybe include some nicely formatted text or TEX using the included mini-word-processor of the Sage Notebook (hover until a blue bar appears between cells and then shift-click).

Use whatever mechanism your instructor has in place for submitting your work. Or save your worksheet and then trade worksheets via email (or another electronic method) with a classmate.

2 The Integers

2.4 Exercises

2.4.1. Prove that

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

for $n \in \mathbb{N}$.

Answer. The base case, $S(1) : [1(1+1)(2(1)+1)]/6 = 1 = 1^2$ is true.
Assume that $S(k) : 1^2 + 2^2 + \cdots + k^2 = [k(k+1)(2k+1)]/6$ is true. Then

$$\begin{aligned} 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 &= [k(k+1)(2k+1)]/6 + (k+1)^2 \\ &= [(k+1)((k+1)+1)(2(k+1)+1)]/6, \end{aligned}$$

and so $S(k+1)$ is true. Thus, $S(n)$ is true for all positive integers n.

2.4.2. Prove that

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

for $n \in \mathbb{N}$.

2.4.3. Prove that $n! > 2^n$ for $n \geq 4$.

Answer. The base case, $S(4) : 4! = 24 > 16 = 2^4$ is true. Assume $S(k) : k! > 2^k$ is true. Then $(k+1)! = k!(k+1) > 2^k \cdot 2 = 2^{k+1}$, so $S(k+1)$ is true. Thus, $S(n)$ is true for all positive integers n.

2.4.4. Prove that

$$x + 4x + 7x + \cdots + (3n-2)x = \frac{n(3n-1)x}{2}$$

for $n \in \mathbb{N}$.

2.4.5. Prove that $10^{n+1} + 10^n + 1$ is divisible by 3 for $n \in \mathbb{N}$.

2.4.6. Prove that $4 \cdot 10^{2n} + 9 \cdot 10^{2n-1} + 5$ is divisible by 99 for $n \in \mathbb{N}$.

2.4.7. Show that

$$\sqrt[n]{a_1 a_2 \cdots a_n} \leq \frac{1}{n} \sum_{k=1}^{n} a_k.$$

2.4.8. Use induction to prove that $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$ for $n \in \mathbb{N}$.

2.4.9. Prove the Leibniz rule for $f^{(n)}(x)$, where $f^{(n)}$ is the nth derivative of f; that is, show that

$$(fg)^{(n)}(x) = \sum_{k=0}^{n} \binom{n}{k} f^{(k)}(x) g^{(n-k)}(x).$$

Hint. Follow the proof in Example 2.1.4.

2.4.10. Prove that
$$\frac{1}{2} + \frac{1}{6} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$$
for $n \in \mathbb{N}$.

2.4.11. If x is a nonnegative real number, then show that $(1+x)^n - 1 \geq nx$ for $n = 0, 1, 2, \ldots$.

Hint. The base case, $S(0) : (1+x)^0 - 1 = 0 \geq 0 = 0 \cdot x$ is true. Assume $S(k) : (1+x)^k - 1 \geq kx$ is true. Then
$$\begin{aligned}(1+x)^{k+1} - 1 &= (1+x)(1+x)^k - 1\\ &= (1+x)^k + x(1+x)^k - 1\\ &\geq kx + x(1+x)^k\\ &\geq kx + x\\ &= (k+1)x,\end{aligned}$$
so $S(k+1)$ is true. Therefore, $S(n)$ is true for all positive integers n.

2.4.12. Power Sets. Let X be a set. Define the **power set** of X, denoted $\mathcal{P}(X)$, to be the set of all subsets of X. For example,
$$\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}.$$
For every positive integer n, show that a set with exactly n elements has a power set with exactly 2^n elements.

2.4.13. Prove that the two principles of mathematical induction stated in Section 2.1 are equivalent.

2.4.14. Show that the Principle of Well-Ordering for the natural numbers implies that 1 is the smallest natural number. Use this result to show that the Principle of Well-Ordering implies the Principle of Mathematical Induction; that is, show that if $S \subset \mathbb{N}$ such that $1 \in S$ and $n + 1 \in S$ whenever $n \in S$, then $S = \mathbb{N}$.

2.4.15. For each of the following pairs of numbers a and b, calculate $\gcd(a, b)$ and find integers r and s such that $\gcd(a, b) = ra + sb$.

(a) 14 and 39

(b) 234 and 165

(c) 1739 and 9923

(d) 471 and 562

(e) 23,771 and 19,945

(f) -4357 and 3754

2.4.16. Let a and b be nonzero integers. If there exist integers r and s such that $ar + bs = 1$, show that a and b are relatively prime.

2.4.17. Fibonacci Numbers. The Fibonacci numbers are
$$1, 1, 2, 3, 5, 8, 13, 21, \ldots.$$
We can define them inductively by $f_1 = 1$, $f_2 = 1$, and $f_{n+2} = f_{n+1} + f_n$ for $n \in \mathbb{N}$.

(a) Prove that $f_n < 2^n$.

(b) Prove that $f_{n+1} f_{n-1} = f_n^2 + (-1)^n$, $n \geq 2$.

(c) Prove that $f_n = [(1+\sqrt{5}\,)^n - (1-\sqrt{5}\,)^n]/2^n\sqrt{5}$.

(d) Show that $\lim_{n \to \infty} f_n / f_{n+1} = (\sqrt{5} - 1)/2$.

(e) Prove that f_n and f_{n+1} are relatively prime.

Hint. For Item 2.4.17.a and Item 2.4.17.b use mathematical induction. Item 2.4.17.c Show that $f_1 = 1$, $f_2 = 1$, and $f_{n+2} = f_{n+1} + f_n$. Item 2.4.17.d Use part Item 2.4.17.c. Item 2.4.17.e Use part Item 2.4.17.b and Exercise 2.4.16.

2.4.18. Let a and b be integers such that $\gcd(a, b) = 1$. Let r and s be integers such that $ar + bs = 1$. Prove that

$$\gcd(a, s) = \gcd(r, b) = \gcd(r, s) = 1.$$

2.4.19. Let $x, y \in \mathbb{N}$ be relatively prime. If xy is a perfect square, prove that x and y must both be perfect squares.

Hint. Use the Fundamental Theorem of Arithmetic.

2.4.20. Using the division algorithm, show that every perfect square is of the form $4k$ or $4k + 1$ for some nonnegative integer k.

2.4.21. Suppose that a, b, r, s are pairwise relatively prime and that

$$\begin{aligned} a^2 + b^2 &= r^2 \\ a^2 - b^2 &= s^2. \end{aligned}$$

Prove that a, r, and s are odd and b is even.

2.4.22. Let $n \in \mathbb{N}$. Use the division algorithm to prove that every integer is congruent mod n to precisely one of the integers $0, 1, \ldots, n-1$. Conclude that if r is an integer, then there is exactly one s in $\mathbb{Z}$ such that $0 \leq s < n$ and $[r] = [s]$. Hence, the integers are indeed partitioned by congruence mod n.

2.4.23. Define the **least common multiple** of two nonzero integers a and b, denoted by $\operatorname{lcm}(a, b)$, to be the nonnegative integer m such that both a and b divide m, and if a and b divide any other integer n, then m also divides n. Prove that any two integers a and b have a unique least common multiple.

Hint. Let $S = \{s \in \mathbb{N} : a \mid s,\ b \mid s\}$. Then $S \neq \emptyset$, since $|ab| \in S$. By the Principle of Well-Ordering, S contains a least element m. To show uniqueness, suppose that $a \mid n$ and $b \mid n$ for some $n \in \mathbb{N}$. By the division algorithm, there exist unique integers q and r such that $n = mq + r$, where $0 \leq r < m$. Since a and b divide both m, and n, it must be the case that a and b both divide r. Thus, $r = 0$ by the minimality of m. Therefore, $m \mid n$.

2.4.24. If $d = \gcd(a, b)$ and $m = \operatorname{lcm}(a, b)$, prove that $dm = |ab|$.

2.4.25. Show that $\operatorname{lcm}(a, b) = ab$ if and only if $\gcd(a, b) = 1$.

2.4.26. Prove that $\gcd(a, c) = \gcd(b, c) = 1$ if and only if $\gcd(ab, c) = 1$ for integers a, b, and c.

2.4.27. Let $a, b, c \in \mathbb{Z}$. Prove that if $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Hint. Since $\gcd(a, b) = 1$, there exist integers r and s such that $ar + bs = 1$. Thus, $acr + bcs = c$. Since a divides both bc and itself, a must divide c.

2.4.28. Let $p \geq 2$. Prove that if $2^p - 1$ is prime, then p must also be prime.

2.4.29. Prove that there are an infinite number of primes of the form $6n + 5$.

Hint. Every prime must be of the form 2, 3, $6n + 1$, or $6n + 5$. Suppose there are only finitely many primes of the form $6k + 5$.

2.4.30. Prove that there are an infinite number of primes of the form $4n - 1$.

2.4.31. Using the fact that 2 is prime, show that there do not exist integers p and q such that $p^2 = 2q^2$. Demonstrate that therefore $\sqrt{2}$ cannot be a rational number.

2.5 Programming Exercises

2.5.1. The Sieve of Eratosthenes. One method of computing all of the prime numbers less than a certain fixed positive integer N is to list all of the numbers n such that $1 < n < N$. Begin by eliminating all of the multiples of 2. Next eliminate all of the multiples of 3. Now eliminate all of the multiples of 5. Notice that 4 has already been crossed out. Continue in this manner, noticing that we do not have to go all the way to N; it suffices to stop at $\sqrt{N}$. Using this method, compute all of the prime numbers less than $N = 250$. We can also use this method to find all of the integers that are relatively prime to an integer N. Simply eliminate the prime factors of N and all of their multiples. Using this method, find all of the numbers that are relatively prime to $N = 120$. Using the Sieve of Eratosthenes, write a program that will compute all of the primes less than an integer N.

2.5.2. Let $\mathbb{N}^0 = \mathbb{N} \cup \{0\}$. Ackermann's function is the function $A : \mathbb{N}^0 \times \mathbb{N}^0 \to \mathbb{N}^0$ defined by the equations

$$\begin{aligned} A(0, y) &= y + 1 \\ A(x + 1, 0) &= A(x, 1) \\ A(x + 1, y + 1) &= A(x, A(x + 1, y)). \end{aligned}$$

Use this definition to compute $A(3, 1)$. Write a program to evaluate Ackermann's function. Modify the program to count the number of statements executed in the program when Ackermann's function is evaluated. How many statements are executed in the evaluation of $A(4, 1)$? What about $A(5, 1)$?

2.5.3. Write a computer program that will implement the Euclidean algorithm. The program should accept two positive integers a and b as input and should output $\gcd(a, b)$ as well as integers r and s such that

$$\gcd(a, b) = ra + sb.$$

2.6 Sage Exercises

2.6.1. Use the `next_prime()` command to construct two different 8-digit prime numbers and save them in variables named `a` and `b`.

2.6.2. Use the `.is_prime()` method to verify that your primes `a` and `b` are really prime.

2.6.3. Verify that 1 is the greatest common divisor of your two primes from the previous exercises.

2.6.4. Find two integers that make a "linear combination" of your two primes equal to 1. Include a verification of your result.

2.6.5. Determine a factorization into powers of primes for $c = 4\,598\,037\,234$.

2.6.6. Write a compute cell that defines the same value of `c` again, and then defines a candidate divisor of `c` named `d`. The third line of the cell should return `True` if and only if `d` is a divisor of `c`. Illustrate the use of your cell by testing your code with $d = 7$ and in a new copy of the cell, testing your code with $d = 11$.

3 Groups

3.5 Exercises

3.5.1. Find all $x \in \mathbb{Z}$ satisfying each of the following equations.

(a) $3x \equiv 2 \pmod{7}$

(b) $5x + 1 \equiv 13 \pmod{23}$

(c) $5x + 1 \equiv 13 \pmod{26}$

(d) $9x \equiv 3 \pmod{5}$

(e) $5x \equiv 1 \pmod{6}$

(f) $3x \equiv 1 \pmod{6}$

Hint. (a) $3 + 7\mathbb{Z} = \{\ldots, -4, 3, 10, \ldots\}$; (c) $18 + 26\mathbb{Z}$; (e) $5 + 6\mathbb{Z}$.

3.5.2. Which of the following multiplication tables defined on the set $G = \{a, b, c, d\}$ form a group? Support your answer in each case.

(a)

$\circ$	a	b	c	d
a	a	c	d	a
b	b	b	c	d
c	c	d	a	b
d	d	a	b	c

(b)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

(c)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

(d)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	b	a	d
d	d	d	b	c

Hint. (a) Not a group; (c) a group.

3.5.3. Write out Cayley tables for groups formed by the symmetries of a rectangle and for $(\mathbb{Z}_4, +)$. How many elements are in each group? Are the groups the same? Why or why not?

3.5.4. Describe the symmetries of a rhombus and prove that the set of symmetries forms a group. Give Cayley tables for both the symmetries of a rectangle and the symmetries of a rhombus. Are the symmetries of a rectangle and those of a rhombus the same?

3.5.5. Describe the symmetries of a square and prove that the set of symmetries is a group. Give a Cayley table for the symmetries. How many ways can the vertices of a square be permuted? Is each permutation necessarily a symmetry of the square? The symmetry group of the square is denoted by D_4.

3.5.6. Give a multiplication table for the group $U(12)$.

Hint.

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

3.5.7. Let $S = \mathbb{R} \setminus \{-1\}$ and define a binary operation on S by $a * b = a + b + ab$. Prove that $(S, *)$ is an abelian group.

3.5.8. Give an example of two elements A and B in $GL_2(\mathbb{R})$ with $AB \neq BA$.

Hint. Pick two matrices. Almost any pair will work.

3.5.9. Prove that the product of two matrices in $SL_2(\mathbb{R})$ has determinant one.

3.5.10. Prove that the set of matrices of the form

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

is a group under matrix multiplication. This group, known as the **Heisenberg group**, is important in quantum physics. Matrix multiplication in the Heisenberg group is defined by

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x' & y' \\ 0 & 1 & z' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x + x' & y + y' + xz' \\ 0 & 1 & z + z' \\ 0 & 0 & 1 \end{pmatrix}.$$

3.5.11. Prove that $\det(AB) = \det(A)\det(B)$ in $GL_2(\mathbb{R})$. Use this result to show that the binary operation in the group $GL_2(\mathbb{R})$ is closed; that is, if A and B are in $GL_2(\mathbb{R})$, then $AB \in GL_2(\mathbb{R})$.

3.5.12. Let $\mathbb{Z}_2^n = \{(a_1, a_2, \ldots, a_n) : a_i \in \mathbb{Z}_2\}$. Define a binary operation on $\mathbb{Z}_2^n$ by

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n).$$

Prove that $\mathbb{Z}_2^n$ is a group under this operation. This group is important in algebraic coding theory.

3.5.13. Show that $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ is a group under the operation of multiplication.

3.5.14. Given the groups $\mathbb{R}^*$ and $\mathbb{Z}$, let $G = \mathbb{R}^* \times \mathbb{Z}$. Define a binary operation $\circ$ on G by $(a, m) \circ (b, n) = (ab, m + n)$. Show that G is a group under this operation.

3.5.15. Prove or disprove that every group containing six elements is abelian.

Hint. There is a nonabelian group containing six elements.

3.5.16. Give a specific example of some group G and elements $g, h \in G$ where $(gh)^n \neq g^n h^n$.

Hint. Look at the symmetry group of an equilateral triangle or a square.

3.5.17. Give an example of three different groups with eight elements. Why are the groups different?

Hint. The are five different groups of order 8.

3.5.18. Show that there are $n!$ permutations of a set containing n items.

Hint. Let

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

be in S_n. All of the a_is must be distinct. There are n ways to choose a_1, $n-1$ ways to choose a_2, ..., 2 ways to choose a_{n-1}, and only one way to choose a_n. Therefore, we can form σ in $n(n-1)\cdots 2\cdot 1 = n!$ ways.

3.5.19. Show that

$$0 + a \equiv a + 0 \equiv a \pmod{n}$$

for all $a \in \mathbb{Z}_n$.

3.5.20. Prove that there is a multiplicative identity for the integers modulo n:

$$a \cdot 1 \equiv a \pmod{n}.$$

3.5.21. For each $a \in \mathbb{Z}_n$ find an element $b \in \mathbb{Z}_n$ such that

$$a + b \equiv b + a \equiv 0 \pmod{n}.$$

3.5.22. Show that addition and multiplication mod n are well defined operations. That is, show that the operations do not depend on the choice of the representative from the equivalence classes mod n.

3.5.23. Show that addition and multiplication mod n are associative operations.

3.5.24. Show that multiplication distributes over addition modulo n:

$$a(b+c) \equiv ab + ac \pmod{n}.$$

3.5.25. Let a and b be elements in a group G. Prove that $ab^n a^{-1} = (aba^{-1})^n$ for $n \in \mathbb{Z}$.

Hint.

$$\begin{aligned} (aba^{-1})^n &= (aba^{-1})(aba^{-1})\cdots(aba^{-1}) \\ &= ab(aa^{-1})b(aa^{-1})b\cdots b(aa^{-1})ba^{-1} \\ &= ab^n a^{-1}. \end{aligned}$$

3.5.26. Let $U(n)$ be the group of units in $\mathbb{Z}_n$. If $n > 2$, prove that there is an element $k \in U(n)$ such that $k^2 = 1$ and $k \neq 1$.

3.5.27. Prove that the inverse of $g_1 g_2 \cdots g_n$ is $g_n^{-1} g_{n-1}^{-1} \cdots g_1^{-1}$.

3.5.28. Prove the remainder of Proposition 3.2.14: if G is a group and $a, b \in G$, then the equation $xa = b$ has a unique solution in G.

3.5.29. Prove Theorem 3.2.16.

3.5.30. Prove the right and left cancellation laws for a group G; that is, show that in the group G, $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$ for elements $a, b, c \in G$.

3.5.31. Show that if $a^2 = e$ for all elements a in a group G, then G must be abelian.

Hint. Since $abab = (ab)^2 = e = a^2b^2 = aabb$, we know that $ba = ab$.

3.5.32. Show that if G is a finite group of even order, then there is an $a \in G$ such that a is not the identity and $a^2 = e$.

3.5.33. Let G be a group and suppose that $(ab)^2 = a^2b^2$ for all a and b in G. Prove that G is an abelian group.

3.5.34. Find all the subgroups of $\mathbb{Z}_3 \times \mathbb{Z}_3$. Use this information to show that $\mathbb{Z}_3 \times \mathbb{Z}_3$ is not the same group as $\mathbb{Z}_9$. (See Example 3.3.5 for a short description of the product of groups.)

3.5.35. Find all the subgroups of the symmetry group of an equilateral triangle.

Hint. $H_1 = \{id\}$, $H_2 = \{id, \rho_1, \rho_2\}$, $H_3 = \{id, \mu_1\}$, $H_4 = \{id, \mu_2\}$, $H_5 = \{id, \mu_3\}$, S_3.

3.5.36. Compute the subgroups of the symmetry group of a square.

3.5.37. Let $H = \{2^k : k \in \mathbb{Z}\}$. Show that H is a subgroup of $\mathbb{Q}^*$.

3.5.38. Let $n = 0, 1, 2, \ldots$ and $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$. Prove that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. Show that these subgroups are the only subgroups of $\mathbb{Z}$.

3.5.39. Let $\mathbb{T} = \{z \in \mathbb{C}^* : |z| = 1\}$. Prove that $\mathbb{T}$ is a subgroup of $\mathbb{C}^*$.

3.5.40.

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

where $\theta \in \mathbb{R}$. Prove that G is a subgroup of $SL_2(\mathbb{R})$.

3.5.41. Prove that

$$G = \{a + b\sqrt{2} : a, b \in \mathbb{Q} \text{ and } a \text{ and } b \text{ are not both zero}\}$$

is a subgroup of $\mathbb{R}^*$ under the group operation of multiplication.

Hint. The identity of G is $1 = 1+0\sqrt{2}$. Since $(a+b\sqrt{2}\,)(c+d\sqrt{2}\,) = (ac+2bd)+(ad+bc)\sqrt{2}$, G is closed under multiplication. Finally, $(a + b\sqrt{2}\,)^{-1} = a/(a^2 - 2b^2) - b\sqrt{2}/(a^2 - 2b^2)$.

3.5.42. Let G be the group of 2×2 matrices under addition and

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a + d = 0 \right\}.$$

Prove that H is a subgroup of G.

3.5.43. Prove or disprove: $SL_2(\mathbb{Z})$, the set of 2×2 matrices with integer entries and determinant one, is a subgroup of $SL_2(\mathbb{R})$.

3.5.44. List the subgroups of the quaternion group, Q_8.

3.5.45. Prove that the intersection of two subgroups of a group G is also a subgroup of G.

3.5.46. Prove or disprove: If H and K are subgroups of a group G, then $H \cup K$ is a subgroup of G.

Hint. Look at S_3.

3.5.47. Prove or disprove: If H and K are subgroups of a group G, then $HK = \{hk : h \in H \text{ and } k \in K\}$ is a subgroup of G. What if G is abelian?

3.5.48. Let G be a group and $g \in G$. Show that

$$Z(G) = \{x \in G : gx = xg \text{ for all } g \in G\}$$

is a subgroup of G. This subgroup is called the **center** of G.

3.5.49. Let a and b be elements of a group G. If $a^4 b = ba$ and $a^3 = e$, prove that $ab = ba$.

Hint. Since $a^4 b = ba$, it must be the case that $b = a^6 b = a^2 ba$, and we can conclude that $ab = a^3 ba = ba$.

3.5.50. Give an example of an infinite group in which every nontrivial subgroup is infinite.

3.5.51. If $xy = x^{-1}y^{-1}$ for all x and y in G, prove that G must be abelian.

3.5.52. Prove or disprove: Every proper subgroup of an nonabelian group is nonabelian.

3.5.53. Let H be a subgroup of G and

$$C(H) = \{g \in G : gh = hg \text{ for all } h \in H\}.$$