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

November 14, 2018

Edition: Annual Edition 2015

Website: 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

1.4.1. Suppose that

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

Describe each of the following sets.

(a) $A \cap B$

(b) $B \cap C$

(c) $A \cup B$

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

Hint. (a) $A \cap B = \{2\}$; (b) $B \cap C = \{5\}$.

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

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

Hint. (a) Not a map since $f(2/3)$ is undefined; (b) this is a map; (c) not a map, since $f(1/2) = 3/4$ but $f(2/4) = 3/8$; (d) this is a map.

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 $f^{-1} \circ f$.

Hint. $f^{-1}(x) = (x+1)/(x-1)$.

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 $m \equiv n \pmod 6$

Hint. (a) NThe relation fails to be symmetric. (b) The relation is not reflexive, since 0 is not equivalent to itself. (c) The relation is not transitive.

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. 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.

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

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

$$a^2 + b^2 = r^2$$
$$a^2 - b^2 = s^2.$$

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 $0 \le s < n$ 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 $0 \le r < m$. 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 $p \ge 2$. 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 $a^4b = ba$ and $a^3 = e$, prove that $ab = ba$.

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

$ab = a^3ba = ba$.

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

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

Prove $C(H)$ is a subgroup of G. This subgroup is called the **centralizer** of H in G.

3.5.54. Let H be a subgroup of G. If $g \in G$, show that $gHg^{-1} = \{g^{-1}hg : h \in H\}$ is also a subgroup of G.

3.6 Additional Exercises: Detecting Errors

3.6.1. UPC Symbols. Universal Product Code (UPC) symbols are found on most products in grocery and retail stores. The UPC symbol is a 12-digit code identifying the manufacturer of a product and the product itself (Figure 3.6.1). The first 11 digits contain information about the product; the twelfth digit is used for error detection. If $d_1d_2 \cdots d_{12}$ is a valid UPC number, then

$$3 \cdot d_1 + 1 \cdot d_2 + 3 \cdot d_3 + \cdots + 3 \cdot d_{11} + 1 \cdot d_{12} \equiv 0 \pmod{10}.$$

(a) Show that the UPC number 0-50000-30042-6, which appears in Figure 3.6.1, is a valid UPC number.

(b) Show that the number 0-50000-30043-6 is not a valid UPC number.

(c) Write a formula to calculate the check digit, d_{12}, in the UPC number.

(d) The UPC error detection scheme can detect most transposition errors; that is, it can determine if two digits have been interchanged. Show that the transposition error 0-05000-30042-6 is not detected. Find a transposition error that is detected. Can you find a general rule for the types of transposition errors that can be detected?

(e) Write a program that will determine whether or not a UPC number is valid.

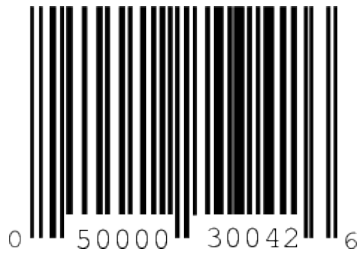

Figure 0.0.1: A UPC code

3.6.2. It is often useful to use an inner product notation for this type of error detection scheme; hence, we will use the notion

$$(d_1, d_2, \ldots, d_k) \cdot (w_1, w_2, \ldots, w_k) \equiv 0 \pmod{n}$$

to mean

$$d_1w_1 + d_2w_2 + \cdots + d_kw_k \equiv 0 \pmod{n}.$$

Suppose that $(d_1, d_2, \ldots, d_k) \cdot (w_1, w_2, \ldots, w_k) \equiv 0 \pmod{n}$ is an error detection scheme for the k-digit identification number $d_1d_2 \cdots d_k$, where $0 \leq d_i < n$. Prove that all single-digit errors are detected if and only if $\gcd(w_i, n) = 1$ for $1 \leq i \leq k$.

3.6.3. Let $(d_1, d_2, \ldots, d_k) \cdot (w_1, w_2, \ldots, w_k) \equiv 0 \pmod{n}$ be an error detection scheme for the k-digit identification number $d_1d_2 \cdots d_k$, where $0 \leq d_i < n$. Prove that all transposition errors of two digits d_i and d_j are detected if and only if $\gcd(w_i - w_j, n) = 1$ for i and j between 1 and k.

3.6.4. ISBN Codes. Every book has an International Standard Book Number (ISBN) code. This is a 10-digit code indicating the book's publisher and title. The tenth digit is a check digit satisfying

$$(d_1, d_2, \ldots, d_{10}) \cdot (10, 9, \ldots, 1) \equiv 0 \pmod{11}.$$

One problem is that d_{10} might have to be a 10 to make the inner product zero; in this case, 11 digits would be needed to make this scheme work. Therefore, the character X is used for the eleventh digit. So ISBN 3-540-96035-X is a valid ISBN code.

(a) Is ISBN 0-534-91500-0 a valid ISBN code? What about ISBN 0-534-91700-0 and ISBN 0-534-19500-0?

(b) Does this method detect all single-digit errors? What about all transposition errors?

(c) How many different ISBN codes are there?

(d) Write a computer program that will calculate the check digit for the first nine digits of an ISBN code.

(e) A publisher has houses in Germany and the United States. Its German prefix is `3-540`. If its United States prefix will be `0-abc`, find `abc` such that the rest of the ISBN code will be the same for a book printed in Germany and in the United States. Under the ISBN coding method the first digit identifies the language; German is `3` and English is `0`. The next group of numbers identifies the publisher, and the last group identifies the specific book.

3.7 Sage Exercises

3.7.1. Create the groups `CyclicPermutationGroup(8)` and `DihedralGroup(4)` and name these groups `C` and `D`, respectively. We will understand these constructions better shortly, but for now just understand that both objects you create are actually groups.

3.7.2. Check that `C` and `D` have the same size by using the `.order()` method. Determine which group is abelian, and which is not, by using the `.is_abelian()` method.

3.7.3. Use the `.cayley_table()` method to create the Cayley table for each group.

3.7.4. Write a nicely formatted discussion identifying differences between the two groups that are discernible in properties of their Cayley tables. In other words, what is {\em different} about these two groups that you can "see" in the Cayley tables? (In the Sage notebook, a Shift-click on a blue bar will bring up a mini-word-processor, and you can use use dollar signs to embed mathematics formatted using TEX syntax.)

3.7.5. For `C` locate the one subgroup of order 4. The group `D` has three subgroups of order 4. Select one of the three subgroups of `D` that has a different structure than the subgroup you obtained from `C`.
The `.subgroups()` method will give you a list of all of the subgroups to help you get started. A Cayley table will help you tell the difference between the two subgroups. What properties of these tables did you use to determine the difference in the structure of the subgroups?

3.7.6. The `.subgroup(elt_list)` method of a group will create the smallest subgroup containing the specified elements of the group, when given the elements as a list `elt_list`. Use this command to discover the shortest list of elements necessary to recreate the subgroups you found in the previous exercise. The equality comparison, `==`, can be used to test if two subgroups are equal.

4 Cyclic Groups

4.5 Exercises

4.5.1. Prove or disprove each of the following statements.

(a) All of the generators of $\mathbb{Z}_{60}$ are prime.

(b) $U(8)$ is cyclic.

(c) $\mathbb{Q}$ is cyclic.

(d) If every proper subgroup of a group G is cyclic, then G is a cyclic group.

(e) A group with a finite number of subgroups is finite.

Hint. (a) False; (c) false; (e) true.

4.5.2. Find the order of each of the following elements.

(a) $5 \in \mathbb{Z}_{12}$

(b) $\sqrt{3} \in \mathbb{R}$

(c) $\sqrt{3} \in \mathbb{R}^*$

(d) $-i \in \mathbb{C}^*$

(e) 72 in $\mathbb{Z}_{240}$

(f) 312 in $\mathbb{Z}_{471}$

Hint. (a) 12; (c) infinite; (e) 10.

4.5.3. List all of the elements in each of the following subgroups.

(a) The subgroup of $\mathbb{Z}$ generated by 7

(b) The subgroup of $\mathbb{Z}_{24}$ generated by 15

(c) All subgroups of $\mathbb{Z}_{12}$

(d) All subgroups of $\mathbb{Z}_{60}$

(e) All subgroups of $\mathbb{Z}_{13}$

(f) All subgroups of $\mathbb{Z}_{48}$

(g) The subgroup generated by 3 in $U(20)$

(h) The subgroup generated by 5 in $U(18)$

(i) The subgroup of $\mathbb{R}^*$ generated by 7

(j) The subgroup of $\mathbb{C}^*$ generated by i where $i^2 = -1$

(k) The subgroup of $\mathbb{C}^*$ generated by $2i$

(l) The subgroup of $\mathbb{C}^*$ generated by $(1+i)/\sqrt{2}$

(m) The subgroup of $\mathbb{C}^*$ generated by $(1+\sqrt{3}\,i)/2$

Hint. (a) $7\mathbb{Z} = \{\ldots, -7, 0, 7, 14, \ldots\}$; (b) $\{0, 3, 6, 9, 12, 15, 18, 21\}$; (c) $\{0\}$, $\{0, 6\}$, $\{0, 4, 8\}$, $\{0, 3, 6, 9\}$, $\{0, 2, 4, 6, 8, 10\}$; (g) $\{1, 3, 7, 9\}$; (j) $\{1, -1, i, -i\}$.

4.5.4. Find the subgroups of $GL_2(\mathbb{R})$ generated by each of the following matrices.

(a) $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ (c) $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ (e) $\begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix}$

(b) $\begin{pmatrix} 0 & 1/3 \\ 3 & 0 \end{pmatrix}$ (d) $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ (f) $\begin{pmatrix} \sqrt{3}/2 & 1/2 \\ -1/2 & \sqrt{3}/2 \end{pmatrix}$

Hint. (a)

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

(c)

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

4.5.5. Find the order of every element in $\mathbb{Z}_{18}$.

4.5.6. Find the order of every element in the symmetry group of the square, D_4.

4.5.7. What are all of the cyclic subgroups of the quaternion group, Q_8?

4.5.8. List all of the cyclic subgroups of $U(30)$.

4.5.9. List every generator of each subgroup of order 8 in $\mathbb{Z}_{32}$.

4.5.10. Find all elements of finite order in each of the following groups. Here the "$*$" indicates the set with zero removed.

(a) $\mathbb{Z}$ (b) $\mathbb{Q}^*$ (c) $\mathbb{R}^*$

Hint. (a) $0, 1, -1$; (b) $1, -1$

4.5.11. If $a^{24} = e$ in a group G, what are the possible orders of a?

Hint. 1, 2, 3, 4, 6, 8, 12, 24.

4.5.12. Find a cyclic group with exactly one generator. Can you find cyclic groups with exactly two generators? Four generators? How about n generators?

4.5.13. For $n \leq 20$, which groups $U(n)$ are cyclic? Make a conjecture as to what is true in general. Can you prove your conjecture?

4.5.14. Let

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

be elements in $GL_2(\mathbb{R})$. Show that A and B have finite orders but AB does not.

4.5.15. Evaluate each of the following.

(a) $(3-2i)+(5i-6)$

(b) $(4-5i)-\overline{(4i-4)}$

(c) $(5-4i)(7+2i)$

(d) $(9-i)\overline{(9-i)}$

(e) i^{45}

(f) $(1+i)+\overline{(1+i)}$

Hint. (a) $-3+3i$; (c) $43-18i$; (e) i

4.5.16. Convert the following complex numbers to the form $a+bi$.

(a) $2\,\mathrm{cis}(\pi/6)$

(b) $5\,\mathrm{cis}(9\pi/4)$

(c) $3\,\mathrm{cis}(\pi)$

(d) $\mathrm{cis}(7\pi/4)/2$

Hint. (a) $\sqrt{3}+i$; (c) -3.

4.5.17. Change the following complex numbers to polar representation.

(a) $1-i$

(b) -5

(c) $2+2i$

(d) $\sqrt{3}+i$

(e) $-3i$

(f) $2i+2\sqrt{3}$

Hint. (a) $\sqrt{2}\,\mathrm{cis}(7\pi/4)$; (c) $2\sqrt{2}\,\mathrm{cis}(\pi/4)$; (e) $3\,\mathrm{cis}(3\pi/2)$.

4.5.18. Calculate each of the following expressions.

(a) $(1+i)^{-1}$

(b) $(1-i)^6$

(c) $(\sqrt{3}+i)^5$

(d) $(-i)^{10}$

(e) $((1-i)/2)^4$

(f) $(-\sqrt{2}-\sqrt{2}\,i)^{12}$

(g) $(-2+2i)^{-5}$

Hint. (a) $(1-i)/2$; (c) $16(i-\sqrt{3}\,)$; (e) $-1/4$.

4.5.19. Prove each of the following statements.

(a) $|z|=|\overline{z}|$

(b) $z\overline{z}=|z|^2$

(c) $z^{-1}=\overline{z}/|z|^2$

(d) $|z+w|\le|z|+|w|$

(e) $|z-w|\ge||z|-|w||$

(f) $|zw|=|z||w|$

4.5.20. List and graph the 6th roots of unity. What are the generators of this group? What are the primitive 6th roots of unity?

4.5.21. List and graph the 5th roots of unity. What are the generators of this group? What are the primitive 5th roots of unity?

4.5.22. Calculate each of the following.

(a) $292^{3171} \pmod{582}$

(b) $2557^{341} \pmod{5681}$

(c) $2071^{9521} \pmod{4724}$

(d) $971^{321} \pmod{765}$

Hint. (a) 292; (c) 1523.

4.5.23. Let $a, b \in G$. Prove the following statements.

(a) The order of a is the same as the order of a^{-1}.

(b) For all $g \in G$, $|a| = |g^{-1}ag|$.

(c) The order of ab is the same as the order of ba.

4.5.24. Let p and q be distinct primes. How many generators does $\mathbb{Z}_{pq}$ have?

4.5.25. Let p be prime and r be a positive integer. How many generators does $\mathbb{Z}_{p^r}$ have?

4.5.26. Prove that $\mathbb{Z}_p$ has no nontrivial subgroups if p is prime.

4.5.27. If g and h have orders 15 and 16 respectively in a group G, what is the order of $\langle g \rangle \cap \langle h \rangle$?

Hint. $|\langle g \rangle \cap \langle h \rangle| = 1$.

4.5.28. Let a be an element in a group G. What is a generator for the subgroup $\langle a^m \rangle \cap \langle a^n \rangle$?

4.5.29. Prove that $\mathbb{Z}_n$ has an even number of generators for $n > 2$.

4.5.30. Suppose that G is a group and let $a, b \in G$. Prove that if $|a| = m$ and $|b| = n$ with $\gcd(m, n) = 1$, then $\langle a \rangle \cap \langle b \rangle = \{e\}$.

4.5.31. Let G be an abelian group. Show that the elements of finite order in G form a subgroup. This subgroup is called the **torsion subgroup** of G.

Hint. The identity element in any group has finite order. Let $g, h \in G$ have orders m and n, respectively. Since $(g^{-1})^m = e$ and $(gh)^{mn} = e$, the elements of finite order in G form a subgroup of G.

4.5.32. Let G be a finite cyclic group of order n generated by x. Show that if $y = x^k$ where $\gcd(k, n) = 1$, then y must be a generator of G.

4.5.33. If G is an abelian group that contains a pair of cyclic subgroups of order 2, show that G must contain a subgroup of order 4. Does this subgroup have to be cyclic?

4.5.34. Let G be an abelian group of order pq where $\gcd(p, q) = 1$. If G contains elements a and b of order p and q respectively, then show that G is cyclic.

4.5.35. Prove that the subgroups of $\mathbb{Z}$ are exactly $n\mathbb{Z}$ for $n = 0, 1, 2, \ldots$.

4.5.36. Prove that the generators of $\mathbb{Z}_n$ are the integers r such that $1 \leq r < n$ and $\gcd(r, n) = 1$.

4.5.37. Prove that if G has no proper nontrivial subgroups, then G is a cyclic group.

Hint. If g is an element distinct from the identity in G, g must generate G; otherwise, $\langle g \rangle$ is a nontrivial proper subgroup of G.

4.5.38. Prove that the order of an element in a cyclic group G must divide the order of the group.

4.5.39. Prove that if G is a cyclic group of order m and $d \mid m$, then G must have a subgroup of order d.

4.5.40. For what integers n is -1 an nth root of unity?

4.5.41. If $z = r(\cos\theta + i\sin\theta)$ and $w = s(\cos\phi + i\sin\phi)$ are two nonzero complex numbers, show that

$$zw = rs[\cos(\theta + \phi) + i\sin(\theta + \phi)].$$

4.5.42. Prove that the circle group is a subgroup of $\mathbb{C}^*$.

4.5.43. Prove that the nth roots of unity form a cyclic subgroup of $\mathbb{T}$ of order n.

4.5.44. Let $\alpha \in \mathbb{T}$. Prove that $\alpha^m = 1$ and $\alpha^n = 1$ if and only if $\alpha^d = 1$ for $d = \gcd(m, n)$.

4.5.45. Let $z \in \mathbb{C}^*$. If $|z| \neq 1$, prove that the order of z is infinite.

4.5.46. Let $z = \cos\theta + i \sin\theta$ be in $\mathbb{T}$ where $\theta \in \mathbb{Q}$. Prove that the order of z is infinite.

4.6 Programming Exercises

4.6.1. Write a computer program that will write any decimal number as the sum of distinct powers of 2. What is the largest integer that yourprogram will handle?

4.6.2. Write a computer program to calculate $a^x \pmod n$ by the method of repeated squares. What are the largest values of n and x that your program will accept?

4.7 Sage Exercises

4.7.1. Execute the statement `R = Integers(40)` to create the set `[0,1,2,...,39]` This is a group under addition mod 40, which we will ignore. Instead we are interested in the subset of elements which have an inverse under *multiplication* mod 40. Determine how big this subgroup is by executing the command `R.unit_group_order()`, and then obtain a list of these elements with `R.list_of_elements_of_multiplicative_group()`.

4.7.2. You can create elements of this group by coercing regular integers into `U`, such as with the statement `a = U(7)`. (Don't confuse this with our mathematical notation $U(40)$.) This will tell Sage that you want to view 7 as an element of U, subject to the corresponding operations. Determine the elements of the cyclic subgroup of U generated by 7 with a list comprehension as follows:

```
R = Integers(40)
a = R(7)
[a^i for i in srange(16)]
```

What is the order of 7 in $U(40)$?

4.7.3. The group $U(49)$ is cyclic. Using only the Sage commands described previously, use Sage to find a generator for this group. Now using *only* theorems about the structure of cyclic groups, describe each of the subgroups of $U(49)$ by specifying its order and by giving an explicit generator. Do not repeat any of the subgroups — in other words, present each subgroup *exactly* once. You can use Sage to check your work on the subgroups, but your answer about the subgroups should rely only on theorems and be a nicely written paragraph with a table, etc.

4.7.4. The group $U(35)$ is not cyclic. Again, using only the Sage commands described previously, use computations to provide irrefutable evidence of this. How many of the 16 different subgroups of $U(35)$ can you list?

4.7.5. Again, using only the Sage commands described previously, explore the structure of $U(n)$ for various values of n and see if you can formulate an interesting conjecture about some basic property of this group. (Yes, this is a *very* open-ended question, but this is ultimately the real power of exploring mathematics with Sage.)

Appendix A

Notation

The following table defines the notation used in this book. Included here in the solutions manual, the page references are missing.

Symbol	Description	Page
$a \in A$	a is in the set A	??
$\mathbb{N}$	the natural numbers	??
$\mathbb{Z}$	the integers	??
$\mathbb{Q}$	the rational numbers	??
$\mathbb{R}$	the real numbers	??
$\mathbb{C}$	the complex numbers	??
$A \subset B$	A is a subset of B	??
$\emptyset$	the empty set	??
$A \cup B$	the union of sets A and B	??
$A \cap B$	the intersection of sets A and B	??
A'	complement of the set A	??
$A \setminus B$	difference between sets A and B	??
$A \times B$	Cartesian product of sets A and B	??
A^n	$A \times \cdots \times A$ (n times)	??
id	identity mapping	??
f^{-1}	inverse of the function f	??
$a \equiv b \pmod{n}$	a is congruent to b modulo n	??
$n!$	n factorial	??
$\binom{n}{k}$	binomial coefficient $n!/(k!(n-k)!)$	??
$a \mid b$	a divides b	??
$\gcd(a, b)$	greatest common divisor of a and b	??
$\mathcal{P}(X)$	power set of X	6
$\operatorname{lcm}(m, n)$	the least common multiple of m and n	7
$\mathbb{Z}_n$	the integers modulo n	??
$U(n)$	group of units in $\mathbb{Z}_n$	??
$\mathbb{M}_n(\mathbb{R})$	the $n \times n$ matrices with entries in $\mathbb{R}$	??
$\det A$	the determinant of A	??
$GL_n(\mathbb{R})$	the general linear group	??
Q_8	the group of quaternions	??
$\mathbb{C}^*$	the multiplicative group of complex numbers	??
$\lvert G \rvert$	the order of a group	??
$\mathbb{R}^*$	the multiplicative group of real numbers	??

(Continued on next page)

Symbol	Description	Page
$\mathbb{Q}^*$	the multiplicative group of rational numbers	**??**
$SL_n(\mathbb{R})$	the special linear group	**??**
$Z(G)$	the center of a group	14
$\langle a \rangle$	cyclic group generated by a	**??**
$\lvert a \rvert$	the order of an element a	**??**
$\operatorname{cis}\theta$	$\cos\theta + i\sin\theta$	**??**
$\mathbb{T}$	the circle group	**??**

Appendix B

GNU Free Documentation License

Version 1.3, 3 November 2008

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE. The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS. This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship

could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "publisher" means any person or entity that distributes copies of the Document to the public.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING. You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced

in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY. If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS. You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties — for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified

Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS. You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS. You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS. A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION. Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but

you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION. You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE. The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See `http://www.gnu.org/copyleft/`.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING. "Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

ADDENDUM: How to use this License for your documents. To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

```
Copyright (C)  YEAR  YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.3
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled "GNU
Free Documentation License".
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with…Texts." line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

Colophon

This solutions manual was authored in PreTeXt.