ABSTRACT ALGEBRA:

A STUDY GUIDE FOR BEGINNERS

John A. Beachy

Northern Illinois University

2014

This is a supplement to

Abstract Algebra, *Third Edition*
by John A. Beachy and William D. Blair

ISBN 1–57766–443–4, Copyright 2005

Waveland Press, Inc.
4180 IL Route 83, Suite 101
Long Grove, Illinois 60047
(847) 634-0081
www.waveland.com

Formatted January 14, 2014, at which time the original was available at:
http://www.math.niu.edu/~beachy/abstract_algebra/

Contents

PREFACE

The changes in the third edition of our book *Abstract Algebra* have dictated a few minor changes in the study guide. In addition to these, I have added a few new problems and done some editing of the solutions of old ones. I hope this edition will continue to be a help to students who are beginning their study of abstract algebra.

DeKalb, Illinois John A. Beachy
October 2006

This study guide now contains over 600 problems, and more than half have detailed solutions, while about a fifth have either an answer or a hint. The ideal way to use the study guide is to work on a solved problem, and if you get stuck, just peek at the solution long enough to get started again. But if the number of problems looks daunting, and you already have a lot of other homework problems, I hope that you can also learn a lot by just reading some solutions. In any case, and however you decide to use the study guide, I hope that you will find the subject as interesting and as challenging as I have.

DeKalb, Illinois John A. Beachy
August 2013

PREFACE TO THE 2ND ED

I first taught an abstract algebra course in 1968, using Herstein's *Topics in Algebra*. It's hard to improve on his book; the subject may have become broader, with applications to computing and other areas, but *Topics* contains the core of any course. Unfortunately, the subject hasn't become any easier, so students meeting abstract algebra still struggle to learn the new concepts, especially since they are probably still learning how to write their own proofs.

This "study guide" is intended to help students who are beginning to learn about abstract algebra. Instead of just expanding the material that is already written down in our textbook, I decided to try to teach by example, by writing out solutions to problems. I've tried to choose problems that would be instructive, and in quite a few cases I've included comments to help the reader see what is really going on. Of course, this study guide isn't a substitute for a good teacher, or for the chance to work together with other students on some hard problems.

Finally, I would like to gratefully acknowledge the support of Northern Illinois University while writing this study guide. As part of the recognition as a "Presidential Teaching Professor," I was given leave in Spring 2000 to work on projects related to teaching.

DeKalb, Illinois John A. Beachy
October 2000

Chapter 1

INTEGERS

Chapter 1 of the text introduces the basic ideas from number theory that are a prerequisite to studying abstract algebra. Many of the concepts introduced there can be abstracted to much more general situations. For example, in Chapter 3 of the text you will be introduced to the concept of a *group*. One of the first broad classes of groups that you will meet depends on the definition of a *cyclic* group, one that is obtained by considering all powers of a particular element. The examples in Section 1.4, constructed using congruence classes of integers, actually tell you everything you will need to know about cyclic groups. In fact, although Chapter 1 is very concrete, it is a significant step forward in the study of abstract algebra.

1.1 Divisors

Before working through the solved problems for this section, you need to make sure that you are familiar with all of the definitions and theorems in the section. In many cases, the proofs of the theorems contain important techniques that you need to copy in solving the exercises in the text. Here are several useful approaches you should know how to use:

—When working on questions involving divisibility you may find it useful to go back to Definition 1.1.1. If you expand the expression $b|a$ by writing "$a = bq$ for some $q \in \mathbf{Z}$", then you have an equation to work with. This equation involves ordinary integers, and so you can use all of the things you already know (from high school algebra) about working with equations. (See the solution to Problem 27.)

—To show that $b|a$, try to write down an expression for a and expand, simplify, or substitute for terms in the expression until you can show how to factor out b. (See the solutions to Problems 26 and 28).

—Another approach to proving that $b|a$ is to use the division algorithm (see Theorem 1.1.3) to write $a = bq + r$, where $0 \leq r < b$. Then to prove that $b|a$ you only need to find some way to check that $r = 0$. (See the solution to Problem 35).

—Theorem 1.1.6 states that any two nonzero integers a and b have a greatest common divisor, which can be expressed as the smallest positive linear combination of a and b. An

integer is a linear combination of a and b if and only if it is a multiple of their greatest common divisor. This is really useful in working on questions involving greatest common divisors. (See the solution to Problem 33).

SOLVED PROBLEMS: §1.1

25. Let a be an integer. Show that if $2 \mid a$ and $3 \mid a$, then $6 \mid a$.

26. Prove that if m and n are odd integers, then $m^2 - n^2$ is divisible by 4.

27. Prove that if a and b are nonzero integers for which $a|b$ and $b|a$, then $b = \pm a$.

28. Prove that if a, b, c are integers for which $a \mid b$ and $a \mid c$, then $a^2 \mid bc$.

29. Find $\gcd(435, 377)$, and express it as a linear combination of 435 and 377.

30. Find $\gcd(3553, 527)$, and express it as a linear combination of 3553 and 527.

31. Which of the integers $0, 1, \ldots, 10$ can be expressed in the form $12m + 20n$, where m, n are integers?

32. If n is a positive integer, find the possible values of $\gcd(n, n + 10)$.

33. Prove that if n is an integer with $n > 1$, then either $\gcd(n - 1,\ n^2 + n + 1) = 1$ or $\gcd(n - 1,\ n^2 + n + 1) = 3$.

34. Prove that if k is a positive odd integer, then any sum of k consecutive integers is divisible by k.

35. Prove that if n is a positive integer, then $\begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}^n = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ if and only if $4|n$.

36. For the complex number $\omega = -\dfrac{1}{2} + \dfrac{\sqrt{3}}{2}i$, prove that $\omega^n = 1$ if and only if $3|n$, for any integer n.

37. Give a proof by induction to show that each number in the sequence 12, 102, 1002, 10002, ..., is divisible by 6.

38. Give a proof by induction to show that $5^{2n} - 1$ is divisible by 24, for all positive integers n.

MORE PROBLEMS: §1.1

Note: The symbol † denotes a problem with an answer or a hint.

39. Find the quotient and remainder when a is divided by b.

†(a) $a = 12345\ ,\quad b = 100$

†(b) $a = -12345\ ,\quad b = 100$

(c) $a = 123\ ,\quad b = 9$

(d) $a = 12345\ ,\quad b = 9$

(e) $a = 7862\ ,\quad b = 9$

(f) $a = 123\ ,\quad b = 11$

(g) $a = 12345\ ,\quad b = 11$

(h) $a = 7862\ ,\quad b = 11$

40.†Find $\gcd(252, 180)$ and write it as a linear combination of 252 and 180.

41.†Find $\gcd(475, 385)$ and express it as a linear combination of 475 and 385.

42. Find $\gcd(1275, 495)$ and express it as a linear combination of 1275 and 495.

43.†Find $\gcd(5917, 4331)$ and express it as a linear combination of 5917 and 4331.

44. Find $\gcd(13651, 3179)$ and express it as a linear combination of 13651 and 3179.

1.2 Primes

Proposition 1.2.2 states that integers a and b are relatively prime if and only if there exist integers m and n with $ma + nb = 1$. This is one of the most useful tools in working with relatively prime integers. Remember that this only works in showing that $\gcd(a, b) = 1$. More generally, if you have a linear combination $ma + nb = d$, it only shows that $\gcd(a, b)$ is a divisor of d (refer back to Theorem 1.1.6).

Since the fundamental theorem of arithmetic (on prime factorization) is proved in this section, you now have some more familiar techniques to use.

SOLVED PROBLEMS: §1.2

26. (a) Use the Euclidean algorithm to find $\gcd(1776, 1492)$.

(b) Use the prime factorizations of 1776 and 1492 to find $\gcd(1776, 1492)$.

27. (a) Use the Euclidean algorithm to find $\gcd(1274, 1089)$.

(b) Use the prime factorizations of 1274 and 1089 to find $\gcd(1274, 1089)$.

28. Give the diagram of all divisors of 250. Do the same for 484.

29. Find all integer solutions of the equation $xy + 2y - 3x = 25$.

30. Let a, b, c be nonzero integers. Prove that if $b \mid a$ and $c \mid a$ and $\gcd(b, c) = d$, then $bc \mid ad$. *Note:* This extends Proposition 1.2.3 (c).

31. For positive integers a, b, c, prove that if $\gcd(a, b) = 1$ and $c \mid b$, then $\gcd(a, c) = 1$.

32. For positive integers a, b, prove that $\gcd(a, b) = 1$ if and only if $\gcd(a^2, b^2) = 1$.

33. Prove that $n - 1$ and $2n - 1$ are relatively prime, for all integers $n > 1$. Is the same true for $2n - 1$ and $3n - 1$?

34. Let m and n be positive integers. Prove that $\gcd(2^m - 1, 2^n - 1) = 1$ if and only if $\gcd(m, n) = 1$.

35. Prove that $\gcd(2n^2 + 4n - 3,\ 2n^2 + 6n - 4) = 1$, for all integers $n > 1$.

36. Prove that if m and n are odd integers, then $m^2 - n^2$ is divisible by 8. (Compare Problem 1.1.26.)

MORE PROBLEMS: §1.2

37.† Find the prime factorizations of 252 and 180 and use them to compute the greatest common divisor and least common multiple of 252 and 180.

(Compare Problem 1.1.40.)

38.† Find the prime factorizations of 475 and 385 and use them to compute the greatest common divisor and least common multiple of 475 and 385.

(Compare Problem 1.1.41.)

39.† Find the prime factorizations of 5917 and 4331 and use them to find $\gcd(5917, 4331)$.

(Compare Problem 1.1.43.)

40. Find the prime factorizations of 13651 and 3179 and use them to find $\gcd(13651, 3179)$.

(Compare Problem 1.1.44.)

41. Give a diagram of all divisors of 90, showing the divisibility relationships.

42.† Show that $\gcd(11n + 5, 7n + 3)$ is 2 if n is odd and 1 if n is even.

43.† Find all positive integer solutions x, y of the equation $xy + 5x - 8y = 79$.

44. Explain why there are no positive integers x, y such that $x^2 - y^2 = 34$.

45. Let a, b, c be positive integers.

(a) Prove that if $\gcd(a, bc) = 1$ and $\gcd(b, c) = 1$, then $\gcd(ab, c) = 1$.

†(b) Prove or disprove the following generalization of part (a): if $\gcd(b, c) = 1$, then $\gcd(a, bc) = \gcd(ab, c)$.

46. Let a, b, c be a **Pythagorean triple** (i.e. positive integers with $a^2 + b^2 = c^2$).

(a) Show that $\gcd(a, b) = 1$ if and only if $\gcd(a, c) = 1$.

†(b) More generally, does $\gcd(a, b) = \gcd(a, c)$?

1.3 Congruences

In this section, it is important to remember that although working with congruences is almost like working with equations, it is not exactly the same.

What things *are* the same? You can add or subtract the same integer on both sides of a congruence, and you can multiply both sides of a congruence by the same integer. You can use substitution, and you can use the fact that if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$. (Review Proposition 1.3.3, and the comments in the text both before and after the proof of the proposition.)

What things are different? In an ordinary equation you can divide through by a nonzero number. In a congruence modulo n, you can only divide through by an integer that is relatively prime to n. This is usually expressed by saying that if $\gcd(a, n) = 1$ and $ac \equiv ad \pmod{n}$, then $c \equiv d \pmod{n}$. Just be very careful when you cancel!

One of the important techniques to understand is how to switch between congruences and ordinary equations. First, any equation involving integers can be converted into a congruence by just reducing modulo n. This works because if two integers are equal, then are certainly congruent modulo n.

To do the opposite conversion you must be more careful. If two integers are congruent modulo n, that doesn't make them equal, but only guarantees that dividing by n produces the same remainder in each case. In other words, the integers may differ by some multiple of n.

The conversion process is illustrated in Example 1.3.5 of the text, where the congruence

$$x \equiv 7 \pmod{8}$$

is converted into the equation

$$x = 7 + 8q \text{ , for some } q \in \mathbf{Z} \text{ .}$$

Notice that converting to an equation makes it more complicated, because we have to introduce another variable. In the example, we really want a congruence modulo 5, so the next step is to rewrite the equation as

$$x \equiv 7 + 8q \pmod{5} \text{ .}$$

Actually, we can reduce each term modulo 5, so that we finally get

$$x \equiv 2 + 3q \pmod{5} \text{ .}$$

You should read the proofs of Theorem 1.3.5 and Theorem 1.3.6 very carefully. These proofs actually show you the necessary techniques to solve all linear congruences of the form $ax \equiv b \pmod{n}$, and all simultaneous linear equations of the form $x \equiv a \pmod{n}$ and $x \equiv b \pmod{m}$, where the moduli n and m are relatively prime.

Many of the theorems in the text should be thought of as "shortcuts". They should become your friends. You can't afford to skip over their proofs, because you might miss important algorithms or computational techniques.

SOLVED PROBLEMS: §1.3

29. Solve the congruence $42x \equiv 12 \pmod{90}$.

30. (a) Find all solutions to the congruence $55x \equiv 35 \pmod{75}$.
    (b) Find all solutions to the congruence $55x \equiv 36 \pmod{75}$.

31. (a) Find one particular integer solution to the equation $110x + 75y = 45$.
    (b) Show that if $x = m$ and $y = n$ is an integer solution to the equation in part (a), then so is $x = m + 15q$ and $y = n - 22q$, for any integer q.

32. Solve the system of congruences $x \equiv 2 \pmod{9}$ $x \equiv 4 \pmod{10}$.

33. Solve the system of congruences $x \equiv 5 \pmod{25}$ $x \equiv 23 \pmod{32}$.

34. Solve the system of congruences $5x \equiv 14 \pmod{17}$ $3x \equiv 2 \pmod{13}$.

35. Give integers a, b, m, n to provide an example of a system
$$x \equiv a \pmod{m} \qquad x \equiv b \pmod{n}$$
that has no solution.

36. Find the additive order of each of the following integers, module 20: 4, 5, 6, 7, and 8.
    Note: The additive order of a modulo n is defined to be the smallest positive solution of the congruence $ax \equiv 0 \pmod{n}$.

37. (a) Compute the last digit in the decimal expansion of 4^{100}.
    (b) Is 4^{100} divisible by 3?

38. Find all integers n for which $13 \mid 4(n^2 + 1)$.

39. Prove that $10^{n+1} + 4 \cdot 10^n + 4$ is divisible by 9, for all positive integers n.

40. Prove that for any integer n, the number $n^3 + 5n$ is divisible by 6.

41. Use techniques of this section to prove that if m and n are odd integers, then $m^2 - n^2$ is divisible by 8. (Compare Problem 1.2.36.)

42. Prove that $4^{2n+1} - 7^{4n-2}$ is divisible by 15, for all positive integers n.

43. Prove that the fourth power of an integer can only have 0, 1, 5, or 6 as its units digit.

MORE PROBLEMS: §1.3

44. Solve the following congruences.
    (a) $4x \equiv 1 \pmod{7}$
    (b) $2x \equiv 1 \pmod{9}$
    (c) $5x \equiv 1 \pmod{32}$
    (d) $19x \equiv 1 \pmod{36}$

45.†Solve the following congruences.

(a) $10x \equiv 5 \pmod{21}$

(b) $10x \equiv 5 \pmod{15}$

(c) $10x \equiv 4 \pmod{15}$

(d) $10x \equiv 4 \pmod{14}$

46. Solve the following congruence: $21x \equiv 6 \pmod{45}$.

47.†Solve the following congruence. $20x \equiv 12 \pmod{72}$

48. Solve the following congruence. $25x \equiv 45 \pmod{60}$

49. Find the additive order of each of the following elements, by solving the appropriate congruences.

†(a) 4, 5, 6 modulo 24

(b) 4, 5, 6 modulo 25

50. Find the additive order of each of the following elements, by solving the appropriate congruences.

(a) 7, 8, 9 modulo 24

(b) 7, 8, 9 modulo 25

51. Find the units digit of $3^{29} + 11^{12} + 15$.

Hint: Choose an appropriate modulus n, and then reduce modulo n.

52. Solve the following system of congruences.

$$x \equiv 15 \pmod{27} \qquad x \equiv 16 \pmod{20}$$

53.†Solve the following system of congruences.

$$x \equiv 11 \pmod{16} \qquad x \equiv 18 \pmod{25}$$

54. Solve the following system of congruences:

$$x \equiv 13 \pmod{25} \qquad x \equiv 9 \pmod{18}$$

55.†Solve the following system of congruences:

$$x \equiv 9 \pmod{25} \qquad x \equiv 13 \pmod{18}$$

56. Solve the following system of congruences.

$$2x \equiv 5 \pmod{7} \qquad 3x \equiv 4 \pmod{8}$$

Hint: First reduce to the usual form.

57.†Solve the following system of congruences.

$$2x \equiv 3 \pmod 7 \qquad x \equiv 4 \pmod 6 \qquad 5x \equiv 50 \pmod{55}$$

58. Prove that if the system

$$x \equiv 1 \pmod m \qquad x \equiv 0 \pmod n$$

has a solution, then m and n are relatively prime.

59.†Use congruences to prove that $5^{2n} - 1$ is divisible by 24, for all positive integers n.

Note: This is Problem 1.1.38, which at that point required a proof by induction.

60. Prove that $n^5 - n$ is divisible by 30, for all integers n.

61.†Prove that if $0 < n < m$, then $2^{2^n} + 1$ and $2^{2^m} + 1$ are relatively prime.

1.4 Integers Modulo n

The ideas in this section allow us to work with equations instead of congruences, provided we think in terms of equivalence classes. To be more precise, any linear congruence of the form

$$ax \equiv b \pmod n$$

can be viewed as an equation in $\mathbf{Z}_n$, written

$$[a]_n[x]_n = [b]_n \ .$$

This gives you one more way to view problems involving congruences. Sometimes it helps to have various ways to think about a problem, and it is worthwhile to learn all of the approaches, so that you can easily shift back and forth between them, and choose whichever approach is the most convenient. For example, trying to divide by a in the congruence $ax \equiv b \pmod n$ can get you into trouble unless $\gcd(a, n) = 1$. Instead of thinking in terms of division, it is probably better to think of multiplying both sides of the equation $[a]_n[x]_n = [b]_n$ by $[a]_n^{-1}$, provided $[a]_n^{-1}$ exists.

It is well worth your time to learn about the sets $\mathbf{Z}_n$ and $\mathbf{Z}_n^\times$. They will provide an important source of examples in Chapter 3, when we begin studying groups. We should mention that we can use negative exponents in $\mathbf{Z}_n^\times$, because if $k < 0$ and $[x]_n \neq [0]_n$, we can define $[x]_n^k = ([x]_n^{-1})^{|k|}$.

The exercises for Section 1.4 of the text contain several definitions for elements of $\mathbf{Z}_n$. If $(a, n) = 1$, then the smallest positive integer k such that $a^k \equiv 1 \pmod n$ is called the *multiplicative order* of $[a]$ in $\mathbf{Z}_n^\times$. The set $\mathbf{Z}_n^\times$ is said to be *cyclic* if it contains an element of multiplicative order $\varphi(n)$. Since $|\mathbf{Z}_n^\times| = \varphi(n)$, this is equivalent to saying that $\mathbf{Z}_n^\times$ is cyclic if has an element $[a]$ such that each element of $\mathbf{Z}_n^\times$ is equal to some power of $[a]$. Finally, the element $[a] \in \mathbf{Z}_n$ is said to be *idempotent* if $[a]^2 = [a]$, and *nilpotent* if $[a]^k = [0]$ for some k.

SOLVED PROBLEMS: §1.4

31. Find the multiplicative inverse of each nonzero element of $\mathbf{Z}_7$.

32. Find the multiplicative inverse of each nonzero element of $\mathbf{Z}_{13}$.

33. Find the multiplicative order of each element of $\mathbf{Z}_7^\times$.

34. Find the multiplicative order of each element of $\mathbf{Z}_9^\times$.

35. Find $[91]_{501}^{-1}$, if possible (in $\mathbf{Z}_{501}^\times$).

36. Find $[3379]_{4061}^{-1}$, if possible (in $\mathbf{Z}_{4061}^\times$).

37. In $\mathbf{Z}_{20}$: find all units (list the multiplicative inverse of each); find all idempotent elements; find all nilpotent elements.

38. Show that $\mathbf{Z}_{17}^\times$ is cyclic.

39. Show that $\mathbf{Z}_{35}^\times$ is not cyclic but that each element has the form $[8]_{35}^i[-4]_{35}^j$, for some positive integers i, j.

40. Solve the equation $[x]_{11}^2 + [x]_{11} - [6]_{11} = [0]_{11}$.

41. Prove that $[a]_n$ is a nilpotent element of $\mathbf{Z}_n$ if and only if each prime divisor of n is a divisor of a.

42. Show that if $n > 1$ is an odd integer, then $\varphi(2n) = \varphi(n)$.

MORE PROBLEMS: §1.4

43.† Write out multiplication tables for the following sets.

(a) $\mathbf{Z}_9^\times$

(b) $\mathbf{Z}_{10}^\times$

(c) $\mathbf{Z}_{12}^\times$

(d) $\mathbf{Z}_{14}^\times$

44. Find the multiplicative inverses of the given elements (if possible).

†(a) [12] in $\mathbf{Z}_{15}$

(b) [14] in $\mathbf{Z}_{15}$

†(c) [7] in $\mathbf{Z}_{15}$

(d) [12] in $\mathbf{Z}_{23}$

(e) [14] in $\mathbf{Z}_{32}$

45. Find the multiplicative orders of the following elements.
    (a) [5] and [7] in $\mathbf{Z}_{16}^{\times}$
    †(b) [5] and [7] in $\mathbf{Z}_{17}^{\times}$
    (c) [5] and [7] in $\mathbf{Z}_{18}^{\times}$

46. Find the multiplicative order of each element of the following sets.
    (a) $\mathbf{Z}_8^{\times}$
    †(b) $\mathbf{Z}_{10}^{\times}$
    (c) $\mathbf{Z}_{11}^{\times}$

47. †Is $\mathbf{Z}_{14}^{\times}$ cyclic?

48. †Is $\mathbf{Z}_{16}^{\times}$ cyclic?

49. †Is $\mathbf{Z}_{18}^{\times}$ cyclic?

50. Find all idempotent elements in the following sets.
    †(a) $\mathbf{Z}_{14}$
    (b) $\mathbf{Z}_{16}$

51. Find all nilpotent elements in the following sets.
    (a) $\mathbf{Z}_{14}$
    (b) $\mathbf{Z}_{16}$

52. †In $\mathbf{Z}_{24}$: find all units (list the multiplicative inverse of each); find all idempotent elements; find all nilpotent elements.

53. †Find $\{n \in \mathbf{Z}^+ \mid \varphi(n) = 2\}$ and $\{n \in \mathbf{Z}^+ \mid \varphi(n) = 4\}$.

54. Prove that if m, n are positive integers with $m \mid n$, then $\varphi(m) \mid \varphi(n)$.

55. Show that $n = 7, 9, 14, 18$ are the only positive integers n such that $\varphi(n) = 6$.

56. Use Fermat's "little" theorem (Corollary 1.4.12) to prove that $n^5 - n$ is divisible by 30, for all integers n.

Chapter 1 Review Problems

1. Prove that if a, b, c are integers for which $b \mid a$ and $b \mid (a - c)$, then $b \mid c$.

2. Find $\gcd(7605, 5733)$, and express it as a linear combination of 7605 and 5733.

3. Find the prime factorizations of 1275 and 495 and use them to find $\gcd(1275, 495)$.

4. Find $\varphi(1275)$ and $\varphi(495)$.

5. Solve the congruence $24x \equiv 168 \pmod{200}$.

6. Find the additive order of 168 modulo 200.

7. Solve the system of congruences $2x \equiv 9 \pmod{15}$ $x \equiv 8 \pmod{11}$.

8. Find $[50]_{501}^{-1}$ and $[51]_{501}^{-1}$, if possible (in $\mathbf{Z}_{501}^{\times}$).

9. List the elements of $\mathbf{Z}_{15}^{\times}$. For each element, find its multiplicative inverse, and find its multiplicative order.

10. Show that $3^n + 4^n - 1$ is divisible by 6, for any positive integer n.

Chapter 2

FUNCTIONS

The first goal of this chapter is to provide a review of functions. In our study of algebraic structures in later chapters, functions will provide a way to compare two different structures. In this setting, the functions that are one-to-one correspondences will be particularly important. There are also important functions that are not one-to-one, and in this case it becomes necessary to work with the equivalence relation defined by such a function.

The second goal of the chapter is to begin studying groups of permutations, which give a very important class of examples. When you begin to study groups in Chapter 3, you will be able draw on your knowledge of permutation groups, as well as on your knowledge of the groups $\mathbf{Z}_n$ and $\mathbf{Z}_n^\times$ that were studied in Chapter 1.

2.1 Functions

Besides reading Section 2.1, it might help to get out your calculus textbook and review composite functions, one-to-one and onto functions, and inverse functions. The functions $f : \mathbf{R} \to \mathbf{R}^+$ and $g : \mathbf{R}^+ \to \mathbf{R}$ defined by $f(x) = e^x$, for all $x \in \mathbf{R}$, and $g(y) = \ln y$, for all $y \in \mathbf{R}^+$, provide one of the most important examples of a pair of inverse functions.

Definition 2.1.1, the definition of function, is stated rather formally in terms of ordered pairs. (Think of this as a definition given in terms of the "graph" of the function.) This puts the definition on the firm foundation of set theory. But in actually using this definition, the text almost immediately goes back to what should be a more familiar definition: a function $f : S \to T$ is a "rule" that assigns to each element of S a unique element of T.

One of the most fundamental ideas of abstract algebra is that algebraic structures should be thought of as essentially the same if the only difference between them is the way elements have been named. To make this precise we will say that structures are the same if we can set up an invertible function from one to the other that preserves the essential algebraic structure. That makes it especially important to understand the concept of an inverse function, as introduced in this section.

SOLVED PROBLEMS: §2.1

21. The "Vertical Line Test" from calculus says that a curve in the xy-plane is the graph

of a function of x if and only if no vertical line intersects the curve more than once. Explain why this agrees with Definition 2.1.1.

22. The "Horizontal Line Test" from calculus says that a function is one-to-one if and only if no horizontal line intersects its graph more than once. Explain why this agrees with Definition 2.1.4.

23. In calculus the graph of an inverse function f^{-1} is obtained by reflecting the graph of f about the line $y = x$. Explain why this agrees with Definition 2.1.6.

24. Show that the function $f : \mathbf{R}^2 \to \mathbf{R}^2$ defined by $f(x, y) = (x^3+y, y)$, for all $(x, y) \in \mathbf{R}^2$, is a one-to-one correspondence.

25. Define $f : \mathbf{R} \to \mathbf{R}$ by $f(x) = x^3 + 3x - 5$, for all $x \in \mathbf{R}$. Is f a one-to-one function? Is f an onto function?

    Hint: Use the derivative of f to show that f is a strictly increasing function.

26. Does the following formula define a function from $\mathbf{Q}$ to $\mathbf{Z}$? Set $f\left(\frac{m}{n}\right) = m$, where m, n are integers and $n \neq 0$.

27. Define the formulas $f : \mathbf{Z}_{12} \to \mathbf{Z}_8$ by $f([x]_{12}) = [2x]_8$, for all $[x]_{12} \in \mathbf{Z}_{12}$, and $g : \mathbf{Z}_{12} \to \mathbf{Z}_8$ by $g([x]_{12}) = [3x]_8$, for all $[x]_{12} \in \mathbf{Z}_{12}$. Show that f defines a function, but g does not.

28. Let a be a fixed element of $\mathbf{Z}_{17}^{\times}$. Define the function $\theta : \mathbf{Z}_{17}^{\times} \to \mathbf{Z}_{17}^{\times}$ by $\theta(x) = ax$, for all $x \in \mathbf{Z}_{17}^{\times}$. Is θ one-to-one? Is θ onto? If possible, find the inverse function θ^{-1}.

29. For integers m, n, b with $n > 1$, define $f : \mathbf{Z}_n \to \mathbf{Z}_n$ by $f([x]_n) = [mx + b]_n$.

    (a) Show that f is a well-defined function.

    (b) Prove that f is a one-to-one correspondence if and only if $\gcd(m, n) = 1$.

    (c) If $\gcd(m, n) = 1$, find the inverse function f^{-1}.

30. Let $f : S \to T$ be a function, and let A, B be subsets of S. Prove the following:

    (a) If $A \subseteq B$, then $f(A) \subseteq f(B)$.

    (b) $f(A \cup B) = f(A) \cup f(B)$

    (c) $f(A \cap B) \subseteq f(A) \cap f(B)$

31. Let $f : S \to T$ be a function. Prove that f is a one-to-one function if and only if $f(A \cap B) = f(A) \cap f(B)$ for all subsets A, B of S.

32. Let $f : S \to T$ be a function, and let X, Y be subsets of T. Prove the following:

    (a) If $X \subseteq Y$, then $f^{-1}(X) \subseteq f^{-1}(Y)$.

    (b) $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$

    (c) $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$

33. Let A be an $n \times n$ matrix with entries in $\mathbf{R}$. Define a linear transformation $L : \mathbf{R}^n \to \mathbf{R}^n$ by $L(\mathbf{x}) = A\mathbf{x}$, for all $\mathbf{x} \in \mathbf{R}^n$.

    (a) Show that L is an invertible function if and only if $\det(A) \neq 0$.

    (b) Show that if L is either one-to-one or onto, then it is invertible.

34. Let A be an $m \times n$ matrix with entries in $\mathbf{R}$, and assume that $m > n$. Define a linear transformation $L : \mathbf{R}^n \to \mathbf{R}^m$ by $L(\mathbf{x}) = A\mathbf{x}$, for all $\mathbf{x} \in \mathbf{R}^n$. Show that L is a one-to-one function if $\det(A^T A) \neq 0$, where A^T is the transpose of A.

35. Let A be an $n \times n$ matrix with entries in $\mathbf{R}$. Define a linear transformation $L : \mathbf{R}^n \to \mathbf{R}^n$ by $L(\mathbf{x}) = A\mathbf{x}$, for all $\mathbf{x} \in \mathbf{R}^n$. Prove that L is one-to-one if and only if no eigenvalue of A is equal to zero.

    Note: A vector $\mathbf{x}$ is called an **eigenvector** of A if it is nonzero and there exists a scalar λ such a that $A\mathbf{x} = \lambda\mathbf{x}$, and in this case λ is called an **eigenvalue** of A.

MORE PROBLEMS: §2.1

36. In each of the following parts, determine whether the given function is one-to-one and whether it is onto.

    †(a) $f : \mathbf{Z}_{12} \to \mathbf{Z}_{12}$; $f([x]_{12}) = [7x + 3]_{12}$, for all $[x]_{12} \in \mathbf{Z}_{12}$

    (b) $f : \mathbf{Z}_{12} \to \mathbf{Z}_{12}$; $f([x]_{12}) = [8x + 3]_{12}$, for all $[x]_{12} \in \mathbf{Z}_{12}$

    †(c) $f : \mathbf{Z}_{12} \to \mathbf{Z}_{12}$; $f([x]_{12}) = [x]_{12}^2$, for all $[x]_{12} \in \mathbf{Z}_{12}$

    (d) $f : \mathbf{Z}_{12} \to \mathbf{Z}_{12}$; $f([x]_{12}) = [x]_{12}^3$, for all $[x]_{12} \in \mathbf{Z}_{12}$

    †(e) $f : \mathbf{Z}_{12}^\times \to \mathbf{Z}_{12}^\times$; $f([x]_{12}) = [x]_{12}^2$, for all $[x]_{12} \in \mathbf{Z}_{12}^\times$

    †(f) $f : \mathbf{Z}_{12}^\times \to \mathbf{Z}_{12}^\times$; $f([x]_{12}) = [x]_{12}^3$, for all $[x]_{12} \in \mathbf{Z}_{12}^\times$

37. †For each one-to-one and onto function in Problem 36, find the inverse of the function.

38. Define $f : \mathbf{Z}_4 \to \mathbf{Z}_{10}^\times$ by $f([m]_4) = [3]_{10}^m$, for all $[m]_4 \in \mathbf{Z}_4$.

    (a) Show that f is a well-defined function.

    (b) Show that f is one-to-one and onto.

39. Define $f : \mathbf{Z}_{10} \to \mathbf{Z}_{11}^\times$ by $f([m]_{10}) = [2]_{11}^m$, for all $[m]_{10} \in \mathbf{Z}_{10}$.

    (a) Show that f is a well-defined function.

    †(b) Is f one-to-one and onto?

40. Define $f : \mathbf{Z}_8 \to \mathbf{Z}_{16}^\times$ by $f([m]_8) = [3]_{16}^m$, for all $[m]_8 \in \mathbf{Z}_8$.

    (a) Show that f is a well-defined function.

    †(b) Is f one-to-one and onto?

41. Show that each of the following formulas yields a well-defined function.
    (a) $f : \mathbf{Z}_8 \to \mathbf{Z}_8$ defined by $f([x]_8) = [3x^2 - 3x + 1]_8$, for all $[x]_8 \in \mathbf{Z}_8$
    (b) $f : \mathbf{Z}_{12} \to \mathbf{Z}_8$ defined by $f([x]_{12}) = [2x^2 - 4x + 6]_8$, for all $[x]_{12} \in \mathbf{Z}_{12}$
    (b) $f : \mathbf{Z}_{15}^\times \to \mathbf{Z}_5^\times$ defined by $f([x]_{15}) = [3x^3]_5$, for all $[x]_{15} \in \mathbf{Z}_{15}^\times$

42.† Consider the function $f : \mathbf{Z}_{10} \to \mathbf{Z}_{10}$ defined by $f([x]_{10}) = [3x + 4]_{10}$. Show that f is one-to-one and onto by computing all values of the function. Then find a formula of the type $g([x]_{10}) = [mx + b]_{10}$ that gives the inverse of f.

43. Let n be a positive integer. Show that $i : \mathbf{Z}_n^\times \to \mathbf{Z}_n^\times$ defined by $i([x]_n) = [x]_n^{-1}$, for all $[x]_n \in \mathbf{Z}_n^\times$ is a well-defined one-to-one correspondence.

44. Let m, n be positive integers with $m \mid n$. Show that $\pi : \mathbf{Z}_n^\times \to \mathbf{Z}_m^\times$ defined by $f([x]_n) = [x]_m$, for all $[x]_n \in \mathbf{Z}_n^\times$ is a well-defined function.

45. Let m, n be positive integers with $m \mid n$, and let k be any integer. Show that $f : \mathbf{Z}_n^\times \to \mathbf{Z}_m^\times$ defined by $f([x]_n) = [x]_m^k$, for all $[x]_n \in \mathbf{Z}_n^\times$ is a well-defined function.
    Hint: We know that $g : \mathbf{Z}_m^\times \to \mathbf{Z}_m^\times$ defined by $g([x]_m) = [x]_m^k$ is a function if k is a positive integer. To prove the general case if k is negative, you can use the composite function $i \circ g \circ \pi$, where i and π are the functions in Problems 43 and 44, respectively.

2.2 Equivalence Relations

In a variety of situations it is useful to split a set up into subsets in which the elements have some property in common. You are already familiar with one of the important examples: in Chapter 1 we split the set of integers up into subsets, depending on the remainder when the integer is divided by the fixed integer n. This led to the concept of congruence modulo n, which is a model for our general notion of an *equivalence relation*.

In this section you will find three different points of view, looking at the one idea of splitting up a set S from three distinct vantage points. First there is the definition of an equivalence relation on S, which tells you when two different elements of S belong to the same subset. Then there is the notion of a partition of S, which places the emphasis on describing the subsets. Finally, it turns out that every partition (and equivalence relation) really comes from a function $f : S \to T$, where we say that x_1 and x_2 are equivalent if $f(x_1) = f(x_2)$.

The reason for considering several different point of view is that in a given situation one point of view may be more useful than another. Your goal should be to learn about each point of view, so that you can easily switch from one to the other, which is a big help in deciding which point of view to take.

SOLVED PROBLEMS: §2.2

13. For the function $f : \mathbf{R} \to \mathbf{R}$ defined by $f(x) = x^2$, for all $x \in \mathbf{R}$, describe the equivalence relation $\sim_f$ on $\mathbf{R}$ that is determined by f.

14. (a) Define the function $f : \mathbf{Z}_{12} \to \mathbf{Z}_{18}$ by setting $f([x]_{12}) = [12x]_{18}$. Find the image $f(\mathbf{Z}_{12})$ of f and the factor set $\mathbf{Z}_{12}/f$ of $\mathbf{Z}_{12}$ determined by f and exhibit the one-to-one correspondence between them.

    (b) Define the formula $f : \mathbf{Z}_{12} \to \mathbf{Z}_{12}$ by $f([x]_{12}) = [x]_{12}^2$, for all $[x]_{12} \in \mathbf{Z}_{12}$. Show that the formula f defines a function. Find the image $f(\mathbf{Z}_{12})$ of f and the factor set $\mathbf{Z}_{12}/f$ of $\mathbf{Z}_{12}$ determined by f and exhibit the one-to-one correspondence between them.

15. For the linear transformation $L : \mathbf{R}^3 \to \mathbf{R}^3$ defined by

$$L(x, y, z) = (x + y + z, x + y + z, x + y + z) ,$$

    for all $(x, y, z) \in \mathbf{R}^3$, give a geometric description of the partition of $\mathbf{R}^3$ that is determined by L.

16. For each of the following relations on the given set, determine which of the three conditions of Definition 2.2.1 hold.

    (a) For $a, b \in \mathbf{Z}$, define $a \sim b$ if $a + b$ is even.

    (b) For $a, b \in \mathbf{Z}$, define $a \sim b$ if $a + b$ is odd.

    (c) On $\mathbf{R}^\times$, define $a \sim b$ if $\dfrac{a}{b} \in \mathbf{Q}$.

    (d) On $\mathbf{R}^\times$, define $a \sim b$ if $\dfrac{a}{b} \in \mathbf{Z}$.

17. On the set $\{(a, b)\}$ of all ordered pairs of positive integers, define $(x_1, y_1) \sim (x_2, y_2)$ if $x_1y_2 = x_2y_1$. Show that this defines an equivalence relation.

18. On the set $\mathbf{R}^2$, define $(x_1, y_1) \sim (x_2, y_2)$ if $x_1y_1 = x_2y_2$. Show that $\sim$ is an equivalence relation, and give a geometric description of the equivalence classes of $\sim$.

19. On $\mathbf{C}$, define $z_1 \sim z_2$ if $|z_1| = |z_2|$. Show that $\sim$ is an equivalence relation, and find the equivalence classes of $\sim$.

20. Let $\mathbf{u}$ be a fixed vector in $\mathbf{R}^3$, and assume that $\mathbf{u}$ has length 1. For vectors $\mathbf{v}$ and $\mathbf{w}$, define $\mathbf{v} \sim \mathbf{w}$ if $\mathbf{v} \cdot \mathbf{u} = \mathbf{w} \cdot \mathbf{u}$, where $\cdot$ denotes the standard dot product. Show that $\sim$ is an equivalence relation, and give a geometric description of the equivalence classes of $\sim$.

21. Let $f : S \to T$ be a function. Given an equivalence relation $\simeq$ on T, define $\sim$ on S by setting $x_1 \sim x_2$ if $f(x_1) \simeq f(x_2)$, for all $x_1, x_2 \in S$. Prove that $\sim$ is an equivalence relation on S.

22. Let $f : S \to T$ be an onto function. Let $\{P_\alpha\}_{\alpha \in I}$ be a partition of T. Prove that $\mathcal{P} = \{f^{-1}(P_\alpha) \mid \alpha \in I\}$ is a partition of S.

MORE PROBLEMS: §2.2

23. Define $f : \mathbf{Z}_8 \to \mathbf{Z}_{12}$ by $f([x]_8) = [3x]_{12}$, for all $[x]_8 \in \mathbf{Z}_8$.

    (a) Show that f is a well-defined function. (*Show that if* $x_1 \equiv x_2 \ (mod\ 8)$, *then* $3x_1 \equiv 3x_2 \ (mod\ 12)$.)

    †(b) Find the image $f(\mathbf{Z}_8)$ and the set of equivalence classes $\mathbf{Z}_8/f$ defined by f, and exhibit the one-to-one correspondence between these sets.

24. For each of the following functions defined on the given set S, find $f(S)$ and S/f and exhibit the one-to-one correspondence between them.

    (a) $f : \mathbf{Z}_{12} \to \mathbf{Z}_4 \times \mathbf{Z}_3$ defined by $f([x]_{12}) = ([x]_4, [x]_3)$ for all $[x]_{12} \in \mathbf{Z}_{12}$.

    (b) $f : \mathbf{Z}_{12} \to \mathbf{Z}_2 \times \mathbf{Z}_6$ defined by $f([x]_{12}) = ([x]_2, [x]_6)$ for all $[x]_{12} \in \mathbf{Z}_{12}$.

    (c) $f : \mathbf{Z}_{18} \to \mathbf{Z}_6 \times \mathbf{Z}_3$ defined by $f([x]_{18}) = ([x]_6, [x]_3)$ for all $[x]_{18} \in \mathbf{Z}_{18}$.

25. For $[x]_{15}$, let $f([x]_{15}) = [3x]_5^3$.

    (a) Show that f defines a function from $\mathbf{Z}_{15}^\times$ to $\mathbf{Z}_5^\times$.

    Hint: You may find Problem 1.2.45 to be helpful.

    †(b) Find $f(\mathbf{Z}_{15}^\times)$ and $\mathbf{Z}_{15}^\times/f$ and exhibit the one-to-one correspondence between them.

26. For each of the following relations on $\mathbf{R}$, determine which of the three conditions of Definition 2.2.1 hold.

    †(a) Define $a \sim b$ if $b = a^2$.

    (b) Define $a \sim b$ if $b = \sin(a)$.

    (c) Define $a \sim b$ if $b = a + k\pi$, for some $k \in \mathbf{Z}$.

    †(d) Define $a \sim b$ if $b = a + q\pi$, for some $q \in \mathbf{Q}^+$.

27. For each of the following relations on the given set, determine which of the three conditions of Definition 2.2.1 hold.

    †(a) For $(x_1, y_1), (x_2, y_2) \in \mathbf{R}^2$, define $(x_1, y_1) \sim (x_2, y_2)$ if $2(y_1 - x_1) = 3(y_2 - x_2)$.

    (b) Let P be the set of all people living in North America. For $p, q \in P$, define $p \sim q$ if p and q have the same biological mother.

    †(c) Let P be the set of all people living in North America. For $p, q \in P$, define $p \sim q$ if p is the sister of q.

28. On the set $\mathcal{C}(\mathbf{R})$ of all continuous functions from $\mathbf{R}$ into $\mathbf{R}$, define $f \sim g$ if $f(0) = g(0)$.

    (a) Show that $\sim$ defines an equivalence relation.

    (b) Find a trig function in the equivalence class of $f(x) = x + 1$.

    (c) Find a polynomial of degree 6 in the equivalence class of $f(x) = x + 1$.

29. On $\mathcal{C}[0, 1]$ of all continuous functions from $[0, 1]$ into $\mathbf{R}$, define $f \sim g$ if $\int_0^1 f(x)dx = \int_0^1 g(x)dx$. Show that $\sim$ is an equivalence relation, and that the equivalence classes of $\sim$ are in one-to-one correspondence with the set of all real numbers.

30.†Let $\sim$ be an equivalence relation on the set S. Show that $[a] = [b]$ if and only if $a \sim b$.

2.3 Permutations

This section introduces and studies the last major example that we need before we begin studying groups in Chapter 3. You need to do enough computations so that you will feel comfortable in dealing with permutations.

If you are reading another book along with **Abstract Algebra**, you need to be aware that some authors multiply permutations by reading from left to right, instead of the way we have defined multiplication. Our point of view is that permutations are functions, and we write functions on the left, just as in calculus, so we have to do the computations from right to left.

In the text we noted that if S is any set, and $\mathrm{Sym}(S)$ is the set of all permutations on S, then we have the following properties. (i) If $\sigma, \tau \in \mathrm{Sym}(S)$, then $\tau\sigma \in \mathrm{Sym}(S)$; (ii) $1_S \in \mathrm{Sym}(S)$; (iii) if $\sigma \in \mathrm{Sym}(S)$, then $\sigma^{-1} \in \mathrm{Sym}(S)$. In two of the problems, we need the following definition.

If G is a nonempty subset of $\mathrm{Sym}(S)$, we will say that G is a *group of permutations* if the following conditions hold.

(i) If $\sigma, \tau \in G$, then $\tau\sigma \in G$;

(ii) $1_S \in G$;

(iii) if $\sigma \in G$, then $\sigma^{-1} \in G$.

We will see later that this agrees with Definition 3.6.1 of the text.

SOLVED PROBLEMS: §2.3

17. For the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 6 & 9 & 2 & 4 & 8 & 1 & 3 \end{pmatrix}$, write σ as a product of disjoint cycles. What is the order of σ? Write σ as a product of transpositions. Is σ an even permutation? Compute σ^{-1}.

18. For the permutations $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 1 & 8 & 3 & 6 & 4 & 7 & 9 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 4 & 7 & 2 & 6 & 8 & 9 & 3 \end{pmatrix}$, write each of these permutations as a product of disjoint cycles: σ, τ, $\sigma\tau$, $\sigma\tau\sigma^{-1}$, σ^{-1}, τ^{-1}, $\tau\sigma$, $\tau\sigma\tau^{-1}$.

19. Let $\sigma = (2, 4, 9, 7,)(6, 4, 2, 5, 9)(1, 6)(3, 8, 6) \in S_9$. Write σ as a product of disjoint cycles. What is the order of σ? Compute σ^{-1}.

20. Compute the order of $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 2 & 11 & 4 & 6 & 8 & 9 & 10 & 1 & 3 & 5 \end{pmatrix}$. For $\sigma = (3, 8, 7)$, compute the order of $\sigma\tau\sigma^{-1}$.

21. Prove that if $\tau \in S_n$ is a permutation with order m, then $\sigma\tau\sigma^{-1}$ has order m, for any permutation $\sigma \in S_n$.

22. Show that S_{10} has elements of order 10, 12, and 14, but not 11 or 13.

23. Let S be a set, and let $X \subseteq S$. Let $G = \{\sigma \in \mathrm{Sym}(S) \mid \sigma(X) = X\}$. Prove that G is a group of permutations.

24. Let G be a group of permutations, with $G \subseteq \mathrm{Sym}(S)$, for the set S. Let τ be a fixed permutation in $\mathrm{Sym}(S)$. Prove that

$$\tau G \tau^{-1} = \{\sigma \in \mathrm{Sym}(S) \mid \sigma = \tau\gamma\tau^{-1} \text{ for some } \gamma \in G\}$$

is a group of permutations.

MORE PROBLEMS: §2.3

25. Consider the following permutations in S_7.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 6 & 1 & 7 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 5 & 7 & 4 & 6 & 3 \end{pmatrix}$$

Compute the following products.

†(a) $\sigma\tau$ (b) $\tau\sigma$ †(c) $\sigma\tau\sigma^{-1}$ (d) $\tau\sigma\tau^{-1}$

26.† Using the permutations σ and τ from Problem 25, write each of the permutations $\sigma\tau$, $\tau\sigma$, $\tau^2\sigma$, σ^{-1}, $\sigma\tau\sigma^{-1}$, $\tau\sigma\tau^{-1}$ and $\tau^{-1}\sigma\tau$ as a product of disjoint cycles. Write σ and τ as products of transpositions.

27. Write $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 10 & 5 & 7 & 8 & 2 & 6 & 9 & 1 \end{pmatrix}$ as a product of disjoint cycles and as a product of transpositions. Construct its associated diagram, find its inverse, and find its order.

28. Let $\sigma = (3, 6, 8)(1, 9, 4, 3, 2, 7, 6, 8, 5)(2, 3, 9, 7) \in S_9$.

(a) Write σ as a product of disjoint cycles.

†(b) Is σ an even permutation or an odd permutation?

†(c) What is the order of σ in S_9?

(d) Compute σ^{-1} in S_9.

29. Let $\sigma = (2, 3, 9, 6)(7, 3, 2, 5, 9)(1, 7)(4, 8, 7) \in S_9$.

(a) Write σ as a product of disjoint cycles.

†(b) Is σ an even permutation or an odd permutation?

†(c) What is the order of σ in S_9?

(d) Compute σ^{-1} in S_9.

30. Find a formula for the number of cycles of length m in S_n, for $2 \leq m \leq n$.

Chapter 2 Review Problems

1. For the function $f : \mathbf{Z}_{16} \to \mathbf{Z}_{16}$ defined by $f([x]_{16}) = [x^2]_{16}$, for all $[x]_{16} \in \mathbf{Z}_{16}$, describe the equivalence relation $\sim_f$ on $\mathbf{Z}_{16}$ that is determined by f.

2. Define $f : \mathbf{Z}_7 \to \mathbf{Z}_7$ by $f([x]_7) = [x^3 + 3x - 5]_7$, for all $[x]_7 \in \mathbf{Z}_7$. Is f a one-to-one correspondence?

3. On the set $\mathbf{Q}$ of rational numbers, define $x \sim y$ if $x - y$ is an integer. Show that $\sim$ is an equivalence relation.

4. In S_{10}, let $\alpha = (1, 3, 5, 7, 9)$, $\beta = (1, 2, 6)$, and $\gamma = (1, 2, 5, 3)$. For $\sigma = \alpha\beta\gamma$, write σ as a product of disjoint cycles, and use this to find its order and its inverse. Is σ even or odd?

5. Define the function $\phi : \mathbf{Z}_{17}^{\times} \to \mathbf{Z}_{17}^{\times}$ by $\phi(x) = x^{-1}$, for all $x \in \mathbf{Z}_{17}^{\times}$. Is ϕ one to one? Is ϕ onto? If possible, find the inverse function ϕ^{-1}.

6. (a) Let α be a fixed element of S_n. Show that $\phi_\alpha : S_n \to S_n$ defined by $\phi_\alpha(\sigma) = \alpha\sigma\alpha^{-1}$, for all $\sigma \in S_n$, is a one-to-one and onto function.

   (b) In S_3, let $\alpha = (1, 2)$. Compute ϕ_α.

7. Let S be the set of all $n \times n$ matrices with real entries. For $A, B \in S$, define $A \sim B$ if there exists an invertible matrix P such that $B = PAP^{-1}$. Prove that $\sim$ is an equivalence relation.

8. Show that S_n contains $n(n-1)/2$ transpositions.

Chapter 3

GROUPS

The study of groups, which we begin in this chapter, is usually thought of as the real beginning of abstract algebra. The step from arithmetic to algebra involves starting to use variables, which just represent various numbers. But the operations are still the usual ones for numbers, addition, subtraction, multiplication, and division.

The step from algebra to abstract algebra involves letting the operation act like a variable. At first we will use $*$ or $\cdot$ to represent an operation, to show that $*$ might represent ordinary addition or multiplication, or possibly operations on matrices or functions, or maybe even something quite far from your experience. One of the things we try to do with notation is to make it look familiar, even if it represents something new; very soon we will just write ab instead of $a * b$, assuming that everyone knows the convention that we are using.

Our general approach in the text is to study specific examples before giving an abstract definition. In particular, you have studied the "most typical" groups in Section 2.3. Section 2.3 of the Study Guide includes the definition of a *group of permutations*, a preview of Definition 3.6.1. Theorem 3.6.2 shows that every group is isomorphic to a group of permutations. Here the term "isomorphic to" means that there is a one-to-one correspondence between the two sets that preserves the algebraic structure, so the elements of the two groups behave the same way, but may be named differently. (See Definition 3.4.1 for the formal definition.) You will also see that $\mathbf{Z}$ and $\mathbf{Z}_n$ serve as examples for the class of "cyclic" groups, since Theorem 3.5.2 shows that any cyclic group is isomorphic to $\mathbf{Z}$ or $\mathbf{Z}_n$, for some n. (Recall from Section 1.4 that $\mathbf{Z}_n^\times$ is said to be cyclic if it contains an element $[a]_n$ of multiplicative order $\varphi(n)$, so that it consists of all powers of $[a]_n$.)

If you would like to know more about the history of group theory, I would suggest that you look at the online resource *The MacTutor History of Mathematics archive*. This web site is maintained by St. Andrew's University, in Scotland. In their section on the history of group theory, you will find a discussion of various attempts to find appropriate axioms to describe the notion of a group, which had come up in several different areas of mathematics. There is a close tie to Galois theory, and if you take the time to read the historical background and the notes at the ends of sections in our text, you will begin to understand the connection. The process the ended in the formal definition of a group given in Definition 3.1.4 took about fifty years. No wonder it may seem a bit mysterious at first!

3.1 Definition of a Group

This section contains the definitions of a *binary operation*, a *group*, an *abelian group*, and a *finite group*. These definitions provide the language you will be working with, and you simply *must* know this language. Try to learn it so well that you don't have even a trace of an accent!

Loosely, a group is a set on which it is possible to define an associative binary operation that has an identity element, and which includes inverses for each of its elements. The precise statement is given in Definition 3.1.4; you must pay careful attention to each part, especially the quantifiers ("for all", "for each", "there exists"), which must be stated in exactly the right order.

From one point of view, the axioms for a group give us just what we need to work with equations involving the operation in the group. For example, one of the rules you are used to states that you can multiply both sides of an equation by equal quantities, and the equation will still hold. This still works for the operation in a group, since if x and y are elements of a group G, and $x = y$, then $a \cdot x = a \cdot y$, for any element a in G. This is a part of the guarantee that comes with the definition of a binary operation. It is important to note that on both sides of the equation, a is multiplied on the left. We could also guarantee that $x \cdot a = y \cdot a$, but we can't guarantee that $a \cdot x = y \cdot a$, since the operation in the group may not satisfy the commutative law.

The existence of inverses allows cancellation (see Proposition 3.1.7 for the precise statement). Remember that in a group there is no mention of division, so whenever you are tempted to write $a \div b$ or a/b, you must write $a \cdot b^{-1}$ or $b^{-1} \cdot a$. If you are careful about the side on which you multiply, and don't fall victim to the temptation to divide, you can be pretty safe in doing the familiar things from high school algebra when working with an equation that involves elements of a group.

Understanding and remembering the definitions will give you one level of understanding. The next level comes from knowing some good examples. The third level of understanding comes from using the definitions to prove various facts about groups.

Here are a few of the important examples. First, the sets of numbers $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ form groups under addition. Next, the sets $\mathbf{Q}^\times$, $\mathbf{R}^\times$, and $\mathbf{C}^\times$ of nonzero numbers form groups under multiplication. The sets $\mathbf{Z}$ and $\mathbf{Z}_n$ are groups under addition, while $\mathbf{Z}_n^\times$ is a group under multiplication. It is common to just list these sets as groups, without mentioning their operations, since in each case only one of the two familiar operations can be used to make the set into a group. Similarly, the set $M_n(\mathbf{R})$ of all $n \times n$ matrices with entries in $\mathbf{R}$ is a group under addition, but not multiplication, while the set $\mathrm{GL}_n(\mathbf{R})$ of all invertible $n \times n$ matrices with entries in $\mathbf{R}$ is a group under multiplication, but not under addition. There shouldn't be any confusion in just listing these as groups, without specifically mentioning which operation is used.

In the study of finite groups, the most important examples come from groups of matrices. I should still mention that the original motivation for studying groups came from studying sets of permutations, and so the symmetric group S_n still has an important role to play.

We give multiplication tables for three different groups of order 8. Various problems in this section and later sections refer to these groups.

Table 3.1: Multiplication Table for O

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	ab	a^2b	a^3b	e	a	a^2	a^3
ab	ab	a^2b	a^3b	b	a	a^2	a^3	e
a^2b	a^2b	a^3b	b	ab	a^2	a^3	e	a
a^3b	a^3b	b	ab	a^2b	a^3	e	a	a^2

Table 3.2: Multiplication Table for P

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

Table 3.3: Multiplication Table for Q

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	a^2	a	e	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	e
a^2b	a^2b	ab	b	a^3b	e	a^3	a^2	a
a^3b	a^3b	a^2b	ab	b	a	e	a^3	a^2

SOLVED PROBLEMS: §3.1

25. Use the dot product to define a multiplication on $\mathbf{R}^3$. Does this make $\mathbf{R}^3$ into a group?

26. For vectors (x_1, y_1, z_1) and (x_2, y_2, z_2) in $\mathbf{R}^3$, the cross product is defined by

$$(x_1, y_1, z_1) \times (x_2, y_2, z_2) = (y_1 z_2 - z_1 y_2,\ z_1 x_2 - x_1 z_2,\ x_1 y_2 - y_1 x_2)\ .$$

Is $\mathbf{R}^3$ a group under this multiplication?

27. On the set $G = \mathbf{Q}^\times$ of nonzero rational numbers, define a new multiplication by $a * b = \dfrac{ab}{2}$, for all $a, b \in G$. Show that G is a group under this multiplication.

28. Write out the multiplication table for $\mathbf{Z}_{18}^\times$.

29. Write out the multiplication table for $\mathbf{Z}_{15}^\times$.

30. Let G be a group, and suppose that a and b are any elements of G. Show that if $(ab)^2 = a^2 b^2$, then $ba = ab$.

31. Let G be a group, and suppose that a and b are any elements of G. Show that $(aba^{-1})^n = ab^n a^{-1}$, for any positive integer n.

32. In Definition 3.1.4, replace condition (iii) with the condition that there exists $e \in G$ such that $e \cdot a = a$ for all $a \in G$, and replace condition (iv) with the condition that for each $a \in G$ there exists $a' \in G$ with $a' \cdot a = e$. Prove that these weaker conditions (given only on the left) still imply that G is a group.

33. Problem 32 shows that in the definition of a group it is sufficient to require the existence of a left identity element and the existence of left inverses. Give an example to show that it is *not* sufficient to require the existence of a left identity element together with the existence of *right* inverses.

34. Let F be the set of all **fractional linear transformations** of the complex plane. That is, F is the set of all functions $f(z) : \mathbf{C} \to \mathbf{C}$ of the form $f(z) = \dfrac{az + b}{cz + d}$, where the coefficients a, b, c, d are integers with $ad - bc = 1$. Show that F forms a group if we take the operation to be composition of functions.

35. Let $G = \{x \in \mathbf{R} \mid x > 1\}$ be the set of all real numbers greater than 1. For $x, y \in G$, define $x * y = xy - x - y + 2$.

    (a) Show that the operation $*$ is closed on G.

    (b) Show that the associative law holds for $*$.

    (c) Show that 2 is the identity element for the operation $*$.

    (d) Show that for element $a \in G$ there exists an inverse $a^{-1} \in G$.

MORE PROBLEMS: §3.1

36.† For each binary operation $*$ given below, determine whether or not $*$ defines a group structure on the given set. If not, list the group axioms that fail to hold.

(a) Define $*$ on $\mathbf{Z}$ by $a * b = \min\{a, b\}$.

(b) Define $*$ on $\mathbf{Z}^+$ by $a * b = \min\{a, b\}$.

(c) Define $*$ on $\mathbf{Z}^+$ by $a * b = \max\{a, b\}$.

37.† For each binary operation $*$ given below, determine whether or not $*$ defines a group structure on the given set. If not, list the group axioms that fail to hold.

(a) Define $*$ on $\mathbf{R}$ by $x * y = x + y - 1$.

(b) Define $*$ on $\mathbf{R}^\times$ by $x * y = xy + 1$.

(c) Define $*$ on $\mathbf{Q}^+$ by $x * y = \dfrac{1}{x} + \dfrac{1}{y}$.

38. For each binary operation $*$ given below, determine whether or not $*$ defines a group structure on the given set. If not, list the group axioms that fail to hold.

(a) Define $*$ on $\mathbf{Z}$ by $x * y = x^2y^3$.

(b) Define $*$ on $\mathbf{Z}^+$ by $x * y = 2^{xy}$.

(c) Define $*$ on $\mathbf{Z}^+$ by $x * y = x^y$.

39.† For each binary operation $*$ given below, determine whether or not $*$ defines a group structure on the given set. If not, list the group axioms that fail to hold.

(a) Use matrix multiplication to define $*$ on $\left\{ \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} \middle| x, y \in \mathbf{R} \right\}$.

(b) Define $*$ on $\mathbf{R}^2$ by $(x_1, y_1) * (x_2, y_2) = (x_1x_2, y_1x_2 + y_2)$.

40. Let G be a group, and suppose that $a, b, c \in G$. Solve the equation $axc = b$.

41. In each of the groups O, P, Q in the tables in Section 3.1 of the *Study Guide*, find the inverse of each of the eight elements.

42. In each of the groups O, P, Q in the tables in Section 3.1 of the *Study Guide*, solve the equations $ax = b$ and $bx = a$.

43. Let G be a group with operation $\cdot$ and let $a \in G$. Define a new operation $*$ on the set G by $x * y = x \cdot a \cdot y$, for all $x, y \in G$. Show that G is a group under the operation $*$.

Note: Problem 27 is a special case of this result.

44.† Let G be a group, with operation $\cdot$. Define a new operation on G by setting $x * y = y$, for $x, y \in G$. Determine which group axioms hold for this operation.

45. Let $\mathcal{C}[0, 1]$ be the set of all continuous functions from $[0, 1]$ to $\mathbf{R}$. Show that $\mathcal{C}[0, 1]$ is a group under addition of functions: $[f + g](x) = f(x) + g(x)$, for $f(x), g(x) \in \mathcal{C}[0, 1]$.

46. Let G be a nonempty finite set with an associative binary operation $\cdot$. Exercise 3.1.20 shows that if the cancellation law holds on both sides, then G is a group. Give an example in which the cancellation law holds on one side, but G is not a group.

47. Let T be the set of functions $t_{c,d} : \mathbf{R}^2 \to \mathbf{R}^2$ defined by $t_{c,d}(x_1, x_2) = (x_1 + c, x_2 + d)$, where c, d are any elements of $\mathbf{R}$. Show that T is a group under composition of functions.

48. Let G be a group. For $x, y \in G$, define $x \sim y$ if there exists some element $a \in G$ such that $y = axa^{-1}$. Show that $\sim$ defines an equivalence relation on G.

    Note: This is a general case of Exercise 2.3.15 in the text, where the problem is stated for the group $G = S_n$.

3.2 Subgroups

Many times a group is defined by looking at a subset of a known group. If the subset is a group in its own right, using the same operation as the larger set, then it is called a *subgroup*. For instance, any group of permutations is a subgroup of $\mathrm{Sym}(S)$, for some set S. Any group of $n \times n$ matrices (with entries in $\mathbf{R}$) is a subgroup of $\mathrm{GL}_n(\mathbf{R})$.

If the idea of a subgroup reminds you of studying subspaces in your linear algebra course, you are right. If you only look at the operation of addition in a vector space, it forms an abelian group, and any subspace is automatically a subgroup. Now might be a good time to pick up your linear algebra text and review vector spaces and subspaces.

Lagrange's theorem (Theorem 3.2.10) is a very important result. It states that in a finite group the number of elements in any subgroup must be a divisor of the total number of elements in the group. This is a useful fact to know when you are looking for subgroups in a given group. In particular, any group of prime order contains no proper nontrivial subgroups and must therefore be cyclic.

It is also important to remember that every element a in a group defines a subgroup $\langle a \rangle$, consisting of all powers (positive and negative) of the element. This subgroup has $o(a)$ elements, where $o(a)$ is the order of a. If the group is finite, then to find $\langle a \rangle$ you only need to calculate the positive powers of a, since in that case the inverse a^{-1} of any element can be expressed in the form a^n, for some $n > 0$.

Lagrange's Theorem implies that the order of any element of a finite group is a divisor of the order of the group. This can be extremely helpful, as the following example shows.

Suppose that we are attempting to show that $[2]_{17}$ is a generator of the group $\mathbf{Z}_{17}^{\times}$. Since $|\mathbf{Z}_{17}^{\times}| = 17$, the possible orders of $[2]$ are 2, 4, 8, or 16. We do not have to calculate *all* powers of $[2]$ to find its order. We have $[2]^2 = [4]$, $[2]^4 = [16] = [-1]$, so $[2]$ does not have order 2 or 4, but the $[2]^8 = ([2]^4)^2 = [-1]^2 = [1]$ so $[2]$ has order 8, showing that $[2]$ is *not* a generator. A similar argument shows that $[3]^2 = [9]$, $[3]^4 = [-4]$, and $[3]^8 = [16]$, so $[3]$ is a generator of $\mathbf{Z}_{17}^{\times}$ since it must have order 16.

SOLVED PROBLEMS: §3.2

28. In $\mathbf{Z}_n$, show that if $\gcd(a, n) = d$, then $\langle [a]_n \rangle = \langle [d]_n \rangle$.

    Note: This result is very useful when you are trying to find cyclic subgroups of $\mathbf{Z}_n$.

29. Find all cyclic subgroups of $\mathbf{Z}_{12}$.

30. Find all cyclic subgroups of $\mathbf{Z}_{24}^{\times}$.

31. In $\mathbf{Z}_{20}^{\times}$, find two subgroups of order 4, one that is cyclic and one that is not cyclic.

32. (a) Find the cyclic subgroup of S_7 generated by the element $(1, 2, 3)(5, 7)$.

    (b) Find a subgroup of S_7 that contains 12 elements. You do not have to list all of the elements if you can explain why there must be 12, and why they must form a subgroup.

33. Let G be an abelian group, and let n be a fixed positive integer. Show that

$$N = \{g \in G \mid g = a^n \text{ for some } a \in G\}$$

    is a subgroup of G.

34. Let K be the following subset of $\mathrm{GL}_2(\mathbf{R})$.

$$K = \left\{ \left[\begin{array}{cc} a & b \\ c & d \end{array} \right] \in \mathrm{GL}_2(\mathbf{R}) \middle| \, d = a, \;\; c = -2b \right\}$$

    Show that K is a subgroup of $\mathrm{GL}_2(\mathbf{R})$.

35. In $G = \mathbf{Z}_{21}^{\times}$, show that $H = \{[x]_{21} \mid x \equiv 1 \pmod 3\}$ and $K = \{[x]_{21} \mid x \equiv 1 \pmod 7\}$ are subgroups of G.

36. Suppose that p is a prime number of the form $p = 2^n + 1$.

    (a) Show that in $\mathbf{Z}_p^{\times}$ the order of $[2]_p$ is $2n$.

    (b) Use part (a) to prove that n must be a power of 2.

37. In the multiplicative group $\mathbf{C}^{\times}$ of complex numbers, find the order of the elements $-\dfrac{\sqrt{2}}{2} + \dfrac{\sqrt{2}}{2}i$ and $-\dfrac{\sqrt{2}}{2} - \dfrac{\sqrt{2}}{2}i$.

38. In the group $G = \mathrm{GL}_2(\mathbf{R})$ of invertible 2×2 matrices with real entries, show that

$$H = \left\{ \left[\begin{array}{cc} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{array} \right] \middle| \, \theta \in \mathbf{R} \right\}$$

    is a subgroup of G.

39. Compute the centralizer in $\mathrm{GL}_2(\mathbf{R})$ of the matrix $\left[\begin{array}{cc} 2 & 1 \\ 1 & 1 \end{array} \right]$.

40. Prove that any infinite group has infinitely many subgroups.

MORE PROBLEMS: §3.2

41.† Let G be a group, and let $a \in G$, with $a \neq e$. Prove or disprove these statements.

(a) The element a has order 2 if and only if $a^2 = e$.

(b) The element a has order 3 if and only if $a^3 = e$.

(c) The element a has order 4 if and only if $a^4 = e$.

42. In each of the groups O, P, Q in the tables in Section 3.1 of the *Study Guide*, find $\langle b \rangle$ and $\langle ab \rangle$. That is, find the cyclic subgroups generated by b and ab.

43.† Is $\{(x, y) \in \mathbf{R}^2 \mid y = x^2\}$ a subgroup of $\mathbf{R}^2$?

44.† Is $\{(x, y) \in \mathbf{R}^2 \mid x, y \in \mathbf{Z}\}$ a subgroup of $\mathbf{R}^2$?

45. Let $G = \mathcal{C}[0, 1]$, the group defined in Problem 3.1.45. Let P_n denote the subset of functions in G of the form $a_n x^n + \ldots + a_1 x + a_0$, where the coefficients a_i all belong to $\mathbf{R}$. Prove that P_n is a subgroup of G.

46. Let $G = \mathcal{C}[0, 1]$, the group defined in Problem 3.1.45. Let X be any subset of $[0, 1]$. Show that $\{f \in \mathcal{C}[0, 1] \mid f(x) = 0 \text{ for all } x \in X\}$ is a subgroup of G.

47. Show that the group T defined in Problem 3.1.47 is a subgroup of $\mathrm{Sym}(\mathbf{R}^2)$.

48. In $G = S_5$, let $H = \{\sigma \in S_5 \mid \sigma(5) = 5\}$. Find $|H|$; show that H is a subgroup of G.

49. Let G be a group, and let H, K be subgroups of G.

(a) Show that $H \cup K$ is a subgroup of G if and only if either $H \subseteq K$ or $K \subseteq H$.

(b) Show that a group cannot be the union of 2 proper subgroups. Give an example to show that it *can* be a union of 3 proper subgroups.

50. Let G be a group, let H be any subgroup of G, and let a be a fixed element of G. Define $aHa^{-1} = \{g \in G \mid g = aha^{-1} \text{ for some } h \in H\}$. Show that aHa^{-1} is a subgroup of G.

51.† Let G be a group, with a subgroup $H \subseteq G$. Define $N(H) = \{g \in G \mid gHg^{-1} = H\}$. Show that $N(H)$ is a subgroup of G that contains H.

52. Let G be a group.

(a) Show that if H_1 and H_2 are two different subgroups of G with $|H_1| = |H_2| = 3$, then $H_1 \cap H_2 = \{e\}$.

(b) Show that G has an even number of elements of order 3.

(c) Show that the number of elements of order 5 in G must be a multiple of 4.

(d) Is the number of elements of order 4 in G a multiple of 3? Give a proof or a counterexample.

53.† In each of the groups O, P, Q in the tables in Section 3.1 of the *Study Guide*, find the centralizers $C(a)$ and $C(ab)$. That is, find the elements that commute with a, and then find the elements that commute with ab.

54. Find the centers of the groups P and Q given in the tables in Section 3.1.

55. In $G = \mathrm{GL}_2(\mathbf{R})$, find the centralizer $C\left(\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\right)$.

56. Let G be a group, and let $a, b \in G$. Show that if either $ab \in C(a)$ or $ba \in C(a)$, then $b \in C(a)$.

57. Let G be an abelian group, and let $G_n = \{x \in G \mid x^n = e\}$.

(a) Show that G_n is a subgroup of G.

Note: This is a generalization of Exercise 3.2.13 in the text.

(b) Let $G = \mathbf{Z}_{11}^{\times}$. Find G_n for $n = 2, 3, \ldots, 10$.

58.† (a) Characterize the elements of $\mathrm{GL}_2(\mathbf{R})$ that have order 2.

(b) Which of the elements in part (a) are upper triangular?

(c) Is $\{A \in \mathrm{GL}_2(\mathbf{R}) \mid A^2 = I\}$ a subgroup of $\mathrm{GL}_2(\mathbf{R})$?

(d) Does the set of upper triangular matrices in $\{A \in \mathrm{GL}_2(\mathbf{R}) \mid A^2 = I\}$ form a subgroup of $\mathrm{GL}_2(\mathbf{R})$?

59. †(a) Characterize the elements of order 3 in $\mathrm{GL}_2(\mathbf{R})$ that have the form $\begin{bmatrix} a & b \\ c & 0 \end{bmatrix}$. Show that there are infinitely many such elements.

(b) Show that there are no upper triangular matrices in $\mathrm{GL}_2(\mathbf{R})$ that have order 3.

60. Let $G = \mathbf{R}^+$, and for any integer $n > 1$ define $H_n = \{x \in \mathbf{R}^+ \mid x^n \in \mathbf{Q}\}$.

(a) Show that H_n is a subgroup of G.

(b) Show that $\mathbf{Q}^+ \subset H_2 \subset H_4 \subset \cdots \subset H_{2^n} \subset \cdots$ is an infinite ascending chain of subgroups of G.

61.† In $\mathrm{GL}_2(\mathbf{R})$, let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, which has infinite order, and let $B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Find the order of B, and find the order of AB.

62. Let K be a subgroup of $\mathbf{R}^{\times}$. Show that $H = \{A \in \mathrm{GL}_n(\mathbf{R}) \mid \det(A) \in K\}$ is a subgroup of $\mathrm{GL}_n(\mathbf{R})$.

63. Let $A = \{f_{m,b} \mid m \neq 0 \text{ and } f_{m,b}(x) = mx + b \text{ for all } x \in \mathbf{R}\}$, which is shown to be a group in Exercise 3.1.10.

(a) Show that $\{f_{1,n} \mid n \in \mathbf{Z}\}$ is a cyclic subgroup of A.

(b) Find the cyclic subgroup $\langle f_{2,1} \rangle$ of A generated by the mapping $f_{2,1}(x) = 2x + 1$.

64.† (a) Find the cyclic subgroup of S_6 generated by the element $(1,2,3)(4,5,6)$.

(b) Find the smallest subgroup of S_6 that contains $(1,2,3)$ and $(4,5,6)$.

65. (a) What are the possibilities for the order of an element of $\mathbf{Z}_{27}^{\times}$? Explain your answer.

(b) Show that $\mathbf{Z}_{27}^{\times}$ is a cyclic group.

3.3 Constructing Examples

The most important result in this section is Proposition 3.3.7, which shows that the set of all invertible $n \times n$ matrices forms a group, in which we can allow the entries in the matrix to come from any field. This includes matrices with entries in the field $\mathbf{Z}_p$, for any prime number p, and this allows us to construct very interesting finite groups as subgroups of $\mathrm{GL}_n(\mathbf{Z}_p)$.

The second construction in this section is the direct product, which takes two known groups and constructs a new one, using ordered pairs. This can be extended to n-tuples, where the entry in the ith component comes from a group G_i, and n-tuples are multiplied component-by-component. This generalizes the construction of n-dimensional vector spaces (that case is much simpler since every entry comes from the same set, and the same operation is used in each component).

SOLVED PROBLEMS: §3.3

From this point on, if the modulus n is fixed throughout the problem, we will write a rather than $[a]_n$ for elements of $\mathbf{Z}_n$.

19. Show that $\mathbf{Z}_5 \times \mathbf{Z}_3$ is a cyclic group, and list all of the generators of the group.

20. Find the order of the element $([9]_{12}, [15]_{18})$ in the group $\mathbf{Z}_{12} \times \mathbf{Z}_{18}$.

21. Find two groups G_1 and G_2 whose direct product $G_1 \times G_2$ has a subgroup that is not of the form $H_1 \times H_2$, for subgroups $H_1 \subseteq G_1$ and $H_2 \subseteq G_2$.

22. In the group $G = \mathbf{Z}_{36}^{\times}$, let $H = \{[x] \mid x \equiv 1 \pmod 4\}$ and $K = \{[y] \mid y \equiv 1 \pmod 9\}$. Show that H and K are subgroups of G, and find the subgroup HK.

23. Let F be a field, and let H be the subset of $\mathrm{GL}_2(F)$ consisting of all invertible upper triangular matrices. Show that H is a subgroup of $\mathrm{GL}_2(F)$.

24. Let p be a prime number.

(a) Show that the order of the general linear group $\mathrm{GL}_2(\mathbf{Z}_p)$ is $(p^2-1)(p^2-p)$.

Hint: Count the number of ways to construct two linearly independent rows.

(b) Show that the subgroup of $\mathrm{GL}_2(\mathbf{Z}_p)$ consisting of all invertible upper triangular matrices has order $(p-1)^2 p$.

25. Find the order of the element $A = \begin{bmatrix} i & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -i \end{bmatrix}$ in the group $\mathrm{GL}_3(\mathbf{C})$.

26. Let G be the subgroup of $\mathrm{GL}_2(\mathbf{R})$ defined by

$$G = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| \, m \neq 0 \right\} .$$

Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$. Find the centralizers $C(A)$ and $C(B)$, and show that $C(A) \cap C(B) = Z(G)$, where $Z(G)$ is the center of G.

27. Compute the centralizer in $\mathrm{GL}_2(\mathbf{Z}_3)$ of the matrix $\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$.

28. Compute the centralizer in $\mathrm{GL}_2(\mathbf{Z}_3)$ of the matrix $\begin{bmatrix} 1 & -1 \\ -1 & 0 \end{bmatrix}$.

29. Let H be the following subset of the group $G = \mathrm{GL}_2(\mathbf{Z}_5)$.

$$H = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \in \mathrm{GL}_2(\mathbf{Z}_5) \middle| \, m, b \in \mathbf{Z}_5, \ m = \pm 1 \right\}$$

(a) Show that H is a subgroup of G with 10 elements.

(b) Show that if we let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$, then $BA = A^{-1}B$.

(c) Show that every element of H can be written uniquely in the form $A^i B^j$, where $0 \leq i < 5$ and $0 \leq j < 2$.

30. Let H and K be subgroups of the group G. Prove that HK is a subgroup of G if and only if $KH \subseteq HK$.

Note: This result strengthens Proposition 3.3.2.

MORE PROBLEMS: §3.3

31.† What is the order of $([15]_{24}, [25]_{30})$ in the group $\mathbf{Z}_{24} \times \mathbf{Z}_{30}$? What is the largest possible order of an element in $\mathbf{Z}_{24} \times \mathbf{Z}_{30}$?

32.† Find the order of each element of the group $\mathbf{Z}_4 \times \mathbf{Z}_4^{\times}$.

33.† Check the order of each element of the quaternion group in Example 3.3.7 by using the matrix form of the element.

34. Let H and K be finite subgroups of the group G. Show that if $|H|$ and $|K|$ are relatively prime, then $H \cap K = \{e\}$.

35.† Let $G = \mathbf{Z}_{10}^{\times} \times \mathbf{Z}_{10}^{\times}$.

(a) If $H = \langle (3,3) \rangle$ and $K = \langle (3,7) \rangle$, list the elements of HK.

(b) If $H = \langle (3,3) \rangle$ and $K = \langle (1,3) \rangle$, list the elements of HK.

36. In $G = \mathbf{Z}_{16}^{\times}$, let $H = \langle 3 \rangle$ and $K = \langle -1 \rangle$. Show that $HK = G$ and $H \cap K = \{1\}$.

37.† In $G = \mathbf{Z}_{15}^{\times}$, find subgroups H and K with $|H| = 4$, $|K| = 2$, $HK = G$, and $H \cap K = \{1\}$.

38. Let G be an abelian group with $|G| = 60$. Show that if $a, b \in G$ with $o(a) = 4$ and $o(b) = 6$, then $a^2 = b^3$.

39. Let G be a group, with subgroup H. Show that $K = \{(x, x) \in G \times G \mid x \in H\}$ is a subgroup of $G \times G$.

40. For groups G_1 and G_2, find the center of $G_1 \times G_2$ in terms of the centers $Z(G_1)$ and $Z(G_2)$.

41.† Find the orders of $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ and $\begin{bmatrix} 1 & 2 \\ 4 & 3 \end{bmatrix}$ in $\mathrm{GL}_2(\mathbf{Z}_5)$.

42. Let $K = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \in \mathrm{GL}_2(\mathbf{Z}_5) \,\middle|\, m, b \in \mathbf{Z}_5,\ m \neq 0 \right\}$.

(a) Show that K is a subgroup of $\mathrm{GL}_2(\mathbf{Z}_5)$ with $|K| = 20$.

†(b) Show, by finding the order of each element in K, that K has elements of order 2 and 5, but no element of order 10.

43. Let H be the subgroup of upper triangular matrices in $\mathrm{GL}_2(\mathbf{Z}_3)$. Note that $|H| = 12$.

(a) Let $A = \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}$ and $B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$. Show that $o(A) = 6$ and $o(B) = 2$.

(b) Show that $BA = A^{-1}B$.

44. Let $H = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \,\middle|\, a, b, c \in \mathbf{Z}_2 \right\}$. Show that H is a subgroup of $\mathrm{GL}_3(\mathbf{Z}_2)$. Is H an abelian group?

45.† Find the cyclic subgroup of $\mathrm{GL}_4(\mathbf{Z}_2)$ generated by $\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$.

46. Let F be a field. Recall that a matrix $A \in \mathrm{GL}_n(F)$ is said to be **orthogonal** if A is invertible and $A^{-1} = A^T$, where A^T denotes the transpose of A.

(a) Show that the set of orthogonal $n \times n$ matrices is a subgroup of $\mathrm{GL}_n(F)$.

(b) Show that in $\mathrm{GL}_2(\mathbf{Z}_2)$ the only orthogonal matrices are $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

47.† List the orthogonal matrices in $\mathrm{GL}_2(\mathbf{Z}_3)$ and find the order of each one.

3.4 Isomorphisms

A one-to-one correspondence $\phi : G_1 \to G_2$ between groups G_1 and G_2 is called a group isomorphism if $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G_1$. The function ϕ can be thought of as simply renaming the elements of G_1, since it is one-to-one and onto. The condition that $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G_1$ makes certain that multiplication can be done in either group and the transferred to the other, since the inverse function ϕ^{-1} also respects the operations in the two groups.

In terms of the respective group multiplication tables for G_1 and G_2, the existence of an isomorphism guarantees that there is a way to set up a correspondence between the elements of the groups in such a way that the group multiplication tables will look exactly the same.

From an algebraic perspective, we should think of isomorphic groups as being essentially the same. The problem of finding all abelian groups of order 8 is impossible to solve, because there are infinitely many possibilities. But if we ask for a list of abelian groups of order 8 that comes with a guarantee that *any* possible abelian group of order 8 must be isomorphic to one of the groups on the list, then the question becomes manageable. In fact, we can show (in Section 7.5) that the answer to this particular question is the list $\mathbf{Z}_8$, $\mathbf{Z}_4 \times \mathbf{Z}_2$, $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$. In this situation we would usually say that we have found all abelian groups of order 8, *up to isomorphism*.

To show that two groups G_1 and G_2 are isomorphic, you should actually produce an isomorphism $\phi : G_1 \to G_2$. To decide on the function to use, you probably need to see some similarity between the group operations.

In some ways it is harder to show that two groups are *not* isomorphic. If you can show that one group has a property that the other one does not have, then you can decide that two groups are not isomorphic (provided that the property would have been transferred by any isomorphism). Suppose that G_1 and G_2 are isomorphic groups. If G_1 is abelian, then so is G_2; if G_1 is cyclic, then so is G_2. Furthermore, for each positive integer n, the two groups must have exactly the same number of elements of order n. Each time you meet a new property of groups, you should ask whether it is preserved by any isomorphism.

SOLVED PROBLEMS: §3.4

29. Show that $\mathbf{Z}_{17}^{\times}$ is isomorphic to $\mathbf{Z}_{16}$.

30. Is $\mathbf{Z}_{16}^{\times}$ isomorphic to $\mathbf{Z}_4 \times \mathbf{Z}_2$?

31. Prove that $\mathbf{Z}_{24}^{\times}$ is not isomorphic to $\mathbf{Z}_{16}^{\times}$.

32. Let $\phi : \mathbf{R}^{\times} \to \mathbf{R}^{\times}$ be defined by $\phi(x) = x^3$, for all $x \in \mathbf{R}$. Show that ϕ is a group isomorphism.

33. Let G_1, G_2, H_1, H_2 be groups, and suppose that $\theta_1 : G_1 \to H_1$ and $\theta_2 : G_2 \to H_2$ are group isomorphisms. Define $\phi : G_1 \times G_2 \to H_1 \times H_2$ by $\phi(x_1, x_2) = (\theta_1(x_1), \theta_2(x_2))$, for all $(x_1, x_2) \in G_1 \times G_2$. Prove that ϕ is a group isomorphism.

34. Prove that the group $\mathbf{Z}_7^\times \times \mathbf{Z}_{11}^\times$ is isomorphic to the group $\mathbf{Z}_6 \times \mathbf{Z}_{10}$.

35. Define $\phi : \mathbf{Z}_{30} \times \mathbf{Z}_2 \to \mathbf{Z}_{10} \times \mathbf{Z}_6$ by $\phi([n]_{30}, [m]_2) = ([n]_{10}, [4n + 3m]_6)$, First prove that ϕ is a well-defined function, and then prove that ϕ is a group isomorphism.

36. Let G be a group, and let H be a subgroup of G. Prove that if a is any element of G, then the subset

$$aHa^{-1} = \{g \in G \mid g = aha^{-1} \text{ for some } h \in H\}$$

is a subgroup of G that is isomorphic to H.

37. Let G, G_1, G_2 be groups. Prove that if $G_1 \times G_2$ is isomorphic to G, then there are subgroups H and K in G such that $H \cap K = \{e\}$, $HK = G$, and $hk = kh$ for all $h \in H$ and $k \in K$.

38. Let G be an abelian group with subgroups H and K. Prove that if $HK = G$ and $H \cap K = \{e\}$, then $G \cong H \times K$.

39. Show that for any prime number p, the subgroup of diagonal matrices in $\mathrm{GL}_2(\mathbf{Z}_p)$ is isomorphic to $\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$.

40. (a) In the group $G = \mathrm{GL}_2(\mathbf{R})$ of invertible 2×2 matrices with real entries, show that

$$H = \left\{ \left[\begin{array}{cc} a_{11} & a_{12} \\ a_{21} & a_{22} \end{array} \right] \in \mathrm{GL}_2(\mathbf{R}) \middle| \, a_{11} = 1,\ a_{21} = 0,\ a_{22} = 1 \right\}$$

is a subgroup of G.

(b) Show that H is isomorphic to the group $\mathbf{R}$ of all real numbers, under addition.

41. Let G be the subgroup of $\mathrm{GL}_2(\mathbf{R})$ defined by

$$G = \left\{ \left[\begin{array}{cc} m & b \\ 0 & 1 \end{array} \right] \middle| \, m \neq 0 \right\} .$$

Show that G is not isomorphic to the direct product $\mathbf{R}^\times \times \mathbf{R}$.

42. Let H be the following subgroup of group $G = \mathrm{GL}_2(\mathbf{Z}_3)$.

$$H = \left\{ \left[\begin{array}{cc} m & b \\ 0 & 1 \end{array} \right] \in \mathrm{GL}_2(\mathbf{Z}_3) \middle| \, m, b \in \mathbf{Z}_3,\ m \neq 0 \right\}$$

Show that H is isomorphic to the symmetric group S_3.

MORE PROBLEMS: §3.4

43.† Let a, b be elements of a group G, with $o(b) = 2$ and $ba = a^2b$. Find $o(a)$.

44.† How many different isomorphisms are there from $\mathbf{Z}_6$ onto $\mathbf{Z}_2 \times \mathbf{Z}_3$?

45.† How many different isomorphisms are there from $\mathbf{Z}_{12}$ onto $\mathbf{Z}_4 \times \mathbf{Z}_3$?

46.† Is $\mathbf{Z}_{24}^\times$ isomorphic to $\mathbf{Z}_{30}^\times$? Give a complete explanation for your answer.

47. Let G be the subgroup of $\mathrm{GL}_2(\mathbf{Z}_{11})$ consisting of all matrices of the form $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$. Show that G is isomorphic to the additive group $\mathbf{Z}_{11}$.

48. Prove that the group $2\mathbf{Z}$ of even integers is isomorphic to the group $\mathbf{Z}$ of all integers.

49. Let $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbf{Z}_3) \,\middle|\, b = c = 0 \right\}$. Show that $G \cong \mathbf{Z}_2 \times \mathbf{Z}_2$.

50. (a) Write out the group table for $\mathbf{Z}_4 \times \mathbf{Z}_2$, in multiplicative form, using $a = (1, 0)$ and $b = (0, 1)$. *Note:* The instructions just mean that you should to write xy instead of $x + y$ to indicate the result of the group operation applied to elements x and y.

(b) Show that $\mathbf{Z}_4 \times \mathbf{Z}_2$ is isomorphic to the group O from the table in Section 3.1.

51. Write out the multiplication table for $\mathbf{Z}_{16}^\times$, using $a = 3$ and $b = -1$. Use Problem 50 to show that $\mathbf{Z}_{16}^\times \cong \mathbf{Z}_4 \times \mathbf{Z}_2$.

52. Use Problem 3.3.36 and Problem 38 to show that $\mathbf{Z}_{16}^\times \cong \mathbf{Z}_4 \times \mathbf{Z}_2$.

53. Show that $G = \{\sigma \in S_5 \mid \sigma(5) = 5\}$ is isomorphic to S_4.

54.† On $\mathbf{R}$, define a new operation by $x * y = x + y - 1$. Show that the group $G = (\mathbf{R}, *)$ is isomorphic to $(\mathbf{R}, +)$. *Note:* The group G is defined in Problem 3.1.37 (a).

55.† Show that the group $\mathbf{Q}$ is not isomorphic to the group $\mathbf{Q}^+$.

56. Let G be a group with operation $\cdot$ and let $a \in G$. Define a new operation $*$ on the set G by $x * y = x \cdot a \cdot y$, for all $x, y \in G$. (This is the group defined in Problem 3.1.43.) Show that $(G, *)$ is isomorphic to $(G, \cdot)$.

57. Let $G = \{x \in \mathbf{R} \mid x > 1\}$ be the set of all real numbers greater than 1. For $x, y \in G$, define $x * y = xy - x - y + 2$. (This is the group defined in Problem 3.1.35). Define $\phi : G \to \mathbf{R}^+$ by $\phi(x) = x - 1$, for all $x \in G$. Show that ϕ is an isomorphism.

58. Let n be an odd integer. Show that $\phi : \mathbf{R}^\times \to \mathbf{R}^\times$ defined by $\phi(x) = x^n$ is an isomorphism. If n is an even integer, what goes wrong?

59.† Let G be a finite abelian group, and let n be a positive integer. Define a function $\phi : G \to G$ by $\phi(g) = g^n$, for all $g \in G$. Find necessary and sufficient conditions to guarantee that ϕ is a group isomorphism.

60. Let G be a group. An isomorphism $\phi : G \to G$ is called an **automorphism** of G, and the set of all automorphisms of G is denoted by $\mathrm{Aut}(G)$. Show that $\mathrm{Aut}(G)$ is a group under composition of functions.

61. An automorphism $\theta : G \to G$ is called an **inner automorphism** of G if there exists $a \in G$ such that $\theta = i_a$, where i_a is defined by setting $i_a(g) = aga^{-1}$ for all $g \in G$. Show that the set $\mathrm{Inn}(G)$ of all inner automorphisms of G is a subgroup of $\mathrm{Aut}(G)$.

62. Let G be a finite abelian group of odd order.

    (a) Show that $\theta : G \to G$ defined by $\theta(x) = x^2$, for all $x \in G$, is an isomorphism.

    (b) The function $\phi : G \to G$ defined by $\phi(x) = x^{-1}$, for all $x \in G$, is an isomorphism by Exercise 3.4.16. Do ϕ and θ commute as elements of $\mathrm{Aut}(G)$?

3.5 Cyclic Groups

We began our study of abstract algebra very concretely, by looking at the group $\mathbf{Z}$ of integers, and the related groups $\mathbf{Z}_n$. We discovered that each of these groups is generated by a single element, and this motivated the definition of an abstract cyclic group. In this section, Theorem 3.5.2 shows that every cyclic group is isomorphic to one of these concrete examples, so all of the information about cyclic groups is already contained in these basic examples.

You should pay particular attention to Proposition 3.5.3, which describes the subgroups of $\mathbf{Z}_n$, showing that they are in one-to-one correspondence with the positive divisors of n. In n is a prime power, then the subgroups are "linearly ordered" in the sense that given any two subgroups, one is a subset of the other. These cyclic groups have a particularly simple structure, and form the basic building blocks for *all* finite abelian groups. (In Theorem 7.5.4 we will prove that every finite abelian group is isomorphic to a direct product of cyclic groups of prime power order.)

SOLVED PROBLEMS: §3.5

21. Show that the three groups $\mathbf{Z}_6$, $\mathbf{Z}_9^\times$, and $\mathbf{Z}_{18}^\times$ are isomorphic to each other.

22. Is $\mathbf{Z}_{20}^\times$ cyclic?

23. Is $\mathbf{Z}_{50}^\times$ cyclic?

24. Is $\mathbf{Z}_4 \times \mathbf{Z}_{10}$ isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_{20}$?

25. Is $\mathbf{Z}_4 \times \mathbf{Z}_{15}$ isomorphic to $\mathbf{Z}_6 \times \mathbf{Z}_{10}$?

26. Give the lattice diagram of subgroups of $\mathbf{Z}_{100}$.

27. Find all generators of the cyclic group $\mathbf{Z}_{28}$.

28. In $\mathbf{Z}_{30}$, find the order of the subgroup $\langle 18\rangle$; find the order of $\langle 24\rangle$.

29. In $\mathbf{Z}_{45}$ find all elements of order 15.

30. Prove that if G_1 and G_2 are groups of order 7 and 11, respectively, then the direct product $G_1 \times G_2$ is a cyclic group.

31. Show that any cyclic group of even order has exactly one element of order 2.

32. Use the the result in Problem 31 to show that the multiplicative groups $\mathbf{Z}_{15}^{\times}$ and $\mathbf{Z}_{21}^{\times}$ are not cyclic groups.

33. Prove that if p and q are different odd primes, then $\mathbf{Z}_{pq}^{\times}$ is not a cyclic group.

34. Find all cyclic subgroups of the quaternion group. Use this information to show that the quaternion group cannot be isomorphic to the subgroup of S_4 generated by $(1,2,3,4)$ and $(1,3)$.

MORE PROBLEMS: §3.5

35.† Let G be a cyclic group of order 25, written multiplicatively, with $G = \langle a\rangle$. Find all elements of G that have order 5.

36.† Let G be a group with an element $a \in G$ with $o(a) = 18$. Find all subgroups of $\langle a\rangle$.

37. Show that $\mathbf{Q}^+$ is not a cyclic group.

38.† Give an example of an infinite group in which every element has finite order.

39. Let G be an abelian group of order 15. Show that if you can find an element a of order 5 and an element b of order 3, then G must be cyclic.

40. Let $H = \left\{\pm 1, \pm i, \pm\frac{\sqrt{2}}{2} \pm \frac{\sqrt{2}}{2}i\right\}$. Show that H is a cyclic subgroup of $\mathbf{C}^{\times}$. Find all of the generators of H.

41. Let G be a group with a subgroup H, and let $a \in G$ be an element of order n. Prove that if $a^m \in H$, where $\gcd(m,n) = 1$, then $a \in H$.

42. Let $H = \left\{ \begin{bmatrix} 1 & m & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in \mathrm{GL}_3(\mathbf{Q}) \mid m \in \mathbf{Z} \right\}$ and $K = \left\{ \begin{bmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in \mathrm{GL}_3(\mathbf{Q}) \mid n \in \mathbf{Z} \right\}$. Show that H and K are cyclic subgroups of $\mathrm{GL}_3(\mathbf{Q})$, and that $H \cong K$.

43. Let $D = \left\{ \left. \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \right| a,b,c \in \mathbf{Z}_2 \right\}$. Note that D is a group by Problem 3.3.44.

†(a) Find the number of elements of order 4 in D. Use this and the fact that D is nonabelian to guess which of the groups O, P, or Q (from Section 3.1) might be isomorphic to D.

(b) Verify your conjecture in part (a) by proving that such an isomorphism exists.

44.† Let n be a positive integer which has the prime decomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, where $p_1 < p_2 < \ldots < p_m$. Prove that $\mathbf{Z}_n^\times \cong \mathbf{Z}_{p_1^{\alpha_1}}^\times \times \mathbf{Z}_{p_2^{\alpha_2}}^\times \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}}^\times$.

45. Use Problem 44 to give an alternate proof of Problem 32.

46. Let G be a group with exactly one proper nontrivial subgroup. Prove that $G \cong \mathbf{Z}_{p^2}$ for some prime p.

Comment: Compare Exercise 3.5.16 in the text, which states that a group with no proper nontrivial subgroups is isomorphic to $\mathbf{Z}_p$, for some prime p.

47.† Let G be a group. Recall from Problem 3.4.60 that an isomorphism $\phi : G \to G$ is called an *automorphism* of G, and the set of all automorphisms of G is denoted by $\mathrm{Aut}(G)$. Show that $\mathrm{Aut}(\mathbf{Z}_n)$ is isomorphic to $\mathbf{Z}_n^\times$.

Hint: An automorphism of $\mathbf{Z}_n$ must send $[1]_n$ to a generator of $\mathbf{Z}_n$.

48. Give an example to show that it is possible to have cyclic groups G_1 and G_2 for which $\mathrm{Aut}(G_1)$ is isomorphic to $\mathrm{Aut}(G_2)$ even though G_1 is not isomorphic to G_2.

3.6 Permutation Groups

As with the previous section, this section revisits the roots of group theory that we began to study in an earlier chapter. Cayley's theorem shows that permutation groups contain all of the information about finite groups, since every finite group of order n is isomorphic to a subgroup of the symmetric group S_n. That isn't as impressive as it sounds at first, because as n gets larger and larger, the subgroups of order n just get lost inside the larger symmetric group, which has order $n!$. This does imply, however, that from the algebraist's point of view the abstract definition of a group is really no more general than the concrete definition of a permutation group. The abstract definition of a group is useful simply because it can be more easily applied to a wide variety of situation.

You should make every effort to get to know the dihedral groups D_n. They have a concrete representation, in terms of the rigid motions of an n-gon, but can also be described more abstractly in terms of two generators a (of order n) and b (of order 2) which satisfy the relation $ba = a^{-1}b$. We can write

$$D_n = \{a^i b^j \mid 0 \le i < n,\ 0 \le j < 2, \text{ with } o(a) = n,\ o(b) = 2, \text{ and } ba = a^{-1}b\}\ .$$

In doing computations in D_n it is useful to have at hand the formula $ba^i = a^{n-i}b$, shown in the first of the solved problems given below.

SOLVED PROBLEMS: §3.6

28. In the dihedral group $D_n = \{a^i b^j \mid 0 \le i < n,\ 0 \le j < 2\}$ with $o(a) = n$, $o(b) = 2$, and $ba = a^{-1}b$, show that $ba^i = a^{n-i}b$, for all $0 \le i < n$.

29. In the dihedral group $D_n = \{a^i b^j \mid 0 \leq i < n,\ 0 \leq j < 2\}$ with $o(a) = n$, $o(b) = 2$, and $ba = a^{-1}b$, show that each element of the form $a^i b$ has order 2.

30. In S_4, find the subgroup H generated by $(1, 2, 3)$ and $(1, 2)$.

31. For the subgroup H of S_4 defined in the previous problem, find the corresponding subgroup $\sigma H \sigma^{-1}$, for $\sigma = (1, 4)$.

32. Show that each element in A_4 can be written as a product of 3-cycles.

33. In the dihedral group $D_n = \{a^i b^j \mid 0 \leq i < n,\ 0 \leq j < 2\}$ with $o(a) = n$, $o(b) = 2$, and $ba = a^{-1}b$, find the centralizer of a.

34. Find the centralizer of $(1, 2, 3)$ in S_3, in S_4, and in A_4.

35. With the notation of the comments preceding the statement of Theorem 3.6.6, find $\sigma(\Delta_3)$ for each $\sigma \in S_n$.

MORE PROBLEMS: §3.6

36.† Compute the centralizer of $(1, 2)(3, 4)$ in S_4.

37.† Show that the group of rigid motions of a cube can be generated by two elements.

38. Explain why there are 144 elements of order 5 in the alternating group A_6.

39.† Describe the possible shapes of the permutations in A_6. Use a combinatorial argument to determine how many of each type there are.

40.† Find the largest possible order of an element in each of the alternating groups A_5, A_6, A_7, A_8.

41.† Let G be the dihedral group D_6, denoted by $G = \{a^i b^j | 0 \leq i < 6 \text{ and } 0 \leq j < 2\}$, where a has order 6, b has order 2, and $ba = a^{-1}b$. Find $C(ab)$.

42. Let $G = D_6$.

    (a) Show that $\{x \in G \mid x^3 = e\}$ is a subgroup of G.

    (b) Is $\{x \in G \mid x^2 = e\}$ a subgroup of G?

43. Show that the set of upper triangular matrices in $\mathrm{GL}_2(\mathbf{Z}_3)$ is isomorphic to D_6.

    Hint: See Problem 3.3.43.

44.† Is D_{12} isomorphic to $D_4 \times \mathbf{Z}_3$?

3.7 Homomorphisms

In Section 3.4 we introduced the concept of an isomorphism, and studied in detail what it means for two groups to be isomorphic. In this section we look at functions that respect the group operations but may not be one-to-one and onto. There are many important examples of group homomorphisms that are not isomorphisms, and, in fact, homomorphisms provide the way to relate one group to another.

The most important result in this section is Theorem 3.7.8, which is a preliminary form of the fundamental homomorphism theorem. (The full statement is given in Theorem 3.8.9, after we develop the concepts of cosets and factor groups.) In this formulation of the fundamental homomorphism theorem, we start with a group homomorphism $\phi : G_1 \to G_2$. It is easy to prove that the image $\phi(G_1)$ is a subgroup of G_2. The function ϕ has an equivalence relation associated with it, where we let $a \sim b$ if $\phi(a) = \phi(b)$, for $a, b \in G_1$. Just as in $\mathbf{Z}$, where we use the equivalence relation defined by congruence modulo n, we can define a group operation on the equivalence classes of $\sim$, using the operation in G_1. Then Theorem 3.7.8 shows that this group is isomorphic to $\phi(G_1)$, so that although the homomorphism may not be an isomorphism between G_1 and G_2, it *does* define an isomorphism between a subgroup of G_2 and what we call a *factor group* of G_1.

Proposition 3.7.6 is also useful, since for any group homomorphism $\phi : G_1 \to G_2$ it describes the connections between subgroups of G_1 and subgroups of G_2. Examples 3.7.6 and 3.7.7 are important, because they give a complete description of all group homomorphisms between two cyclic groups.

SOLVED PROBLEMS: §3.7

21. Find all group homomorphisms from $\mathbf{Z}_4$ into $\mathbf{Z}_{10}$.

22. (a) Find the formulas for all group homomorphisms from $\mathbf{Z}_{18}$ into $\mathbf{Z}_{30}$.

    (b) Choose one of the nonzero formulas in part (a), and name it ϕ. Find $\phi(\mathbf{Z}_{18})$ and $\ker(\phi)$, and show how elements of $\phi(\mathbf{Z}_{18})$ correspond to equivalence classes of $\sim_\phi$.

23. (a) Show that $\mathbf{Z}_{11}^\times$ is cyclic, with generator $[2]_{11}$.

    (b) Show that $\mathbf{Z}_{19}^\times$ is cyclic, with generator $[2]_{19}$.

    (c) Completely determine all group homomorphisms from $\mathbf{Z}_{19}^\times$ into $\mathbf{Z}_{11}^\times$.

24. Define $\phi : \mathbf{Z}_4 \times \mathbf{Z}_6 \to \mathbf{Z}_4 \times \mathbf{Z}_3$ by $\phi([x]_4, [y]_6) = ([x + 2y]_4, [y]_3)$.

    (a) Show that ϕ is a well-defined group homomorphism.

    (b) Find the kernel and image of ϕ, and apply Theorem 3.7.8.

25. Let n and m be positive integers, such that m is a divisor of n. Show that $\phi : \mathbf{Z}_n^\times \to \mathbf{Z}_m^\times$ defined by $\phi([x]_n) = [x]_m$, for all $[x]_n \in \mathbf{Z}_n^\times$, is a well-defined group homomorphism.

26. For the group homomorphism $\phi : \mathbf{Z}_{36}^\times \to \mathbf{Z}_{12}^\times$ defined by $\phi([x]_{36}) = [x]_{12}$, for all $[x]_{36} \in \mathbf{Z}_{36}^\times$, find the kernel and image of ϕ, and apply Theorem 3.7.8.

27. Prove that $\mathrm{SL}_n(\mathbf{R})$ is a normal subgroup of $\mathrm{GL}_n(\mathbf{R})$.

MORE PROBLEMS: §3.7

28.† Prove or disprove each of the following assertions:

(a) The set of all nonzero scalar matrices is a normal subgroup of $\mathrm{GL}_n(\mathbf{R})$.

(b) The set of all diagonal matrices with nonzero determinant is a normal subgroup of $\mathrm{GL}_n(\mathbf{R})$.

29. Define $\phi : \mathbf{Z}_8 \to \mathbf{Z}_{16}^\times$ by $\phi([m]_8) = [3]_{16}^m$, for all $[m]_8 \in \mathbf{Z}_8$. Show that ϕ is a group homomorphism. Compute the kernel and image of ϕ.

Note: Problem 2.1.40 shows that ϕ is a well-defined function. This also follows from the fact that $o([3]_{16})$ is a divisor of $\varphi(16) = 8 = |\mathbf{Z}_8|$.

30. Define $\phi : \mathbf{Z}_{15}^\times \to \mathbf{Z}_{15}^\times$ by $\phi([x]_{15}) = [x]_{15}^2$, for all $[x]_{15} \in \mathbf{Z}_{15}^\times$. Find the kernel and image of ϕ.

Note: The function ϕ is a group homomorphism by Exercise 3.7.4, which states that if G is an abelian group and n is a positive integer, then $\phi : G \to G$ defined by $\phi(x) = x^n$ for all $x \in G$ is a group homomorphism.

31.† Define $\phi : \mathbf{Z}_{15}^\times \to \mathbf{Z}_{15}^\times$ by $\phi([x]_{15}) = [x]_{15}^3$, for all $[x]_{15} \in \mathbf{Z}_{15}^\times$. Find the kernel and image of ϕ.

32.† Define $\phi : \mathbf{Z}_{15}^\times \to \mathbf{Z}_5^\times$ by $\phi([x]_{15}) = [x]_5^3$. Show that ϕ is a group homomorphism, and find its kernel and image.

33. Exercise 3.7.15 states that the intersection of two normal subgroups is a normal subgroup. Extend that exercise by showing that the intersection of *any* collection of normal subgroups is a normal subgroup.

Note: Exercise 3.2.17 states that the intersection of any collection of subgroups is again a subgroup.

34.† How many homomorphisms are there from $\mathbf{Z}_{12}$ into $\mathbf{Z}_4 \times \mathbf{Z}_3$?

Note: Compare Problem 3.4.45.

35. Let G be the group $\mathbf{R}[x]$ of all polynomials with real coefficients. For any polynomial $f(x)$, show that for any element $a \in \mathbf{R}$ the function $\phi : \mathbf{R}[x] \to \mathbf{R}$ defined by $\phi(f(x)) = f(a)$, for all $f(x) \in \mathbf{R}[x]$, is a group homomorphism.

36.† Define $\phi : \mathbf{R} \to \mathbf{C}^\times$ by setting $\phi(x) = e^{ix}$, for all $x \in \mathbf{R}$. Show that ϕ is a group homomorphism, and find $\ker(\phi)$ and the image $\phi(\mathbf{R})$.

37. Let G be a group, with a subgroup $H \subseteq G$. Define $N(H) = \{g \in G \mid gHg^{-1} = H\}$.

(a) Problem 3.2.51 shows that is a subgroup of G that contains H, called the **normalizer of H in G**. Show that H is a normal subgroup of $N(H)$.

†(b) Let $G = S_4$. Find $N(H)$ for the subgroup H generated by $(1, 2, 3)$ and $(1, 2)$.

38.† Find all normal subgroups of A_4.

3.8 Cosets, Normal Subgroups, and Factor Groups

The notion of a factor group is one of the most important concepts in abstract algebra. To construct a factor group, we start with a normal subgroup and the equivalence classes it determines. This construction parallels the construction of $\mathbf{Z}_n$ from $\mathbf{Z}$, where we have $a \equiv b \pmod{n}$ if and only if $a - b \in n\mathbf{Z}$. The only complication is that the equivalence relation respects the operation in G only when the subgroup is a normal subgroup. Of course, in an abelian group we can use any subgroup, since all subgroups of an abelian group are normal.

The key idea is to begin thinking of equivalence classes as elements in their own right. That is what we did in Chapter 1, where at first we thought of congruence classes as infinite sets of integers, and then in Section 1.4 when we started working with $\mathbf{Z}_n$ we started to use the notation $[a]_n$ to suggest that we were now thinking of a single element of a set.

In actually using the fundamental homomorphism theorem, it is important to let the theorem do its job, so that it does as much of the hard work as possible. Quite often we need to show that a factor group G/N that we have constructed is isomorphic to another group G_1. The easiest way to do this is to just define a homomorphism ϕ from G to G_1, making sure that N is the kernel of ϕ. If you prove that ϕ maps G onto G_1, then the fundamental homomorphism theorem does the rest of the work, showing that there exists a well-defined isomorphism between G/N and G_1.

The moral of this story is that if you define a function on G rather than G/N, you ordinarily don't need to worry that it is well-defined. On the other hand, if you define a function on the cosets of G/N, the most convenient way is use a formula defined on representatives of the cosets of N. But then you must be careful to prove that the formula you are using does not depend on the particular choice of a representative. That is, you must prove that your formula actually defines a function. Then you must prove that your function is one-to-one, in addition to proving that it is onto and respects the operations in the two groups. Once again, if your function is defined on cosets, it can be much trickier to prove that it is one-to-one than to simply compute the kernel of a homomorphism defined on G.

SOLVED PROBLEMS: §3.8

29. Define $\phi : \mathbf{C}^\times \to \mathbf{R}^\times$ by $\phi(z) = |z|$, for all $z \in \mathbf{C}^\times$.

    (a) Show that ϕ is a group homomorphism.

    (b) Find $\ker(\phi)$ and $\phi(\mathbf{C}^\times)$.

    (c) Describe the cosets of $\ker(\phi)$, and explain how they are in one-to-one correspondence with the elements of $\phi(\mathbf{C}^\times)$.

30. List the cosets of $\langle 9 \rangle$ in $\mathbf{Z}_{16}^\times$, and find the order of each coset in $\mathbf{Z}_{16}^\times / \langle 9 \rangle$.

31. List the cosets of $\langle 7\rangle$ in $\mathbf{Z}_{16}^{\times}$. Is the factor group $\mathbf{Z}_{16}^{\times}/\langle 7\rangle$ cyclic?

32. Let $G = \mathbf{Z}_6 \times \mathbf{Z}_4$, let $H = \{([0]_6, [0]_4), ([0]_6, [2]_4)\}$, and let $K = \{([0]_6, [0]_4), ([3]_6, [0]_4)\}$.

    (a) List all cosets of H; list all cosets of K.

    (b) You may assume that any abelian group of order 12 is isomorphic to either $\mathbf{Z}_{12}$ or $\mathbf{Z}_6 \times \mathbf{Z}_2$. Which answer is correct for G/H? For G/K?

33. Let the dihedral group D_n be given via generators and relations, with generators a of order n and b of order 2, satisfying $ba = a^{-1}b$.

    (a) Show that $ba^i = a^{-i}b$ for all i with $1 \leq i < n$, and that any element of the form a^ib has order 2.

    (b) List all left cosets and all right cosets of $\langle a\rangle$.

    (c) List all left cosets and all right cosets of $\langle b\rangle$.

    (d) List all left cosets and all right cosets of $\langle ab\rangle$.

34. Let G be the dihedral group D_6 and let N be the subgroup $\langle a^3\rangle = \{e, a^3\}$ of G.

    (a) Show that N is a normal subgroup of G.

    (b) Since $|G/N| = 6$, you can assume that G/N is isomorphic to either $\mathbf{Z}_6$ or S_3. (Exercise 3.3.17 characterizes groups of order 6 as isomorphic to either $\mathbf{Z}_6$ or S_3.) Which group gives the correct answer?

35. Let G be the dihedral group D_6 and let H be the subgroup $\langle b\rangle = \{e, b\}$ of G. Show that H is not a normal subgroup of G.

36. Let G be the dihedral group D_6 and let H be the subset $\{e, a^3, b, a^3b\}$ of G.

    (a) Show that H is subgroup of G.

    (b) Is H a normal subgroup of G?

37. Let G be the dihedral group D_{12}, and let N be the subgroup $\langle a^3\rangle = \{e, a^3, a^6, a^9\}$.

    (a) Prove that N is a normal subgroup of G, and list all cosets of N.

    (b) Since $|G/N| = 6$, you can assume that G/N is isomorphic to either $\mathbf{Z}_6$ or S_3. Which group gives the correct answer?

38. Let G be a group. For $a, b \in G$ we say that b is **conjugate** to a, written $b \sim a$, if there exists $g \in G$ such that $b = gag^{-1}$. Following part (a), the equivalence classes of $\sim$ are called the **conjugacy classes** of G.

    (a) Show that $\sim$ is an equivalence relation on G.

    (b) Show that a subgroup N of G is normal in G if and only if N is a union of conjugacy classes.

39. Find the conjugacy classes of D_4.

40. Show that A_4 is the only subgroup of index 2 in S_4.

41. Let G be a group, and let N and H be subgroups of G such that N is normal in G. It follows from Proposition 3.3.2 that HN is a subgroup, and Exercise 3.8.27 shows that N is a normal in HN. Prove that if $H \cap N = \{e\}$, then $HN/N \cong H$.

42. Use Problem 41 to show that $\mathbf{Z}_{16}^{\times}/\langle 7\rangle \cong \mathbf{Z}_4$.

MORE PROBLEMS: §3.8

43.† In $\mathbf{Z}_{25}^{\times}/\langle 6\rangle$, find the order of each of the cosets $2\langle 6\rangle$, $3\langle 6\rangle$, and $4\langle 6\rangle$.

44. Let V be a vector space over $\mathbf{R}$, and let W be a subspace of V. On the factor group V/W, define scalar multiplication by letting $c \cdot (v + W) = cv + W$.

    (a) Show that V/W is a vector space over $\mathbf{R}$, using the given definition of scalar multiplication.

    (b) Show that if $\dim(V) = n$ and $\dim(W) = m$, then $\dim(V/W) = n - m$.

45. Let G_1 and G_2 be groups with normal subgroups $N_1 \subseteq G_1$ and $N_2 \subseteq G_2$.

    (a) Show that $N_1 \times N_2 = \{(x_1, x_2) \in G_1 \times G_2 \mid x_1 \in N_1 \text{ and } x_2 \in N_2\}$ is a normal subgroup of $G_1 \times G_2$. *Recall:* $N_1 \times N_2$ is a subgroup by Exercise 3.3.8.

    †(b) Show that $G_1 \times G_2/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2)$.

    Hint: Define a group homomorphism from $G_1 \times G_2$ onto $(G_1/N_1) \times (G_2/N_2)$ with kernel $N_1 \times N_2$ and let the fundamental homomorphism theorem do the rest of the work.

46.† Exercise 3.8.25 asks for an example of a finite group G with two normal subgroups H and K such that $G/H \cong G/K$ but $H \ncong K$. As a complement to that exercise, give an example of a finite group G with normal subgroups $H \cong K$ but $G/H \ncong G/K$.

47. Let G be a group. Show that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

    Note: See Problems 3.4.60 and 3.4.61 for the definitions of $\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$.

48. Let G be a finite abelian group, whose operation is denoted additively, and let H and K be subgroups of G. Define $\phi : H \times K \to H + K$ by $\phi((x, y)) = x - y$, for all $(x, y) \in H \times K$. Show that ϕ is a group homomorphism that maps $H \times K$ onto $H + K$, and that $\ker(\phi) = \{(x, y) \mid x = y\}$. Then show why this implies that $|H + K| = \dfrac{|H||K|}{|H \cap K|}$.

Exercise 3.8.16 shows that if G is a group with normal subgroups H and K such that $HK = G$ and $H \cap K = \{e\}$, then $G \cong H \times K$. (Note that Problem 3.4.38 gives the proof in case G is abelian.)

Definition. If G has normal subgroups H and K such that $HK = G$ and $H \cap K = \{e\}$, then we say that G is the **internal direct product** of H and K.

Compare Problems 3.4.37 and 3.4.38. See Problems 3.3.36 and 3.3.37 for examples of internal direct products.

49. Let $n = pq$, where p and q are distinct prime numbers.

    (a) Show that $\mathbf{Z}_n^\times$ is the internal direct product of the subgroups $H = \{[x] \in \mathbf{Z}_n^\times \mid x \equiv 1 \pmod{p}\}$ and $K = \{[y] \in \mathbf{Z}_n^\times \mid y \equiv 1 \pmod{q}\}$.

    Hint: Recall Exercise 3.3.13 in **Abstract Algebra**, which states that $HK = \mathbf{Z}_n^\times$.

    (b) Use Problem 41 (c) to show that $H \cong \mathbf{Z}_q^\times$ and $K \cong \mathbf{Z}_p^\times$.

    (c) Explain how parts (a) and (b) prove a special case of Exercise 3.4.21 in the text, which states that $\mathbf{Z}_{mn}^\times \cong \mathbf{Z}_m^\times \times \mathbf{Z}_n^\times$ if $\gcd(m, n) = 1$.

50. (a) Show that $\mathbf{Z}_{20}^\times$ is the internal direct product of the subgroups $\langle [-1]_{20} \rangle$ and $\langle [3]_{20} \rangle$.

    (b) Show that $\mathbf{Z}_{28}^\times$ is the internal direct product of the subgroups $\langle [-1]_{28} \rangle$ and $\langle [5]_{28} \rangle$.

    (c) Conjecture and prove a generalization of these two cases.

51. Show that D_4 cannot be the internal direct product of two proper subgroups.

52.† Show that the quaternion group Q cannot be the internal direct product of two proper subgroups.

Definition. Let G be a group with subgroups N and K. We say that G is the **internal semidirect product** of N and K if N is normal, $NK = G$ and $N \cap K = \{e\}$.

Take careful note of the distinction between the internal direct product and the internal semidirect product: in the second case only one of the subgroups must be normal.

53. Let D_n be described in the usual way via generators a of order n and b of order 2, with $ba = a^{-1}b$. Show that D_n is the internal semidirect product of $\langle a \rangle$ and $\langle b \rangle$.

54. Show that S_n is the internal semidirect product of A_n and $\langle (1, 2) \rangle$.

55. Let G be the set of all matrices in $\mathrm{GL}_2(\mathbf{Z}_5)$ of the form $\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$, let N be the set of matrices in $\mathrm{GL}_2(\mathbf{Z}_5)$ of the form $\begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix}$, with $c \in \mathbf{Z}_5$, and let K be the set of matrices in $\mathrm{GL}_2(\mathbf{Z}_5)$ of the form $\begin{bmatrix} m & 0 \\ 0 & 1 \end{bmatrix}$, with $0 \neq m \in \mathbf{Z}_5$. Show that G is the internal semidirect product of N and K.

56. Let G be the internal semidirect product of subgroups N and K. Show that $G/N \cong K$.

Definition. Let G be a group. A subgroup H of G is called a **characteristic subgroup** subgroup of G if $\phi(H) \subseteq H$ for all $\phi \in \mathrm{Aut}(G)$.

57. Let G be a group with subgroups H and K.

    (a) Prove that if H is a characteristic subgroup of G, then H is a normal of G.

    (b) Prove that if H is a normal subgroup of G, and K is a characteristic subgroup of H, then K is normal in G.

58. Prove that the center of any group is a characteristic subgroup.

59. Let H and K be characteristic subgroups of G.
    (a) Show that HK is a subgroup of G.
    (b) Show that HK is a characteristic subgroup of G.

60. Let n be a positive integer, and let G be a group that has only one subgroup H of order n. Show that H is a characteristic subgroup of G.

Chapter 3 Review Problems

§3.1–3.5

1. (a) What are the possibilities for the order of an element of $\mathbf{Z}_{13}^{\times}$? Explain your answer.
   (b) Show that $\mathbf{Z}_{13}^{\times}$ is a cyclic group.

2. What is the largest order of an element in $\mathbf{Z}_{12} \times \mathbf{Z}_{18}$? Use your answer to show, in particular, that the group is not cyclic.

3. Find all subgroups of $\mathbf{Z}_{11}^{\times}$, and the diagram showing the inclusions between them.

4. Which of the groups listed below are isomorphic to each other?
   $G_1 = \mathbf{Z}_8$, $G_2 = \mathbf{Z}_4 \times \mathbf{Z}_2$, $G_3 = \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$, $G_4 = \mathbf{Z}_{24}^{\times}$, $G_5 = \mathbf{Z}_{30}^{\times}$, $G_6 = D_4$.

5. Let G be the subset of $\mathrm{GL}_3(\mathbf{R})$ consisting of all matrices of the form $\begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ such that $a, b \in \mathbf{R}$. Show that G is a subgroup of $\mathrm{GL}_3(\mathbf{R})$.

6. Show that the group G in Problem 5 is isomorphic to the direct product $\mathbf{R} \times \mathbf{R}$.

§3.6–3.8

7. List the cosets of the cyclic subgroup $\langle 9 \rangle$ in $\mathbf{Z}_{20}^{\times}$. Is $\mathbf{Z}_{20}^{\times} / \langle 9 \rangle$ cyclic?

8. Let F be a field, let $G = \mathrm{GL}_2(F)$, let H be the subset of upper triangular matrices in G, and let N be the subset of $\mathrm{GL}_2(F)$ consisting of all matrices of the form $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$.
   (a) Show that H is a subgroup of G, but that H is not normal in G.
   (b) Show that N is a normal subgroup of H.
   (c) Show that H/N is isomorphic to the multiplicative group $F^{\times}$.

9. Assume that the dihedral group D_4 is given as $\{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e$, $b^2 = e$, and $ba = a^3b$. Let N be the subgroup $\langle a^2 \rangle = \{e, a^2\}$.

   (a) Show by a direct computation that N is a normal subgroup.

   (b) Is the factor group D_4/N a cyclic group?

   (c) Find all subgroups of D_4/N.

10. Let $G = D_8$, and let $N = \{e, a^2, a^4, a^6\}$.

    (a) List all left cosets and all right cosets of N, and verify that N is a normal subgroup of G.

    (b) Show that G/N has order 4, but is not cyclic.

11. (a) Show that $\mathbf{R}^\times/\mathbf{R}^+$ is cyclic of order 2.

    (b) Let H be a subgroup of $\mathbf{R}^\times$ that contains $\mathbf{R}^+$. Show that either $H = \mathbf{R}^\times$ or $H = \mathbf{R}^+$.

12. (a) Show that every element of the group $\mathbf{Q}/\mathbf{Z}$ has finite order.

    (b) Show that for each $n \in \mathbf{Z}^+$, the group $\mathbf{Q}/\mathbf{Z}$ contains an element of order n.

Chapter 4

POLYNOMIALS

In this chapter we return to several of the themes in Chapter 1. We need to talk about the greatest common divisor of two polynomials, and when two polynomials are relatively prime. The notion of a prime number is replaced by that of an *irreducible polynomial*. We can work with congruence classes of polynomials, just as we did with congruence classes of integers. The point of saying this is that it will be worth your time to review the definitions and theorems in Chapter 1.

In addition to generalizing ideas from the integers to polynomials, we want to go beyond high school algebra, to be able to work with coefficients that may not be real numbers. This motivates the definition of a field, which is quite closely related to the definition of a group (now there are two operations instead of just one). The point here is that you can benefit from reviewing Chapter 3.

4.1 Fields; Roots of Polynomials

This section begins the study of fields in earnest. Besides the standard examples $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ from high school algebra, you should become familiar with $\mathbf{Z}_p$ (viewed as a field) and with the other examples in the text. The axioms of field are the ones we need to work with polynomials and matrices, so these are the primary examples in the section.

The remainder theorem (Theorem 4.1.9) is a special case of the division algorithm (Theorem 4.2.1). Since the proof can be given much more easily in the special case than in the general one, we chose to include the remainder theorem in the first section. It has the important consequence that a polynomial of degree n with coefficients in a field can have at most n distinct roots in the field.

SOLVED PROBLEMS: §4.1

25. Let F be a field, and let $f(x), g(x) \in F[x]$ be polynomials of degree less than n. Assume that $f(x)$ agrees with $g(x)$ on n distinct elements of F. (That is, $f(x_i) = g(x_i)$ for distinct elements $x_1, \ldots, x_n \in F$.) Prove that $f(x) = g(x)$ (as polynomials).

26. Let $c \in F$ and let $f(x) \in F[x]$. Show that $r \in F$ is a root of $f(x)$ if and only if $r - c$ is a root of $f(x + c)$.

27. For $f(x) = x^3 - 5x^2 - 6x + 2 \in \mathbf{Q}[x]$, use the method of Theorem 4.1.9 to write $f(x) = q(x)(x + 1) + f(-1)$.

28. For $f(x) = x^3 - 2x^2 + x + 3 \in \mathbf{Z}_7[x]$, use the method of Theorem 4.1.9 to write $f(x) = q(x)(x - 2) + f(2)$.

29. Show that the set of matrices of the form $\begin{bmatrix} a & b \\ -3b & a \end{bmatrix}$, where $a, b \in \mathbf{Q}$, is a field under the operations of matrix addition and multiplication.

30. Prove that if p is a prime number, then the multiplicative group $\mathbf{Z}_p^\times$ is cyclic.

31. Let p be a prime number, and let $a, b \in \mathbf{Z}_p^\times$. Show that if neither a nor b is a square, then ab *is* a square.

Exercise 17 in the text introduces a special case of the *Lagrange interpolation formula*, which provides a way to write down a polynomial of degree n whose graph passes through $n+1$ points in the plane. Let (x_0, y_0), (x_1, y_1), (x_2, y_2) be points in the Euclidean plane $\mathbf{R}^2$ such that x_0, x_1, x_2 are distinct. Then the formula

$$f(x) = \frac{y_0(x - x_1)(x - x_2)}{(x_0 - x_1)(x_0 - x_2)} + \frac{y_1(x - x_0)(x - x_2)}{(x_1 - x_0)(x_1 - x_2)} + \frac{y_2(x - x_0)(x - x_1)}{(x_2 - x_0)(x_2 - x_1)}$$

defines a polynomial $f(x)$, called the **Lagrange interpolation formula** such that $f(x_0) = y_0$, $f(x_1) = y_1$, and $f(x_2) = y_2$. It is easy to extend this formula to the general case of $n+1$ points.

This is a very interesting formula, but one problem is that if an additional point is given, then every term must be recomputed. There is an alternative formula, which uses the method of *divided differences*, and we will present this formula in some detail since it is easier to adjust to include additional information.

To motivate the divided differences approach, we go back to the two point form of a straight line, as given below.

$$f(x) = y_0 + \frac{y_1 - y_0}{x_1 - x_0}(x - x_0) \ .$$

In this case our function is expressed as a sum of two functions $f_0(x)$ and $f_1(x)$ such that $f_0(x_0) = y_0$ and $f_1(x_0) = 0$, while $f_0(x_1) = y_0$ and $f_1(x_1) = y_1 - y_0$.

Our goal is to add a third term $f_2(x)$ so that

$$f(x) = f_0(x) + f_1(x) + f_2(x)$$

will define a quadratic function passing through (x_0, y_0), (x_1, y_1), and (x_2, y_2), where the original terms are $f_0(x) = y_0$ and $f_1(x) = \frac{y_1 - y_0}{x_1 - x_0}(x - x_0)$, and the new term $f_2(x)$ has degree two. We want to have the following conditions.

$$\begin{array}{lll} f_0(x_0) = y_0 & f_1(x_0) = 0 & f_2(x_0) = 0 \\ f_0(x_1) = y_0 & f_1(x_1) = y_1 - y_0 & f_2(x_1) = 0 \\ f_0(x_2) = y_0 & f_1(x_2) = f_1(x_2) & f_2(x_2) = y_2 - f_1(x_2) - y_0 \end{array}$$

Since $f_2(x_0) = 0$ and $f_2(x_1) = 0$, we need to look for a quadratic function of the form

$$f_2(x) = k(x - x_0)(x - x_1) \ .$$

Because we must have $f(x_2) = y_2$, we can determine the constant k by just substituting $x = x_2$ into the above equation. This gives us

$$k = \frac{\dfrac{y_2 - y_1}{x_2 - x_1} - \dfrac{y_1 - y_0}{x_1 - x_0}}{(x_2 - x_0)}$$

and leads to the equation

$$f(x) = y_0 + \frac{y_1 - y_0}{x_1 - x_0}(x - x_0) + k(x - x_0)(x - x_1) \ .$$

Notice that the first term in the numerator of k is the slope of the line segment joining (x_1, y_1) and (x_2, y_2), while the second term is the slope of the line segment joining (x_0, y_0) and (x_1, y_1), which we have already computed. The expression $f(x)$ is called the **divided differences** interpolation formula (for three points).

Example 4.1.6. We will use the divided differences method to determine a quadratic through the points $(1, 1)$, $(2, 4)$, and $(3, 9)$, knowing that we should obtain the function $f(x) = x^2$. We let $x_0 = 1$, $x_1 = 2$, and $x_2 = 3$. Then the function we are looking for has the form

$$f(x) = a + b(x - 1) + c(x - 1)(x - 2) \ ,$$

where

$$a = 1, \ b = \frac{4 - 1}{2 - 1} = 3, \text{ and } c = \frac{\dfrac{9 - 4}{3 - 2} - \dfrac{4 - 1}{2 - 1}}{3 - 1} = \frac{5 - 3}{3 - 1} = 1 \ .$$

This gives us the polynomial $f(x) = 1 + 3(x - 1) + 1(x - 1)(x - 2)$. It can be used in this form, without combining terms. (You can check that it reduces to $f(x) = x^2$, if you like.) For example, $f(2.5) = 1 + 3(1.5) + (1.5)(.5) = 6.25$.

Note that the computation of c uses the value obtained for b, together with another value computed similarly. To simplify the computations, it is convenient to arrange the necessary terms in a table in the following way. Here each column of divided differences is constructed from the previous one. Then the coefficients of the polynomial are found by reading from left to right, along the bottom of each column.

x	y		
3	9		
		$\frac{9-4}{3-2} = 5$	
2	4		$\frac{5-3}{3-1} = 1$
		$\frac{4-1}{2-1} = 3$	
1	1		

32. Use the method of divided differences to find the polynomial of degree 2 whose graph passes through $(0, 5)$, $(1, 7)$, and $(-1, 9)$.

33. Use the method of divided differences to find a formula for $\sum_{i=1}^{n} i^2$.

MORE PROBLEMS: §4.1

34.† Find the number of elements $a \in \mathbf{Z}_p$ for which $x^2 - a$ has a root in $\mathbf{Z}_p$, where p is prime.

35. Show that $x^2 - a$ has a root in $\mathbf{Z}_p$ (where $p > 2$ is prime) if and only if $a^{(p+1)/2} = a$.

36. Determine conditions on the integers b and c for which the quadratic equation $x^2 + bx + c = 0$ has a solution in $\mathbf{Z}_p$ (where $p > 2$ is prime).

37. Show that $x^2 + 3x + 2$ has four roots in $\mathbf{Z}_6$.

38. Prove that if F is an infinite field and two polynomials in $F[x]$ are equal as functions on F, then they are equal as polynomials.

39.† Use the method of divided differences to find the cubic polynomial whose graph passes through the points $(0, -5)$, $(1, -3)$, $(-1, -11)$, and $(2, 1)$.

40. The following values give $\sqrt{x}$ to 6 decimal place accuracy: (55, 7.416198), (54, 7.348469), (53, 7.280110), (52, 7.211103), (51, 7.141428), (50, 7.071068).

    (a) Compute the entire table of divided differences.

    (b) Find the interpolating polynomial of degree 5 for the given values (do not simplify) and use it to approximate $\sqrt{50.25}$, $\sqrt{52.37}$, and $\sqrt{53.91}$.

41.† Use the method of divided differences to verify the formula for $\sum_{i=1}^{n} i^3$.

42.† Let F be a finite field, and let $f(x) : F \to F$ be any function. Prove that there exists a polynomial $p(x) \in F[x]$ such that $f(a) = p(a)$ for all $a \in F$.

4.2 Factors

This section introduces concepts for polynomials that model those for integers. The division algorithm for polynomials is similar to that of integers, except that the remainder is determined by its degree (which replaces the size of an integer). We can define the greatest common divisor of two polynomials, and we can find it via the Euclidean algorithm. This, in turn, leads to a unique factorization theorem, in which the notion of an *irreducible* polynomial replaces that of a prime number.

In Chapter 1 we used a matrix method to write $\gcd(a, b)$ as a linear combination of a and b. A similar result holds for polynomials, but in solving the corresponding problems for polynomials use the "back-substitution" method. Trying to put polynomials into a matrix just gets too complicated.

SOLVED PROBLEMS: §4.2

21. Over the field of rational numbers, use the Euclidean algorithm to show that $2x^3 - 2x^2 - 3x + 1$ and $2x^2 - x - 2$ are relatively prime.

    Let $2x^3 - 2x^2 - 3x + 1 = f(x)$ and $2x^2 - x - 2 = g(x)$.

22. Over the field of rational numbers, find the greatest common divisor of $x^3 - 1$ and $x^4 + x^3 + 2x^2 + x + 1$, and express it as a linear combination of the given polynomials.

23. Find the greatest common divisor of $x^3 - 2x + 1$ and $x^2 - x - 2$ in $\mathbf{Z}_5[x]$, and express it as a linear combination of the given polynomials.

24. (a) Express $x^4 + x$ as a product of polynomials irreducible over $\mathbf{Z}_5$.

    (b) Show that $x^3 + 2x^2 + 3$ is irreducible over $\mathbf{Z}_5$.

25. Express $2x^3 + x^2 + 2x + 2$ as a product of polynomials irreducible over $\mathbf{Z}_5$.

26. Factor $x^4 + 2$ over $\mathbf{Z}_3$.

27. Factor $x^4 + 1$ over $\mathbf{Z}_2$, over $\mathbf{Z}_5$, over $\mathbf{Z}_7$, and over $\mathbf{Z}_{11}$.

28. Find a polynomial $q(x)$ such that $(a + bx)q(x) \equiv 1 \pmod{x^2 + 1}$ over $\mathbf{Z}_3$.

29. Let F be a field, and let $f(x), g(x) \in F[x]$, with $\deg(f(x) = n$ and $\deg(g(x) = m$, where $m < n \in \mathbf{Z}^+$. Write $n = qm + r$, where $r = 0$ or $r < m$. Show that there exist polynomials $r_0(x), r_1(x), \ldots, r_q(x)$ such $f(x) = r_q(x)g(x)^q + \ldots + r_1(x)g(x) + r_0(x)$, where $\deg(r_i(x)) < m$ for $0 \leq i \leq q$.

30. Let F be a field, and let $f(x) \in F[x]$. Prove that $f(x)$ is irreducible over F if and only if $f(x + c)$ is irreducible over F.

MORE PROBLEMS: §4.2

31. Show that $x^4 - 4x^3 + 4x^2 + 17$ has no repeated roots in $\mathbf{Q}$.

32. Show that $x^4 + 4x^2 - 4x - 3$ has no repeated roots in $\mathbf{Q}$.

33.† Over $\mathbf{Z}_3$, find $\gcd(x^5 - x^4 + x^3 - x^2,\ x^3 - x^2 + x - 1)$ and write it as a linear combination of the given polynomials.

34.† Over $\mathbf{Z}_5$, find $\gcd(x^5 + x^4 - 2x^3 - x^2 + 2x - 2,\ x^3 - x^2 + x - 1)$ and write it as a linear combination of the given polynomials.

35.† Over $\mathbf{Z}_7$, find $\gcd(x^5 + 3x^4 - 2x^3 - 3x - 3,\ x^3 - x^2 + x - 1)$ and write it as a linear combination of the given polynomials.

36.† Over $\mathbf{Q}$, find $\gcd(x^5 - 8x^4 + 25x^3 - 38x^2 + 28x - 8,\ x^5 - x^4 - 2x^3 + 2x^2 + x - 1)$ and write it as a linear combination of the given polynomials.

37. Factor $x^4 + 2$ over $\mathbf{Z}_3$

38. Factor $x^4 + x^3 + x^2 + 1$ over $\mathbf{Z}_2$.

39.† Factor $x^3 + 6$ over $\mathbf{Z}_7$.

40.† Show that $x^4 + 1$ has a proper factorization over $\mathbf{Z}_p$, for all primes p.

4.3 Existence of Roots

This section introduces congruences for polynomials, paralleling the development of congruence classes for integers. We know that if p is a prime number, then $\mathbf{Z}_p$ is a field. The corresponding construction for a polynomial $p(x)$ is denoted by $F[x]/\langle p(x)\rangle$, and Theorem 4.3.6 shows that we get a field if and only if $p(x)$ is irreducible.

This construction of fields is extremely important. It allows us to give a very careful and precise definition of the complex numbers. It also allows us to construct finite extension fields of $\mathbf{Z}_p$ that are used in algebraic coding theory and many other places. Whenever you store information on the hard drive of a computer, listen to digital music, or make a cell phone call you are making use of some sophisticated modern algebra (in the form of algebraic coding theory) to reduce the possibility of errors.

You should pay particular attention to Kronecker's theorem (Theorem 4.3.8) because it will reappear in Chapter 6 when we study extension fields in more detail.

SOLVED PROBLEMS: §4.3

25. Show that the field $F = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| \, a, b \in \mathbf{R} \right\}$ defined in Exercise 4.1.13 is isomorphic to the field of complex numbers.

26. Show that $\mathbf{Q}(\sqrt{3}i) = \{a + b\sqrt{3}i \mid a, b \in \mathbf{Q}\}$ is a field isomorphic to $\mathbf{Q}[x]/\langle x^2 + 3\rangle$.

27. Show that the following set of matrices, with entries from $\mathbf{Z}_3$, is a field isomorphic to $\mathbf{Z}_3[x]/\langle x^2 + 1\rangle$.
$$\left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ -1 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 1 & -1 \end{bmatrix} \right\} = F$$

28. Construct a field with 25 elements.

29. Find all powers of $[x]$ in $\mathbf{Z}_3[x]/\langle x^2 + x - 1\rangle$, and then find $[x]^{-1}$.

30. In $\mathbf{Z}_2[x]/\langle x^3 + x + 1\rangle$, find the multiplicative inverse of $[x + 1]$.

31. Is $[x]$ a generator of the multiplicative group of the field $\mathbf{Z}_5[x]/\langle x^2 + x + 1\rangle$? Is $[1+x]$ a generator?

32. Show that x^4+x+1 is irreducible over $\mathbf{Z}_2$. Factor x^4+x+1 over $\mathbf{Z}_2[x]/\langle x^4+x+1\rangle$.

MORE PROBLEMS: §4.3

33.† Factor $f(x) = x^5 - x^4 + x^3 - x^2$ and $g(x) = x^3 - x^2 + x - 1$ over $\mathbf{Z}_3$ and use the factorizations to find their greatest common divisor.

34.† Factor $f(x) = x^5 + x^4 - 2x^3 - x^2 + 2x - 2$ and $g(x) = x^3 - x^2 + x - 1$ over $\mathbf{Z}_5$ and use the factorizations to find their greatest common divisor.

35.† Factor $f(x) = x^5 + 3x^4 - 2x^3 - 3x - 3$ and $g(x) = x^3 - x^2 + x - 1$ over $\mathbf{Z}_7$ and use the factorizations to find their greatest common divisor.

36. Show that the set of matrices in Problem 4.1.29 is isomorphic to $\mathbf{Q}(\sqrt{3}i)$.

37.† Find a generator for the multiplicative group of the field $\mathbf{Z}_2[x]/\langle x^4+x+1\rangle$. As in the solution to Problem 32, let $[x] = \alpha$.

38.† Find the multiplicative inverses of $[1+x]$ and $[1-x]$ in $\mathbf{Z}_3[x]/\langle x^2+x+2\rangle$.

39. For $a, b \in \mathbf{Q}$, find $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}^{-1}$ when $a^2 - 2b^2 \neq 0$. Note that Exercise 4.3.12 and Exercise 4.3.15 show that the set $\left\{ \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \middle| a, b \in \mathbf{Q} \text{ and } a^2 - 2b^2 \neq 0 \right\}$ is a field isomorphic to $\mathbf{Q}[x]/\langle x^2-2\rangle$ and $\mathbf{Q}(\sqrt{2})$. Compare your answer to that of Exercise 4.3.21 (b), which asks you to find the inverse of $[a+bx]$ in $\mathbf{Q}[x]/\langle x^2-2\rangle$.

40.† Use a calculation in $\mathbf{Q}[x]/\langle x^3-2\rangle$ to rationalize the denominator of $\dfrac{1}{1-\sqrt[3]{2}+\sqrt[3]{4}}$.

4.4 Polynomials over Z, Q, R, and C

Section 4.4 returns to the setting of high school algebra. The most important theorems here are Eisenstein's irreducibility criterion for polynomials with integer coefficients (Theorem 4.4.6) and the fundamental theorem of algebra (Theorem 4.4.9), which states that any polynomial of positive degree in $\mathbf{C}[x]$ has a root in $\mathbf{C}$. Unfortunately, it is relatively hard to give a strictly algebraic proof of the fundamental theorem, so the proof has to be postponed to Chapter 8 after we have studied some Galois theory.

SOLVED PROBLEMS: §4.4

21. Factor $x^5 - 10x^4 + 24x^3 + 9x^2 - 33x - 12$ over $\mathbf{Q}$.

22. Show that $x^3 + (3m-1)x + (3n+1)$ is irreducible in $\mathbf{Q}[x]$ for all $m, n \in \mathbf{Z}$.

23. Use Eisenstein's criterion to show that $x^4 + 120x^3 - 90x + 60$ is irreducible over $\mathbf{Q}$.

24. Factor $x^8 - 1$ over $\mathbf{C}$.

25. Factor $x^4 - 2$ over $\mathbf{C}$.

26. Factor $x^3 - 2$ over $\mathbf{C}$.

MORE PROBLEMS: §4.4

27.† Find all rational roots of $f(x) = x^3 - x^2 + x - 1$.

28.† Find all rational roots of $g(x) = x^5 - 4x^4 - 2x^3 + 14x^2 - 3x + 18$.

29.† Factor the polynomials $f(x)$ and $g(x)$ in Problems 27 and 28 and use the factorizations to find $\gcd(f(x), g(x))$ in $\mathbf{Q}[x]$.

30.† Find all rational roots of $f(x) = x^5 - 8x^4 + 25x^3 - 38x^2 + 28x - 8$.

31.† Find all rational roots of $g(x) = x^5 - x^4 - 2x^3 + 2x^2 + x - 1$.

32.† Factor the polynomials $f(x)$ and $g(x)$ in Problems 30 and 31 and use the factorizations to find $\gcd(f(x), g(x))$ in $\mathbf{Q}[x]$.

33. Find all rational roots of $x^5 - 6x^4 + 3x^3 - 3x^2 + 2x - 12$.

34. Use Eisenstein's criterion to show that $x^4 - 10x^2 + 1$ is irreducible over $\mathbf{Q}$.

35.† Show that $x^4 - 4x^3 + 13x^2 - 32x + 43$ is irreducible over $\mathbf{Q}$. Use Eisenstein's criterion.

36.† Show that $x^5 + 5x^4 - 40x^2 - 75x - 48$ is irreducible over $\mathbf{Q}$. Use Eisenstein's criterion.

37. Show that $p(x) = [(x-1)(x-2)\cdots(x-n)] - 1$ is irreducible over $\mathbf{Q}$ for all integers $n > 1$.

38. Show that $x^4 - 3x^3 + 2x^2 + x + 5$ has $2 - i$ as a root in $\mathbf{C}$. Then find the other roots of $f(x)$ in $\mathbf{C}$.

39. Factor $x^6 - 1$ over $\mathbf{C}$.

The following subset of $M_2(\mathbf{C})$ is called the set of **quaternions**.

$$\mathbf{H} = \left\{ \left[\begin{array}{cc} z & w \\ -\overline{w} & \overline{z} \end{array} \right] \middle| \, z, w \in \mathbf{C} \right\}$$

If we represent the complex numbers z and w as $z = a + bi$ and $w = c + di$, then

$$\begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} = a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} + c \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} + d \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

If we let

$$1 = \left[\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right], \ \mathbf{i} = \left[\begin{array}{cc} i & 0 \\ 0 & -i \end{array} \right], \ \mathbf{j} = \left[\begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array} \right], \ \mathbf{k} = \left[\begin{array}{cc} 0 & i \\ i & 0 \end{array} \right],$$

then we can write

$$\mathbf{H} = \{a \cdot 1 + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \mid a, b, c, d \in \mathbf{R}\} \ .$$

Direct computations with the elements $\mathbf{i}, \mathbf{j}, \mathbf{k}$ show that we have the following identities:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1 \ ;$$

$$\mathbf{ij} = \mathbf{k}, \quad \mathbf{jk} = \mathbf{i}, \quad \mathbf{ki} = \mathbf{j}; \qquad \mathbf{ji} = -\mathbf{k}, \quad \mathbf{kj} = -\mathbf{i}, \quad \mathbf{ik} = -\mathbf{j} \ .$$

These identities show that $\mathbf{H}$ is closed under matrix addition and multiplication. It can be shown that $\mathbf{H}$ satisfies all of the axioms of a field, with the exception of the commutative law for multiplication.

The determinant of the matrix corresponding to $a \cdot 1 + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}$ is $z\overline{z} + w\overline{w} = a^2 + b^2 + c^2 + d^2$, and this observation shows that each nonzero element of $\mathbf{H}$ has a multiplicative inverse. The full name for $\mathbf{H}$ is the **division ring of real quaternions**. The notation $\mathbf{H}$ is used in honor of Hamilton, who discovered the quaternions after about ten years of trying to construct a field using 3-tuples of real numbers. He finally realized that if he would sacrifice the commutative law and extend the multiplication to 4-tuples then he could construct a division ring.

40.† Show that there are infinitely many quaternions that are roots of the polynomial $x^2 + 1$.

Chapter 4 Review Problems

1. Use the Euclidean algorithm to find $\gcd(x^8 - 1,\ x^6 - 1)$ in $\mathbf{Q}[x]$ and write it as a linear combination of $x^8 - 1$ and $x^6 - 1$.

2. Over the field of rational numbers, find the greatest common divisor of $2x^4 - x^3 + x^2 + 3x + 1$ and $2x^3 - 3x^2 + 2x + 2$ and express it as a linear combination of the given polynomials.

3. Are the following polynomials irreducible over $\mathbf{Q}$?

   (a) $3x^5 + 18x^2 + 24x + 6$

   (b) $7x^3 + 12x^2 + 3x + 45$

   (c) $2x^{10} + 25x^3 + 10x^2 - 30$

4. Factor $x^5 - 2x^4 - 2x^3 + 12x^2 - 15x - 2$ over $\mathbf{Q}$.

5. (a) Show that $x^2 + 1$ is irreducible over $\mathbf{Z}_3$.

   (b) List the elements of the field $F = \mathbf{Z}_3[x]/\langle x^2 + 1\rangle$.

   (c) In the multiplicative group of nonzero elements of F, show that $[x + 1]$ is a generator, but $[x]$ is not.

6. Construct an example of a field with $343 = 7^3$ elements.

7. Find the multiplicative inverse of $[x^2 + x + 1]$
   (a) in $\mathbf{Q}[x]/\langle x^3 - 2\rangle$;
   (b) in $\mathbf{Z}_3[x]/\langle x^3 + 2x^2 + x + 1\rangle$.

8. In $\mathbf{Z}_5[x]/\langle x^3 + x + 1\rangle$, find $[x]^{-1}$ and $[x+1]^{-1}$, and use your answers to find $[x^2+x]^{-1}$.

Chapter 5

COMMUTATIVE RINGS

This chapter takes its motivation from Chapter 1 and Chapter 4. We have studied some properties of the set of integers in Chapter 1, and some properties of polynomials in Chapter 4. The axioms of a commutative ring provide a general context in which to study other sets with similar properties.

We have already worked with fields in Chapter 4, so you can think of a commutative ring as a set that would like to be a field, but is missing multiplicative inverses for some of its elements. As a familiar example, compare the ring $\mathbf{Z}$ and the field $\mathbf{Q}$. In the former you can only divide by ± 1, while in $\mathbf{Q}$ you can divide by any nonzero element.

In Section 5.3 the concept of a factor ring depends heavily on the corresponding definition for groups, so you may need to review the last two sections of Chapter 3. Finally, remember that the distributive law is all that connects the two operations in a ring, so it is crucial in many of the proofs you will see.

5.1 Commutative rings; Integral Domains

This section gives some basic properties and examples of commutative rings, and introduces the important notion of an integral domain. An integral domain is a nontrivial commutative ring in which the cancellation law holds for multiplication. The most basic examples are $\mathbf{Z}$, any field F, and the polynomial ring $F[x]$. Other rings, such as $\mathbf{Z}_n$ (when n is a composite number) are not as well behaved. (Remember how carefully we had to deal with cancellation when we studied congruences in $\mathbf{Z}_n$.)

Some important definitions come from the exercises. If R is a ring, an element $a \in R$ is called nilpotent if $a^n = 0$ for some $n \in \mathbf{Z}^+$ (see Exercise 7), and idempotent if $a^2 = a$ (see Exercise 20). Then R is a Boolean ring if every element is idempotent (see Exercise 11).

If R and S are rings, their direct sum is $R \oplus S = \{(r, s) \mid r \in R, s \in S\}$, with the operations of componentwise addition and multiplication. (See Exercise 16 for the definition.)

SOLVED PROBLEMS: §5.1

23. Let R be a commutative ring. Prove the following statements (listed in Section 5.1):

(d) $a \cdot 0 = 0$ for all $a \in R$;

(e) $-(-a) = a$ for all $a \in R$;

(f) $(-a) \cdot (-b) = ab$ for all $a, b \in R$.

24. (a) Is $\mathbf{Z}_2$ a subring of $\mathbf{Z}_6$?

(b) Is $3\mathbf{Z}_6$ a subring of $\mathbf{Z}_6$?

25. (a) Show that the ring of Gaussian integers is an integral domain.

(b) Show that $\mathbf{Z}[\sqrt{2}] = \{m + n\sqrt{2} \mid m, n \in \mathbf{Z}\}$ is an integral domain.

26. Let R be a commutative ring. Prove that the intersection of any collection of subrings of R is a subring of R.

27. Show that in an integral domain the only idempotent elements are 0 and 1.

28. Show that if $n = p^k$ (p prime), then in $\mathbf{Z}_n$ the only idempotent elements are 0 and 1.

29. In $\mathbf{Z}_{24}$,

(a) find all nilpotent elements;

(b) find all idempotent elements.

30. Let R be the set of all 3×3 matrices of the form $\begin{bmatrix} a & 0 & 0 \\ b & a & 0 \\ c & b & a \end{bmatrix}$ with $a, b, c \in \mathbf{Z}$.

(a) Show that R is a commutative ring.

(b) Find the units of R.

(c) Find the nilpotent elements of R.

31. Let R and S be commutative rings. Prove or disprove the following statements.

(a) An element $(a, b) \in R \oplus S$ is idempotent if and only if a an idempotent in R and b is idempotent in S.

(b) An element $(a, b) \in R \oplus S$ is nilpotent if and only if a nilpotent in R and b is nilpotent in S.

(c) An element $(a, b) \in R \oplus S$ is a zero divisor if and only if a is a zero divisor in R and b is a zero divisor in S.

32. In the ring $\mathbf{Z} \oplus \mathbf{Z}$, let $R = \{(x, y) \mid x \equiv y \pmod 2\}$.

(a) Show that R is a subring of $\mathbf{Z} \oplus \mathbf{Z}$.

(b) Is R an integral domain?

(c) Find all idempotent elements of R.

33. Find a commutative ring with zero divisors a, b such that $a + b$ is *not* a zero divisor and $a + b \neq 0$.

34. Although the set $\mathbf{Z}_2[x]/\langle x^2+1\rangle$ is not a field, Proposition 4.3.4 shows that addition and multiplication of congruence classes of polynomials is well-defined. Show that in this set the cancellation law for multiplication does not hold.

35. Recall that $\mathbf{Z}_3[x]/\langle x^2+1\rangle$ is a field (this follows from Theorem 4.3.6 since x^2+1 is irreducible over $\mathbf{Z}_3$). Find the order of each element in its group of units.

36. Let p be an odd prime number that is not congruent to 1 modulo 4. Prove that the ring $\mathbf{Z}_p[x]/\langle x^2+1\rangle$ is a field.

    Hint: A root of $x^2 = -1$ leads to an element of order 4 in $\mathbf{Z}_p^\times$.

37. Let S be a commutative ring.

    (a) Let $R = \{n \cdot 1 \mid n \in \mathbf{Z}\}$. Show that R is a subring of S.

    (b) Find the subring defined in part (a) for the ring given in Problem 30 and for the field given in Problem 35.

38. (a) Let S be a set that satisfies all of the axioms of commutative ring, with the possible exception of the commutative law for multiplication. Show that the set $R = \{r \in S \mid rs = sr \text{ for all } s \in S\}$ is a commutative ring.

    Note: The ring R is called the **center** of S.

    (b) Find the center of the set $M_2(\mathbf{R})$ of all 2×2 matrices with real entries.

MORE PROBLEMS: §5.1

39. Give an example of an integral domain with nonzero elements a, b such that $a^2+b^2 = 0$.

40. Show that if D is an integral domain and $a^2 = b^2$ for $a, b \in D$, then $a = \pm b$.

41. Let R be a commutative ring with $a, b \in R$.

    (a) Show that if ab is a unit, then both a and b are units.

    (b) Show that if ab is a divisor of zero, then either a is a divisor of zero or b is a divisor of zero.

42.† Let R and S be commutative rings. Show that $(R \oplus S)^\times \cong R^\times \times S^\times$ (as groups).

43. Let R, S be commutative rings. Prove that $R \oplus S$ is a Boolean ring if and only if R and S are Boolean rings.

44.† Let R be a Boolean ring with 16 elements. Find $R^\times$.

45. Let R be the ring of continuous functions from $\mathbf{R}$ to $\mathbf{R}$. (Remember that R is a ring under multiplication of functions, *not* composition of functions.)

    (a) Show that R has nonzero divisors of zero.

    †(b) Characterize the units of R.

    (c) Characterize the idempotent elements of R.

    †(d) Characterize the nilpotent elements of R.

46. (a) Prove that if F is a field, then $f(x) \in F[x]$ has an inverse if and only if $f(x)$ has degree 0.

    (b) Show that if $R = \mathbf{Z}_4$, then $2x + 1$ has a multiplicative inverse in $R[x]$.

47. Show that $[1 + x]$ is a nilpotent element of $\mathbf{Z}_2[x]/\langle x^3 + x^2 + x + 1\rangle$.

48.† Let R be a commutative ring.

    (a) Can $R[x]$ have nilpotent elements of positive degree?

    (b) Can $R[x]$ have idempotent elements of positive degree?

49. Let R be a commutative ring. Show that an element $a_0 + \ldots + a_n x^n$ in $R[x]$ is a unit if and only if a_0 is a unit in R and $a_1, \ldots, a_n$ are nilpotent.

50. Let R be a commutative ring, and let x be an indeterminate. Let $R[[x]]$ denote the set of all expressions of the form $f(x) = \sum_{i=0}^{\infty} a_i x^i$ such that $a_i \in R$. If $g(x) = \sum_{i=0}^{\infty} b_i x^i$ is an element of $R[[x]]$, we define addition and multiplication as with polynomials: $f(x) + g(x) = \sum_{i=0}^{\infty} c_i x^i$, where $c_i = a_i + b_i$ for all i, and $f(x)g(x) = \sum_{i=0}^{\infty} d_i x^i$, where $d_i = \sum_{j+k=i} a_j b_k$. With these operations, $R[[x]]$ is called the **ring of formal power series** (in the indeterminate x) **over** R. Note that $R[[x]]$ contains $R[x]$ as a subring.

    (a) Show that $R[[x]]$ is a commutative ring.

    (b) Show that an element $f(x) = \sum_{i=0}^{\infty} a_i x^i$ is a unit of $R[[x]]$ if and only if a_0 is a unit of R.

5.2 Ring Homomorphisms

Ring homomorphisms are the functions that are used to relate one ring to another. Since a ring has two operations, they must respect these operations. A group homomorphism must always map the identity of the domain to the identity of the codomain, but this is not necessarily true for ring homomorphisms, and so we include it in the definition.

The fundamental homomorphism theorem is a good shortcut. When you define a mapping on equivalence classes, you must always show that it is well-defined. The fundamental homomorphism theorem does this in a general setting, so often it is possible to use it to avoid some parts of the proof that two rings are isomorphic.

SOLVED PROBLEMS: §5.2

24. (Back to Calculus) Does the derivative define a ring homomorphism from $\mathbf{R}[x]$ to $\mathbf{R}[x]$?

25. Is an isomorphism of fields a ring isomorphism?

26. Let R and S be commutative rings, and let $\phi : R \to S$ be a ring homomorphism.
    (a) Does ϕ map idempotent elements to idempotent elements?
    (b) Does ϕ map nilpotent elements to nilpotent elements?
    (c) Does ϕ map zero divisors to zero divisors?

27. Let R and S be commutative rings. Show that the set of 2×2 diagonal matrices with entries from R and S (respectively) forms a commutative ring isomorphic to $R \oplus S$.

28. Let R be a commutative ring, with identity 1.
    (a) Show that if e is an idempotent element of R, then $1 - e$ is also idempotent.
    (b) Show that if e is idempotent, then $R \cong Re \oplus R(1 - e)$.

29. Use methods of this section to find, in $\mathbf{Z}_{24}$,
    (a) all nilpotent elements;
    (b) all idempotent elements.

30. Let F be a subfield of the field E. For the element $u \in E$, define $\phi_u : F[x] \to E$ by setting by $\phi_u(f(x)) = f(u)$, for all $f(x) \in F[x]$.
    (a) Show that if $\ker(\phi_u) \neq \{0\}$, then $\ker(\phi_u) = \langle p(x) \rangle$, where $p(x)$ is the unique monic polynomial of minimal degree in $\ker(\phi_u)$.
    (b) Show that the polynomial $p(x)$ in part (a) is irreducible over F.

31. Find the kernel of the evaluation map from $\mathbf{R}[x]$ into $\mathbf{C}$ defined by
    (a) substitution of i;
    (b) substitution of $\sqrt{2}i$.

32. Use the techniques of this section to prove that $\mathbf{Q}[x]/\langle x^2 + 3 \rangle \cong \mathbf{Q}(\sqrt{3}i)$. Note: This is a repeat of Problem 4.3.26.

33. Prove that the ring of Gaussian integers $\mathbf{Z}[i]$ is isomorphic to $\mathbf{Z}[x]/\langle x^2 + 1 \rangle$.

34. Show that the ring $\mathbf{Z}[\sqrt{2}]$ has precisely two automorphisms.

35. Let F be a field, and define $\phi : F[x] \to F[x]$ by $\phi(f(x)) = f(x^2)$, for all $f(x) \in F[x]$. Show that ϕ is a one-to-one ring homomorphism that is not an automorphism of $F[x]$.

36. Find an example of an infinite integral domain that has finite characteristic.

37. What is the characteristic of $\mathbf{Z}_m \oplus \mathbf{Z}_n$?

38. Let R be a commutative ring with $\text{char}(R) = 2$. Define $\phi : R \to R$ by $\phi(x) = x^2$, for all $x \in R$.
    (a) Show that ϕ is a ring homomorphism.
    (b) Find an example of such a ring in which ϕ is an automorphism.
    (c) Find an example of such a ring in which ϕ is not onto.

39. In the multiplicative group $\mathbf{Z}_{180}^{\times}$ of the ring $\mathbf{Z}_{180}$, what is the largest possible order of an element?

40. Find all group homomorphisms $\phi : \mathbf{Z}_{120} \to \mathbf{Z}_{42}$ such that

$$\phi([a]_{120}[b]_{120}) = \phi([a]_{120})\phi([b]_{120})$$

for all $[a]_{120}, [b]_{120} \in \mathbf{Z}_{120}$.

Note: These are not ring homomorphisms, since we are not requiring that $\phi([1]_{120}) = [1]_{42}$. Exercise 5.2.15 shows that there is only one possible ring homomorphism.

MORE PROBLEMS: §5.2

41. Define $\mathbf{Z}_n[i] = \{a + bi \mid a, b \in \mathbf{Z}_n \text{ and } i^2 = -1\}$. Show that $\mathbf{Z}_n[i]$ is a commutative ring.

42. Let R and S be commutative rings, and let $\phi : R \to S$ be an onto ring homomorphism. Show that if the characteristic of R is nonzero, then $\text{char}(S)$ is a divisor of $\text{char}(R)$.

43.† Let R and S be commutative rings, and let $\phi : R \to S$ be a ring homomorphism.

(a) Give an example in which R is an integral domain but S is not.

(b) Give an example in which R is an field but S is not.

44. Let R and S be commutative rings, and let $\phi : R \to S$ be a ring homomorphism. Show that if R is a Boolean ring and ϕ is onto, then S is a Boolean ring.

45. Let R_1, R_2, S_1, and S_2 be commutative rings. Show that if $R_1 \cong R_2$ and $S_1 \cong S_2$, then $R_1 \oplus S_1 \cong R_2 \oplus S_2$.

46.† Show that if R and S are isomorphic commutative rings, then the polynomial rings $R[x]$ and $S[x]$ are isomorphic.

47. Define $\phi : \mathbf{Z}[i] \to \mathbf{Z}_5$ by $\phi(n + mi) = [n + 2m]_5$.

(a) Show that ϕ is a ring homomorphism.

(b) Find $\ker(\phi)$.

48. Prove that the ring $\mathbf{Z}[\sqrt{2}]$ is isomorphic to $\mathbf{Z}[x]/\langle x^2 - 2\rangle$.

49. Prove that $\mathbf{Q}(\sqrt{3}) \cong \mathbf{Q}[x]/\langle x^2 - 3\rangle$.

50. Prove that the ring $D = \left\{ \begin{bmatrix} m & n \\ -n & m \end{bmatrix} \middle| m, n \in \mathbf{Z} \right\}$ is isomorphic to the ring $\mathbf{Z}[i]$ of Gaussian integers.

5.3 Ideals and Factor Rings

This section considers factor rings, using results on factor groups. The analogy to the material in Section 3.8 is a very close one, and the first goal is to determine which subsets of a ring will play the same role as that of normal subgroups of a group. These are the *ideals* of the ring, which correspond to the kernels of ring homomorphisms from the ring to other rings. (Remember that normal subgroups are precisely the kernels of group homomorphisms.)

The most important examples of principal ideal domains are the ring $\mathbf{Z}$, in which any nonzero ideal I is generated by the smallest positive integer in I, and the ring $F[x]$ of polynomials over a field F, in which any nonzero ideal I is generated by the monic polynomial of minimal degree in I.

Let I and J be ideals of the commutative ring R. Exercise 5.3.13 shows that the **sum** of I and J, denoted

$$I + J = \{x \in R \mid x = a + b \text{ for some } a \in I, b \in J\} ,$$

is an ideal of R. Exercise 5.3.14 defines the **product** of the ideals I and J, which is a bit more complicated:

$$IJ = \{\textstyle\sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J, n \in \mathbf{Z}^+\} \ .$$

The product IJ is also an ideal of R. Exercise 5.3.11 defines the **annihilator** of $a \in R$ to be $\text{Ann}(a) = \{x \in R \mid xa = 0\}$.

SOLVED PROBLEMS: §5.3

27. Give an example to show that the set of all zero divisors of a commutative ring need not be an ideal of the ring.

28. Show that in $\mathbf{R}[x]$ the set of polynomials whose graph passes through the origin and is tangent to the x-axis at the origin is an ideal of $\mathbf{R}[x]$.

29. To illustrate Proposition 5.3.7 (b), give the lattice diagram of ideals of $\mathbf{Z}_{100} = \mathbf{Z}/\langle 100\rangle$, and the lattice diagram of ideals of $\mathbf{Z}$ that contain $\langle 100\rangle$.

30. Let R be the ring $\mathbf{Z}_2[x]/\langle x^3 + 1\rangle$.
    (a) Find all ideals of R.
    (b) Find the units of R.
    (c) Find the idempotent elements of R.

31. Let S be the ring $\mathbf{Z}_2[x]/\langle x^3 + x\rangle$.
    (a) Find all ideals of S.
    (b) Find the units of S.
    (c) Find the idempotent elements of S.

32. Show that the rings R and S in Problems 30 and 31 are isomorphic as abelian groups, but not as rings.

33. Let I, J be ideals of the commutative ring R, and for $r \in R$, define the function $\phi : R \to R/I \oplus R/J$ by $\phi(r) = (r + I, r + J)$.
    (a) Show that ϕ is a ring homomorphism, with $\ker(\phi) = I \cap J$.
    (b) Show that if $I + J = R$, then ϕ is onto, and thus $R/(I \cap J) \cong R/I \oplus R/J$.

34. Let I, J be ideals of the commutative ring R. Show that if $I+J = R$, then $I^2+J^2 = R$.

35. Show that $\langle x^2 + 1\rangle$ is a maximal ideal of $\mathbf{R}[x]$.

36. Is $\langle x^2 + 1\rangle$ a maximal ideal of $\mathbf{Z}_2[x]$?

37. Let R and S be commutative rings, and let $\phi : R \to S$ be a ring homomorphism.
    (a) Show that if I is an ideal of S, then $\phi^{-1}(I) = \{a \in R \mid \phi(a) \in I\}$ is an ideal of R.
    (b) Show that if P is a prime ideal of S, then $\phi^{-1}(P)$ is a prime ideal of R.

38. Prove that in a Boolean ring every prime ideal is maximal.

39. In $R = \mathbf{Z}[i]$, let $I = \{m + ni \mid m \equiv n \pmod 2\}$.
    (a) Show that I is an ideal of R.
    (b) Find a familiar commutative ring isomorphic to R/I.

MORE PROBLEMS: §5.3

40. To illustrate Proposition 3.5.7 (b), give the lattice diagram of ideals of $\mathbf{Z}_{45}$ and the lattice diagram of ideals of $\mathbf{Z}$ that contain $\langle 45\rangle$.

41. Let R and S be commutative rings, and let $\phi : R \to S$ be a ring homomorphism. Show that if ϕ is onto and every ideal of R is a principal ideal, then the same condition holds in S.

42. Show that if I, J are ideals of the commutative ring R with $I+J = R$, then $I\cap J = IJ$.

43. Let I, J be ideals of the commutative ring R. Show that $\{r \in R \mid rx \in J \text{ for all } x \in I\}$ is an ideal of R.

44. Prove that $R/\{0\}$ is isomorphic to R, for any commutative ring R.

45.† Let P and Q be maximal ideals of the commutative ring R. Show that $R/(P \cap Q) \cong R/P \oplus R/Q$.

46. Suppose that $\{I_n\}_{n\in\mathbf{N}}$ is a set of ideals of the commutative ring R such that $I_n \subset I_m$ whenever $n \leq m$. Prove that $\cup_{n\in\mathbf{N}} I_n$ is an ideal of R.

47. Let R be the set of all 3×3 matrices of the form $\begin{bmatrix} a & 0 & 0 \\ b & a & 0 \\ c & b & a \end{bmatrix}$ with $a, b, c \in \mathbf{Z}$. (See Problem 5.1.27.) Let I be the subset of R consisting of all matrices with $a = 0$. Show that $I^2 \neq (0)$ but $I^3 = (0)$.

48.† Show that in $\mathbf{Z}[\sqrt{2}]$ the principal ideal generated by $\sqrt{2}$ is a maximal ideal.

49. In $R = \mathbf{Z}[i]$, let I be the principal ideal generated by 5. Prove that $R/I \cong \mathbf{Z}_5 \oplus \mathbf{Z}_5$.

50. Let R be a commutative ring, and let I, J, K be ideals of R. Prove the following facts.
    (a) $(IJ)K = I(JK)$
    (b) $(I \cdot (J \cap K) \subseteq IJ \cap IK$
    (c) $I \cap (J + K) \supset (I \cap J) + (I \cap K)$
    (d) $I + (J \cap K) \subset (I + J) \cap (I + K)$

5.4 Quotient Fields

We know that any subring of a field is an integral domain. This section contains a converse: any integral domain is isomorphic to a subring of a field. The proof constructs a field that is as small as possible, and this field contains no more elements than absolutely necessary to provide inverses for the elements of the domain. The example to keep in mind is that of the ring $\mathbf{Z}$ thought of as a subring of the field $\mathbf{Q}$.

SOLVED PROBLEMS: §5.4

15. Let F be a field. Explain why $Q(F)$ is isomorphic to F. Why can't we just say that $Q(F) = F$?

16. Find the quotient field of $\mathbf{Z}_2[x]$.

17. Prove that if D_1 and D_2 are isomorphic integral domains, then $Q(D_1) \cong Q(D_2)$.

MORE PROBLEMS: §5.4

18.† Find the quotient field of $\mathbf{Z}[\sqrt{3}i]$.

19.† Find the quotient field of $D = \left\{ \begin{bmatrix} m & n \\ -3n & m \end{bmatrix} \middle| m, n \in \mathbf{Z} \right\}$.

20.† Find the quotient field of $D = \left\{ \begin{bmatrix} m & n \\ -n & m \end{bmatrix} \middle| m, n \in \mathbf{Z} \right\}$.

21. Let R be a set that satisfies all properties of a commutative ring, with the exception of the existence of an identity element 1. Show that if R has no nonzero divisors of zero, then it has a quotient field (which must necessarily contain an identity element).

22. Let R be a commutative ring. A nonempty subset S of R is called a **multiplicative set** if $ab \in S$ for all $a, b \in S$, and $0 \notin S$.

    (a) Let S be a multiplicative set of R. Show that the relation defined on $R \times S$ by $(a, c) \sim (b, d)$ if $s(ad - bc) = 0$ for some $s \in S$ is an equivalence relation.

    (b) Denote the equivalence class of $(a, c) \in R \times S$ by $[a, c]$, and denote the set of equivalence classes by R_S. Show that the following addition and multiplication of equivalence classes is well-defined, for $a, b \in R$ and $c, d \in S$.

$$[a, c] + [b, d] = [ad + bc, cd] \quad \text{and} \quad [a, c] \cdot [b, d] = [ab, dc] \; .$$

    (c) Show that R_S is a commutative ring under the above operations.

Chapter 5 Review Problems

1. Let R be the ring with 8 elements consisting of all 3×3 matrices with entries in $\mathbf{Z}_2$ which have the following form:

$$\begin{bmatrix} a & 0 & 0 \\ 0 & a & 0 \\ b & c & a \end{bmatrix}$$

    You may assume that the standard laws for addition and multiplication of matrices are valid.

    (a) Show that R is a commutative ring (you only need to check closure, the existence of a 1, and commutativity of multiplication).

    (b) Find all units of R, and all nilpotent elements of R.

    (c) Find all idempotent elements of R.

2. Let R be the ring $\mathbf{Z}_2[x]/\langle x^2 + 1 \rangle$. Show that although R has 4 elements, it is not ring isomorphic to either $\mathbf{Z}_4$ or $\mathbf{Z}_2 \oplus \mathbf{Z}_2$.

3. Let R and S be commutative rings. Prove that $R \oplus S \cong S \oplus R$.

4. For the element $a = (0, 2)$ of the ring $R = \mathbf{Z}_{12} \oplus \mathbf{Z}_8$, find $\text{Ann}(a) = \{r \in R \mid ra = 0\}$. Check that $\text{Ann}(a)$ is an ideal of R.

5. Let R be the ring $\mathbf{Z}_2[x]/\langle x^4 + 1 \rangle$, and let I be the set of all congruence classes in R of the form $[f(x)(x^2 + 1)]$.

    (a) Show that I is an ideal of R.

(b) Show that $R/I \cong \mathbf{Z}_2[x]/\langle x^2+1\rangle$.

(c) Is I a prime ideal of R?

Hint: If you use the fundamental homomorphism theorem, you can do the first two parts together.

6. Find all maximal ideals, and all prime ideals, of $\mathbf{Z}_{36} = \mathbf{Z}/36\mathbf{Z}$.

7. Let I be the subset of $\mathbf{Z}[x]$ consisting of all polynomials with even coefficients. Prove that I is a prime ideal; prove that I is not maximal.

8. Let $\mathbf{Z}[i]$ be the ring of Gaussian integers, i.e. the subring of $\mathbf{C}$ given by

$$\mathbf{Z}[i] = \{m + ni \in \mathbf{C} \mid m, n \in \mathbf{Z}\} .$$

(a) Define $\phi : \mathbf{Z}[i] \to \mathbf{Z}_2$ by $\phi(m+ni) = [m+n]_2$. Prove that ϕ is a ring homomorphism. Find $\ker(\phi)$ and show that it is a principal ideal of $\mathbf{Z}[i]$.

(b) For any prime number p, define $\theta : \mathbf{Z}[i] \to \mathbf{Z}_p[x]/\langle x^2+1\rangle$ by $\theta(m+ni) = [m+nx]$. Prove that θ is an onto ring homomorphism.

Chapter 6

Fields

Solving polynomial equations has motivated a great deal of work in algebra. Although problems leading to quadratic equations were considered by the Babylonians, it wasn't until 1145 that a book containing the complete solution to the general quadratic was published in Europe. The familiar quadratic formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

gives a solution of the equation $ax^2+bx+c = 0$ (where $a \neq 0$) in terms of its coefficients and extraction of a square root. An equation $a_n x^n + \ldots + a_1 x + a_0 = 0$ is said to be **solvable by radicals** if its solutions can be given in a form that involves sums, differences, products, or quotients of the coefficients a_n, ..., a_1, a_0, together with the possible use of square roots, cube roots, etc., of such combinations of the coefficients.

In 1798, Paolo Ruffini (1765–1822) published a proof claiming to show that there are polynomial equations of degree five that are not solvable by radicals. The general idea was correct, but there were gaps in the proof, and it was not until 1826 that a correct proof was finally given by Niels Abel (1802–1829). Evariste Galois (1811-1832) determined exactly which polynomial equations are solvable by radicals. He considered certain permutations of the roots of a polynomial—those that leave the coefficients fixed—and showed that the equation is solvable by radicals if and only if the associated group of permutations has a particularly nice structure.

Galois theory has deep and very beautiful results, and our text **Abstract Algebra** was written with Galois theory as its ultimate goal. This study guide (intended for students just beginning to study modern algebra) ends in the middle of this chapter, but the website for the text includes a study guide for Galois theory and more advanced topics in group theory. To learn more about the history of algebra, and about the major contributors to the field, you can explore the math history site maintained by the University of St. Andrews.

If you are studying abstract algebra because you plan to be a high school teacher, the sections most directly relevant to teaching algebra are Sections 6.1 and 6.2 on field extensions, Section 6.3 on geometric constructions, and the earlier material in Chapter 4 on polynomials. But remember that the study of general operations (as in group theory) is also important, and provides the foundation for all of algebra.

6.1 Algebraic Elements

In this section we often start with a known field K, and then construct a larger field F. Recall Definition 4.3.1: the field F is said to be an *extension field* of the field K if K is a subset of F which is a field under the operations of F. Equivalently, K is a *subfield* of F, often called the *base field* in this situation. If $u \in F$ is a root of some nonzero polynomial $f(x) \in K[x]$, and $p(x)$ has minimal degree among all polynomials of which u is a root, then we can use the division algorithm to show that $p(x) \mid f(x)$. It is very useful to know that the field $K(u)$ is isomorphic to $K[x]/\langle p(x)\rangle$, so that calculations can be done in either field.

SOLVED PROBLEMS: §6.1

13. Let u be a root of the polynomial $x^3 + 3x + 3$. In $\mathbf{Q}(u)$, express $(7 - 2u + u^2)^{-1}$ in the form $a + bu + cu^2$.

14. Find the minimal polynomial of the real number $1 + \sqrt[3]{2}$ over $\mathbf{Q}$.

15. Find the minimal polynomial of the complex number $1 + \sqrt{3}i$ over $\mathbf{Q}$.

16. (a) Show that $\mathbf{Q}(\sqrt{2} + i) = \mathbf{Q}(\sqrt{2}, i)$.
    (b) Find the minimal polynomial of the complex number $\sqrt{2} + i$ over $\mathbf{Q}$.

17. Show that the polynomial $f(x) = x^2 + x - 1$ is irreducible over the field $K = \mathbf{Z}_3$, but has two roots in the extension field $F = \mathbf{Z}_3[x]/\langle x^2 + 1\rangle$.

18. Let F be an extension field of K. Let G be the set of all automorphisms $\phi : F \to F$ such that $\phi(x) = x$ for all $x \in K$. Show that G is a group (under composition of functions).

MORE PROBLEMS: §6.1

19. Find the minimal polynomial of the complex number $\sqrt{2} + \sqrt{3}i$ over $\mathbf{Q}$.

20. Find $[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}(\sqrt{6})]$.

21. Let $a + bi$ be a complex number that is algebraic over $\mathbf{Q}$. Show that $\sqrt{a + bi}$ is algebraic over $\mathbf{Q}$, and find its minimal polynomial over $\mathbf{Q}$ in terms of the minimal polynomial of $a + bi$ over $\mathbf{Q}$.

22. Let F be an extension field of K, and let $u \in F$. Show that if $f(u)$ is algebraic over K for some $f(x) \in K[x]$, then u itself is algebraic over K.

23. Let a and b be nonzero rational numbers. Show that $\mathbf{Q}(\sqrt{a}) = \mathbf{Q}(\sqrt{b})$ if and only if there exists $c \in \mathbf{Q}$ with $a = bc^2$.

24. Let F be an extension field of K, and let $u, v \in F$. Prove that $K(u, v) = K(v, u)$.

25. Show that if u and v are transcendental over $\mathbf{Q}$, then either uv or $u+v$ is transcendental over $\mathbf{Q}$.

6.2 Finite and Algebraic Extensions

Never underestimate the power of counting something. If E is a finite extension of K and F is a finite extension of E, then F is a finite extension of K, and $[F : K] = [F : E][E : K]$.

SOLVED PROBLEMS: §6.2

12. Show that $x^3 + 6x^2 - 12x + 2$ is irreducible over $\mathbf{Q}$, and remains irreducible over $\mathbf{Q}(\sqrt[5]{2})$.

13. Find a basis for $\mathbf{Q}(\sqrt{5}, \sqrt[3]{5})$ over $\mathbf{Q}$.

14. Show that $[\mathbf{Q}(\sqrt{2} + \sqrt[3]{5}) : \mathbf{Q}] = 6$.

15. Find $[\mathbf{Q}(\sqrt[7]{16} + 3\sqrt[7]{8}) : \mathbf{Q}]$.

16. Find the degree of $\sqrt[3]{2} + i$ over $\mathbf{Q}$. Does $\sqrt[4]{2}$ belong to $\mathbf{Q}(\sqrt[3]{2} + i)$?

17. Let F be a field whose multiplicative group $F^\times$ is cyclic. Prove that F must be a finite field.

18. Let F be a finite field of characteristic p. Show that F has p^n elements, for some positive integer n.

MORE PROBLEMS: §6.2

19.† Over $\mathbf{Z}_2$, factor $x^4 - x$, $x^8 - x$, and $x^{16} - x$.

20. For any real numbers a, b, show that $\mathbf{Q}(\sqrt{a} + \sqrt{b}) = \mathbf{Q}(\sqrt{a}, \sqrt{b})$.

    Note: This extends Exercise 6.2.9, where it is assumed that $a, b \in \mathbf{Z}^+$.

21.† In the finite field $F = \mathbf{Z}_2[x]/\langle x^4 + x + 1\rangle$, find a subfield K with 4 elements.

22.† Suppose that E and F are extension fields of $\mathbf{Z}_2$, with $\mathbf{Z}_2 \subset E \subset F$. Given that $[E : \mathbf{Z}_2] = 2$ and $[F : E] = 3$, find $|E|$ and $|F|$.

23. Show that if u is an algebraic number, then so is u^r, for any rational number r.

24. Let F be an extension field of K, with $u, v \in F$. Show that if u and v are algebraic of degree m and n over K, respectively, where $\gcd(m, n) = 1$, then $[K(u, v) : K] = mn$.

25. Let F be an extension field of K, and let $f(x) \in K[x]$ be a polynomial of degree $n > 0$. If $r_1, \ldots, r_n \in F$ are roots of $f(x)$, show that $[K(r_1, r_2, \ldots r_n) : K] \leq n!$.

6.3 Geometric Constructions

This section uses facts about finite extension fields to demonstrate the impossibility of several geometric constructions studied in antiquity. The constructions use only a straightedge and compass, not a ruler, and the compass cannot be used to transfer lengths.

There is no general method for trisecting an angle, since a 20° angle cannot be constructed. Secondly, given a circle, there is no general way to to construct a square with the same area. Finally, given a cube, it is not generally possible to construct a cube with double the volume of the given cube.

Since the constructions involve only a straightedge and compass, they are limited to the following: (i) constructing a line through two points whose coordinates are known, (ii) constructing a circle with center at a point with known coordinates and passing though a point with known coordinates, and (iii) finding the points of intersection of given lines and circles.

MORE PROBLEMS: §6.3

5. Show that an angle θ is constructible if and only if $\sin\theta$ is constructible.

6. Show that $\cos\theta$ is constructible if and only if $\sin\theta$ is constructible.

Chapter 1

Integers

1.1 Divisors

25. Let a be an integer. Show that if $2 \mid a$ and $3 \mid a$, then $6 \mid a$.

    Solution: Suppose that $2 \mid a$ and $3 \mid a$. Then we know from Definition 1.1.1 that there are integers q_1 and q_2 with $a = 2q_1$ and $a = 3q_2$. (Note that we need to use different symbols for the two factors q_1 and q_2, because we can't assume that they are equal. A common mistake is to mimic the definition and write $a = 2q$ and $a = 3q$, giving two equations that would be correct only if $a = 0$ and $q = 0$.)

    Since $a = 2q_1$ and $a = 3q_2$, we must have $2q_1 = 3q_2 = 2q_2 + q_2$, so solving for q_2 gives us $q_2 = 2q_1 - 2q_2 = 2(q_1 - q_2)$. We want to show that we can factor 6 out of a, so let's start with the equation $a = 3q_2$. Then we can substitute our expression for q_2, to get $a = 3(2(q_1 - q_2)) = 6(q_1 - q_2)$. This shows (by applying Definition 1.1.1) that $6 \mid a$.

    Comment: This proof will be reduced to a one line proof after we develop some shortcuts (theorems) in the next section.

26. Prove that if m and n are odd integers, then $m^2 - n^2$ is divisible by 4.

    Solution: First, we need to use the given information about m and n. Since they are odd, we can write them in the form $m = 2k + 1$ and $n = 2q + 1$, for some integers k and q. We can factor $m^2 - n^2$ to get $(m + n)(m - n)$, so substituting for m and n we get

    $$m^2 - n^2 = (2k + 1 + 2q + 1)(2k + 1 - 2q - 1) = (2)(k + q + 1)(2)(k - q) \ .$$

    Thus $m^2 - n^2 = 4(k + q + 1)(k - q)$, showing that $4 \mid (m^2 - n^2)$.

    Comment: See Problem 1.2.36 for a sharper result.

27. Prove that if a and b are nonzero integers for which $a|b$ and $b|a$, then $b = \pm a$.

    Comment: The first step is to use Definition 1.1.1 to rewrite $a|b$ and $b|a$ as equations, to give something concrete to work with. You will need to use the cancellation property for integers (listed in Proposition A.3.6 in Appendix A.3 of **Abstract Algebra**).

Solution: Since $a \mid b$, there is an integer m with $b = ma$. Since $b \mid a$, there is an integer k with $a = kb$. Substituting $a = kb$ in the equation $b = ma$, we get $b = m(kb)$, so since b is nonzero we can cancel it to get $1 = mk$. Since both m and k are integers, and $|1| = |m|\,|k|$, we must have $|m| = 1$ and $|k| = 1$, so either $b = a$ or $b = -a$.

28. Prove that if a, b, c are integers for which $a \mid b$ and $a \mid c$, then $a^2 \mid bc$.

Solution: Assume that $a \mid b$ and $a \mid c$. Then by definition there exist integers k and q with $b = aq$ and $c = ak$. Since we need to show that bc has a^2 as a factor, we need an expression for bc. Multiplying the equations gives us $bc = (aq)(ak) = a^2(qk)$. This shows that $a^2 \mid bc$, as required.

29. Find $\gcd(435, 377)$, and express it as a linear combination of 435 and 377.

Comment: You definitely can't avoid learning how to do these computations.

Solution: We will use the Euclidean algorithm. Divide the larger number by the smaller, which gives you a quotient of 1 and a remainder of 58. Then divide the remainder 58 into 377, and continue using the division algorithm, as shown below. You then have the following equations.

$$\begin{aligned} 435 &= 1 \cdot 377 + 58 \\ 377 &= 6 \cdot 58 + 29 \\ 58 &= 2 \cdot 29 \end{aligned} \qquad \begin{aligned} \gcd(435, 377) &= \gcd(377, 58) \\ &= \gcd(58, 29) \\ &= 29 \end{aligned}$$

The repeated divisions show that $\gcd(435, 377) = 29$, since the remainder in the last equation is 0. To write 29 as a linear combination of 435 and 377 we need to use the same equations, but we need to solve them for the remainders.

$$\begin{aligned} 58 &= 435 - 1 \cdot 377 \\ 29 &= 377 - 6 \cdot 58 \end{aligned}$$

Now take the equation involving the remainder 29, and substitute for 58, the remainder in the previous equation.

$$\begin{aligned} 29 &= 377 - 6 \cdot 58 \\ &= 377 - 6 \cdot (435 - 1 \cdot 377) \\ &= 7 \cdot 377 - 6 \cdot 435 \end{aligned}$$

This gives us the linear combination we are looking for: $29 = (7)(377) + (-6)(435)$.

30. Find $\gcd(3553, 527)$, and express it as a linear combination of 3553 and 527.

Comment: This time we will use the matrix form of the Euclidean algorithm. You should be able to use both the back-solving form (as in Problem 29) and the matrix form. In Chapter 4 the Euclidean algorithm is used for polynomials, and there the matrix method gets too complicated, so you will *have* to use the back-solving method.

Solution: The first step is to divide the smaller number into the larger, giving $3553 = 6 \cdot 527 + 391$, and this tells us to multiply the bottom row of the matrix $\begin{bmatrix} 1 & 0 & 3553 \\ 0 & 1 & 527 \end{bmatrix}$

by 6 and subtract from the first row. Remember the goal: to use row operations to minimize the entries in the right hand column (keeping them ≥ 0). Guided by repeated use of the division algorithm, we have

$$\begin{bmatrix} 1 & 0 & 3553 \\ 0 & 1 & 527 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -6 & 391 \\ 0 & 1 & 527 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -6 & 391 \\ -1 & 7 & 136 \end{bmatrix} \rightsquigarrow$$

$$\begin{bmatrix} 3 & -20 & 119 \\ -1 & 7 & 136 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 3 & -20 & 119 \\ -4 & 27 & 17 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 31 & -209 & 0 \\ -4 & 27 & 17 \end{bmatrix}.$$

Therefore $\gcd(3553, 527) = 17$, and $17 = (-4)(3553) + (27)(527)$.

31. Which of the integers $0, 1, \ldots, 10$ can be expressed in the form $12m + 20n$, where m, n are integers?

Solution: Theorem 1.1.6 provides the answer. An integer k is a linear combination of 12 and 20 if and only if it is a multiple of their greatest common divisor, which is 4. Therefore we can express 0, 4, and 8 in the required form, but we can't do it for the rest.

Comment: Check out the answer in concrete terms. We can write

$0 = 12 \cdot 0 + 20 \cdot 0$; $4 = 12 \cdot 2 + 20 \cdot (-1)$; $8 = 12 \cdot (-1) + 20 \cdot 1$.

32. If n is a positive integer, find the possible values of $\gcd(n, n + 10)$.

Solution: Let $d = \gcd(n, n+10)$. Then $d|n$ and $d|(n+10)$, so we must have $d|10$, and therefore d is limited to one of 1, 2, 5, or 10. Can each of these occur for some n?

Yes: $\gcd(3, 13) = 1$; $\gcd(2, 12) = 2$; $\gcd(5, 15) = 5$; $\gcd(10, 20) = 10$.

33. Prove that if n is an integer with $n > 1$, then either $\gcd(n - 1, n^2 + n + 1) = 1$ or $\gcd(n - 1, n^2 + n + 1) = 3$.

Comment: It's not a bad idea to check this out for some values of n, just to get a feeling for the problem. For $n = 3$, we have $\gcd(2, 13) = 1$. For $n = 4$, we have $\gcd(3, 21) = 3$. For $n = 5$, we have $\gcd(4, 31) = 1$. For $n = 6$, we have $\gcd(5, 43) = 1$. For $n = 7$, we have $\gcd(6, 57) = 1$. These examples don't prove anything, but maybe they do make the problem look plausible, and they show that both 1 and 3 can occur as the greatest common divisor.

The solution to Problem 32 gives a hint as to a possible method for solving the problem. In that problem, since the gcd was a divisor of n and $n + 10$, it had to be a divisor of 10. To use the same approach, we would have to write $n^2 + n + 1$ as $n - 1$ plus something. That doesn't work, but we are very close to a way to approach the problem.

Solution: Using long division of polynomials to divide $n^2 + n + 1$ by $n - 1$, we get a quotient of $n + 2$ and a remainder of 3, so $n^2 + n + 1 = (n + 2)(n - 1) + 3$. This gives us the linear combination $3 = (1)(n^2 + n + 1) + (-n - 2)(n + 1)$, and so Theorem 1.1.6 shows that 3 is a multiple of the gcd, which means that the answer has to be 1 or 3.

Alternate Solution: If we continue using long division, with the Euclidean algorithm in mind, the long division in the first solution shows that $\gcd(n^2+n+1, n-1) = \gcd(n-1, 3)$. We can conclude that the greatest common divisor is a divisor of 3.

34. Prove that if k is a positive odd integer, then any sum of k consecutive integers is divisible by k.

Solution: We can represent the k consecutive integers as $n+1$, $n+2$, ..., $n+k$. Then

$$\sum_{i=1}^{k}(n+i) = \sum_{i=1}^{k} n + \sum_{i=1}^{k} i = kn + \tfrac{k(k+1)}{2}$$

and since k is odd, it follows that $k+1$ is divisible by 2, say $k+1 = 2q$, for some integer q. Thus $\sum_{i=1}^{k}(n+i) = kn + k(2q)/2 = k(n+q)$, completing the proof.

Comment: If you've forgotten the formula $1+2+\ldots+k = k(k+1)/2$, you can find it in Example A.4.1 of Appendix A.4 in **Abstract Algebra**. The example includes a proof of the formula, using mathematical induction.

35. Prove that if n is a positive integer, then $\begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}^n = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

if and only if $4|n$.

Comment: Let's use A for the matrix, and I for the identity matrix. The proof must be given in two pieces. We need to show that if $4|n$, then $A^n = I$. We also need to show that $A^n = I$ *only* when $4|n$, and this is easier to state as the *converse* of the first statement: if $A^n = I$, then $4|n$. The first half of the proof is easier than the second, since it just takes a computation. In the second half of the proof, if $A^n = I$ then we will use the division algorithm, to divide n by 4, and then show that the remainder has to be 0.

Solution: We begin by computing A^2, $A^3 = A \cdot A^2$, $A^4 = A \cdot A^3$, etc.

$$\begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}^3 = \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}\begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}^4 = \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Now we can see that if $4|n$, say $n = 4q$, then $A^n = A^{4q} = (A^4)^q = I^q = I$.

Conversely, if $A^n = I$, we can use the division algorithm to write $n = 4q + r$, with r equal to one of $0, 1, 2, 3$. Then $A^r = A^{n-4q} = A^n(A^4)^{-q} = I \cdot I^{-q} = I$, so $r = 0$ since A, A^2, and A^3 are not equal to I. We conclude that $4|n$.

36. For the complex number $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, prove that $\omega^n = 1$ if and only if $3|n$, for any integer n.

Solution: Since $(a+bi)(c+di) = (ac-bd)+(ad+bd)i$, a short calculation shows that $\omega^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$, and $\omega^3 = 1$. If $n \in \mathbf{Z}$, and $3|n$, then $n = 3q$ for some $q \in \mathbf{Z}$. Then $\omega^n = \omega^{3q} = (\omega^3)^q = 1^q = 1$. Conversely, if $n \in \mathbf{Z}$ and $\omega^n = 1$, use the division algorithm to write $n = q \cdot 3 + r$, where the remainder satisfies $0 \leq r < 3$. Then $1 = \omega^n = \omega^{3q+r} = (\omega^3)^q\omega^r = \omega^r$. Since $r = 0, 1, 2$ and we have shown that $\omega \neq 1$ and $\omega^2 \neq 1$, the only possibility is $r = 0$, and therefore $3|n$.

37. Give a proof by induction to show that each number in the sequence 12, 102, 1002, 10002, ..., is divisible by 6.

Comment: If you are unsure about doing a proof by induction, you should read Appendix A.4 in **Abstract Algebra**.

Solution: To give a proof by induction, we need a statement that depends on an integer n. We can write the numbers in the given sequence in the form $10^n + 2$, for $n = 1, 2, \ldots$, so we can prove the following statement: for each positive integer n, the integer $10^n + 2$ is divisible by 6.

The first step is to check that the statement is true for $n = 1$. (This "anchors" the induction argument.) Clearly 12 is divisible by 6.

The next step is to prove that if we assume that the statement is true for $n = k$, then we can show that the statement must also be true for $n = k + 1$. Let's start by assuming that $10^k + 2$ is divisible by 6, say $10^k + 2 = 6q$, for some $q \in \mathbf{Z}$, and then look at the expression when $n = k + 1$. We can easily factor a 10 out of 10^{k+1}, to get $10^{k+1} + 2 = (10)(10^k) + 2$, but we need to involve the expression $10^k + 2$ in some way. Adding and subtracting 20 makes it possible to get this term, and then it turns out that we can factor out 6.

$$\begin{aligned} 10^{k+1} + 2 &= (10)(10^k) + 20 - 20 + 2 \;=\; (10)(10^k + 2) - 18 \\ &= (10)(6q) - (6)(3) \;=\; (6)(10q - 3) \end{aligned}$$

We have now shown that if $10^k + 2$ is divisible by 6, then $10^{k+1} + 2$ is divisible by 6. This completes the induction argument.

38. Give a proof by induction to show that $5^{2n} - 1$ is divisible by 24, for all positive integers n.

Solution: For $n = 1$, we have $5^{2n} - 1 = 24$, so the result certainly holds in this case.

Next, assume that the result holds for $n = k$. For $n = k + 1$, we have the following expression.

$$\begin{aligned} 5^{2(k+1)} - 1 &= (5^{2k})(5^2) - 1 \;=\; (5^{2k})(25) - 25 + 25 - 1 \\ &= (5^{2k} - 1)(25) + 24 \end{aligned}$$

By the induction hypothesis, 24 is a factor of $5^{2k} - 1$, and so it follows that 24 is a factor of $5^{2(k+1)} - 1$, completing the induction argument.

ANSWERS AND HINTS

39. Find the quotient and remainder when a is divided by b.
(a) $a = 12345$, $b = 100$ *Answer:* $q = 123$ and $r = 45$
(b) $a = -12345$, $b = 100$ *Answer:* $q = -124$ and $r = 55$

40. Find $\gcd(252, 180)$ and write it as a linear combination of 252 and 180.
Answer: $\gcd(252, 180) = 36 = (-2)(252) + (3)(180)$
Comment: If your linear combination is different, that doesn't mean your answer is necessarily wrong, because you can add multiples of $0 = (5)(252) + (-7)(180)$ to the given linear combination.

41. Find $\gcd(475, 385)$ and express it as a linear combination of 475 and 385.
Answer: $\gcd(475, 385) = 5 = (30)(475) + (-37)(385)$
Note: $0 = (-77)(475) + (95)(385)$

43. Find $\gcd(5917, 4331)$ and express it as a linear combination of 5917 and 4331.
Answer: $\gcd(5917, 4331) = 61 = (-30)(5917) + (41)(4331)$
Note: $0 = (71)(5917) + (-97)(4331)$

1.2 Primes

26. (a) Use the Euclidean algorithm to find $\gcd(1776, 1492)$.

Solution: We have $1776 = 1492 \cdot 1 + 284$; $1492 = 284 \cdot 5 + 72$;

$284 = 72 \cdot 3 + 68$; $72 = 68 \cdot 1 + 4$; $68 = 4 \cdot 17$. Thus $\gcd(1776, 1492) = 4$.

(b) Use the prime factorizations of 1776 and 1492 to find $\gcd(1776, 1492)$.

Solution: Since $1776 = 2^4 \cdot 3 \cdot 37$ and $1492 = 2^2 \cdot 373$, Proposition 1.2.10 shows that $\gcd(1776, 1492) = 2^2$. Showing that 373 is prime takes a bit of work. You need to check that it is not divisible by any prime number smaller than $\sqrt{373} \sim 19.3$.

27. (a) Use the Euclidean algorithm to find $\gcd(1274, 1089)$.

Solution: We have $1274 = 1089 \cdot 1 + 185$; $1089 = 185 \cdot 5 + 164$;

$185 = 164 \cdot 1 + 21$; $164 = 21 \cdot 7 + 17$; $21 = 17 \cdot 1 + 4$; $17 = 4 \cdot 4 + 1$.

Thus $\gcd(1274, 1089) = 1$.

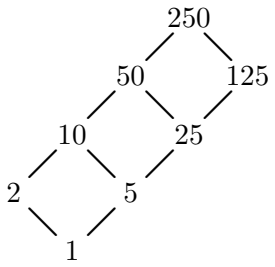
(b) Use the prime factorizations of 1274 and 1089 to find $\gcd(1274, 1089)$.

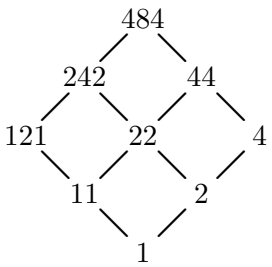
Solution: Since $1274 = 2 \cdot 7^2 \cdot 13$ and $1089 = 3^2 \cdot 11^2$, we see that 1274 and 1089 are relatively prime.

28. Give the diagram of all divisors of 250. Do the same for 484.

Solution: The prime factorizations are $250 = 2 \cdot 5^3$ and $484 = 2^2 \cdot 11^2$. In each diagram, we need to use one axis for each prime. Then we can just divide (successively) by the prime, to give the factors along the corresponding axis. For example, dividing

250 repeatedly by 5 produces 50, 10, and 2. These numbers go along one side of the rectangular diagram. Divide each of these by 2 to get the opposite side of the diagram.





29. Find all integer solutions of the equation $xy + 2y - 3x = 25$.

Solution: If we had a product, we could use the prime factorization theorem. That motivates one possible method of solution.

$$\begin{aligned} xy + 2y - 3x &= 25 \\ (x+2)y - 3x &= 25 \\ (x+2)y - 3x - 6 &= 25 - 6 \\ (x+2)y - 3(x+2) &= 19 \\ (x+2)(y-3) &= 19 \end{aligned}$$

Now since 19 is prime, the only way it can be factored is to have $1 \cdot 19 = 19$ or $(-1) \cdot (-19) = 19$. Therefore we have 4 possibilities: $x + 2 = 1$, $x + 2 = -1$, $x + 2 = 19$, or $x + 2 = -19$. For each of these values there is a corresponding value for y, since the complementary factor must be equal to $y - 3$. Listing the solutions as ordered pairs (x, y), we have the four solutions $(-1, 22)$, $(-3, -16)$, $(17, 4)$, and $(-21, 2)$.

30. Let a, b, c be nonzero integers. Prove that if $b \mid a$ and $c \mid a$ and $\gcd(b, c) = d$, then $bc \mid ad$. *Note:* This extends Proposition 1.2.3 (c).

Comment: Try to find an expression for ad that has bc as a factor.

Solution: Assume that $b \mid a$ and $c \mid a$, so that $a = bp$ and $a = cq$ for some $p, q \in \mathbf{Z}$. We can also write $d = mb + nc$, for some $m, n \in Z$. Then $ad = mba + nca = mb(cq) + nc(bp) = (mp + nq)(bc)$, so $bc \mid ad$.

31. For positive integers a, b, c, prove that if $\gcd(a, b) = 1$ and $c \mid b$, then $\gcd(a, c) = 1$.

Solution: To help you see why this is a consequence of Proposition 1.2.3 (d), rewrite that proposition to say that $\gcd(x, y) = 1$ and $\gcd(x, z) = 1$ if and only if $\gcd(x, yz) = 1$. Write $b = cq$ for some integer q. If we let $x = a$, $y = c$, and $z = q$, then $\gcd(a, b) = 1$ means that $\gcd(a, cq) = 1$. Using Proposition 1.2.3 (d), this implies that $\gcd(a, c) = 1$.

32. For positive integers a, b, prove that $\gcd(a, b) = 1$ if and only if $\gcd(a^2, b^2) = 1$.

Solution: Proposition 1.2.3 (d) states that $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$. Using $c = b$ gives $\gcd(a, b^2) = 1$ if and only if $\gcd(a, b) = 1$. Then a similar argument yields $\gcd(a^2, b^2) = 1$ if and only if $\gcd(a, b^2) = 1$.

Alternate Solution: It is also possible to use Proposition 1.2.10, which shows that $\gcd(a, b) = 1$ if and only if a and b have no prime divisors in common. By Euclid's lemma, this happens if and only if a^2 and b^2 have no prime divisors in common, and this is equivalent to $\gcd(a^2, b^2) = 1$.

33. Prove that $n - 1$ and $2n - 1$ are relatively prime, for all integers $n > 1$. Is the same true for $2n - 1$ and $3n - 1$?

Solution: Since $(1)(2n - 1) + (-2)(n - 1) = 1$, we have $\gcd(2n - 1, n - 1) = 1$. Similarly, $(2)(3n - 1) + (-3)(2n - 1) = 1$, and so $\gcd(3n - 1, 2n - 1) = 1$.

Comment: Is this really a proof? Yes–producing the necessary linear combinations is enough; you don't have to explain how you found them.

If this proof just looks like a trick, that's because it probably is. Maybe there is a bit of justification, in trying to find a linear combination that eliminates the variable n, and you might still ask if there is a general principle involved here.

34. Let m and n be positive integers. Prove that $\gcd(2^m - 1, 2^n - 1) = 1$ if and only if $\gcd(m, n) = 1$.

Comment: We need to do the proof in two parts. First, we will prove that if $\gcd(m, n) = 1$, then $\gcd(2^m - 1, 2^n - 1) = 1$. Then we will prove the converse, which states that if $\gcd(2^m - 1, 2^n - 1) = 1$, then $\gcd(m, n) = 1$, To prove the converse, we will use a proof by contradiction, assuming that $\gcd(m, n) \neq 1$ and showing that this forces $\gcd(2^m - 1, 2^n - 1) \neq 1$.

Before beginning the proof, remember (from calculus, if not from high school algebra) that $x^k - 1 = (x - 1)(x^{k-1} + x^{k-2} + \cdots + x + 1)$ holds for all values of x:

Solution: If $\gcd(m, n) = 1$, then there exist $a, b \in \mathbf{Z}$ with $am + bn = 1$. Substituting $x = 2^m$ and $k = a$ in the identity given above in the comment shows that $2^m - 1$ is a factor of $2^{am} - 1$, say $2^{am} - 1 = (2^m - 1)(s)$, for some $s \in \mathbf{Z}$. The same argument shows that we can write $2^{bn} - 1 = (2^n - 1)(t)$, for some $t \in \mathbf{Z}$. The proof now involves what may look like a trick (but this time it is a useful one). We have

$$\begin{aligned} 1 &= 2^1 - 1 \\ &= 2^{am+bn} - 2^{bn} + 2^{bn} - 1 \\ &= 2^{bn}(2^{am} - 1) + 2^{bn} - 1 \\ &= 2^{bn}(s)(2^m - 1) + (t)(2^n - 1) \end{aligned}$$

and so we have found a linear combination of $2^m - 1$ and $2^n - 1$ that equals 1, which proves that $\gcd(2^m - 1, 2^n - 1) = 1$.

If $\gcd(m, n) \neq 1$, say $\gcd(m, n) = d$, then there exist $p, q \in \mathbf{Z}$ with $m = dq$ and $n = dp$. But then an argument similar to the one given for the first part shows that

$2^d - 1$ is a common divisor of $2^{dq} - 1$ and $2^{dp} - 1$. Therefore $\gcd(2^m - 1, 2^n - 1) \neq 1$, and this completes the proof.

35. Prove that $\gcd(2n^2 + 4n - 3,\ 2n^2 + 6n - 4) = 1$, for all integers $n > 1$.

Solution: We can use the Euclidean algorithm. Long division of polynomials shows that dividing $2n^2 + 6n - 4$ by $2n^2 + 4n - 3$ gives a quotient of 1 and a remainder of $2n - 1$. The next step is to divide $2n^2 + 4n - 3$ by $2n - 1$, and this gives a quotient of $n + 2$ and a remainder of $n - 1$. This argument shows that

$$\gcd(2n^2 + 6n - 4, 2n^2 + 4n - 3) = \gcd(2n^2 + 4n - 3, 2n - 1) = \gcd(2n - 1, n - 1)$$

and so we can use Problem 33 to conclude that $2n^2 + 4n - 3$ and $2n^2 + 6n - 4$ are relatively prime since $2n - 1$ and $n - 1$ are relatively prime.

Comment: You could also continue on with the Euclidean algorithm, to obtain $\gcd(2n - 1, n - 1) = \gcd(n - 2, 1) = 1$.

36. Prove that if m and n are odd integers, then $m^2 - n^2$ is divisible by 8. (Compare Problem 1.1.26.)

Solution: Since m, n are odd, we can write $m = 2k + 1$ and $n = 2q + 1$, for some integers k and q. Then

$$m^2 - n^2 = (2k + 1 + 2q + 1)(2k + 1 - 2q - 1) = (4)(k + q + 1)(k - q)\ .$$

Now we need to take two cases. If $k - q$ is even, then $k - q$ has 2 as a factor, say $k - q = 2p$, for some integer p. Substituting for $k - q$ gives us

$$m^2 - n^2 = (4)(k + q + 1)(2p) = (8)(k + q + 1)(p)\ .$$

If $k - q$ is odd, then $k + q = (k - q) + (2q)$ is the sum of an odd integer and an even integer, so it must also be odd. That means that $k + q + 1$ is even, so it has 2 as a factor. Now we can suppose that $k + q + 1 = 2t$, for some integer t. In this case, substituting for $k + q + 1$ gives us

$$m^2 - n^2 = (4)(2t)(k - q) = (8)(t)(k - q)\ .$$

Showing that we can factor 8 out of $m^2 - n^2$ gives exactly what we were to prove: if m and n are odd, then $m^2 - n^2$ is divisible by 8.

Comment: There is a more elegant solution in §1.3, which can be given after some new techniques have been developed. (See Problem 1.3.41.)

ANSWERS AND HINTS

37. Find the prime factorizations of 252 and 180 and use them to compute the greatest common divisor and least common multiple of 252 and 180.
Answer: $252 = 2^2 \cdot 3^2 \cdot 7, \quad 180 = 2^2 \cdot 3^2 \cdot 5$
$\gcd(252, 180) = 2^2 \cdot 3^2 = 36, \quad \text{lcm}[252, 180] = 2^2 \cdot 3^2 \cdot 5 \cdot 7 = 1260$

38. Find the prime factorizations of 475 and 385 and use them to compute the greatest common divisor and least common multiple of 475 and 385.
Answer: $475 = 5^2 \cdot 19, \quad 385 = 5 \cdot 7 \cdot 11,$
$\gcd(475, 385) = 5, \quad \text{lcm}[475, 385] = 5^2 \cdot 7 \cdot 11 \cdot 19 = 36,575$

39. Find the prime factorizations of 5917 and 4331 and use them to find $\gcd(5917, 4331)$.
Answer: $5917 = 61 \cdot 97, \quad 4331 = 61 \cdot 71, \quad \gcd(5917, 4331) = 61$

42. Show that $\gcd(11n + 5, 7n + 3)$ is 2 if n is odd and 1 if n is even.
Hint: Use the Euclidean algorithm to show that $\gcd(11n+5, 7n+3) = \gcd(n+1, 2n)$. (See the solution to Problem 35.)

43. Find all positive integer solutions x, y of the equation $xy + 5x - 8y = 79$.
Answer: The positive solutions are $x = 9, y = 34$ and $x = 11, y = 8$.
Hint: See the solution to Problem 29.

45. Part (b): Let a, b, c be positive integers. Prove or disprove that if $\gcd(b, c) = 1$, then $\gcd(a, bc) = \gcd(ab, c)$.
Hint: Look for a counterexample.

46. Part (b): Let a, b, c be positive integers with $a^2 + b^2 = c^2$. Does $\gcd(a, b) = \gcd(a, c)$?
Answer: Yes. *Hint:* Look at the common prime divisors of a, b, c.

1.3 Congruences

29. Solve the congruence $42x \equiv 12 \pmod{90}$.

Comment: You need to recall Theorem 1.3.5, which states that $ax \equiv b \pmod{n}$ has a solution if an only if $\gcd(a, n)$ is a divisor of b. Also note that the congruence is stated modulo 90, and so the most satisfying answer is given in terms of congruence classes modulo 90.

Solution: We have $\gcd(42, 90) = 6$, so there is a solution since 6 is a factor of 12. Solving the congruence $42x \equiv 12 \pmod{90}$ is equivalent to solving the equation $42x = 12 + 90q$ for integers x and q. This reduces to $7x = 2 + 15q$, or $7x \equiv 2 \pmod{15}$. (Equivalently, we could obtain $7x \equiv 2 \pmod{15}$ by dividing $42x \equiv 12 \pmod{90}$ through by 6.) We next use trial and error to look for the multiplicative inverse of 7 modulo 15. The numbers congruent to 1 modulo 15 are 16, 31, 46, 61, etc., and -14, -29, -44, etc. Among these, we see that 7 is a factor of -14, so we multiply both sides of the congruence by -2 since $(-2)(7) = -14 \equiv 1 \pmod{15}$. Thus we have $-14x \equiv -4 \pmod{15}$, or $x \equiv 11 \pmod{15}$. The solution is $x \equiv 11, 26, 41, 56, 71, 86 \pmod{90}$.

30. (a) Find all solutions to the congruence $55x \equiv 35 \pmod{75}$.

Solution: We have $\gcd(55, 75) = 5$, which is a divisor of 35. Thus we have

$55x \equiv 35 \pmod{75}; \quad 11x \equiv 7 \pmod{15}; \quad 44x \equiv 28 \pmod{15};$

$-x \equiv 13 \pmod{15}; \quad x \equiv 2 \pmod{15}.$ The solution is

$x \equiv 2, 17, 32, 47, 62 \pmod{75}.$

Comment: In the solution, the congruence $11x \equiv 7 \pmod{15}$ is multiplied by 4 since trial and error produces the congruence $4 \cdot 11 \equiv -1 \pmod{15}$, a relatively easy way to eliminate the coefficient of x.

(b) Find all solutions to the congruence $55x \equiv 36 \pmod{75}$.

Solution: There is no solution, since $\gcd(55, 75) = 5$ is not a divisor of 36.

31. (a) Find one particular integer solution to the equation $110x + 75y = 45$.

Solution: By Theorem 1.1.6, any linear combination of 110 and 75 is a multiple of their greatest common divisor. We have following matrix reduction.

$$\begin{bmatrix} 1 & 0 & 110 \\ 0 & 1 & 75 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 35 \\ 0 & 1 & 75 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 35 \\ -2 & 3 & 5 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 15 & -22 & 0 \\ -2 & 3 & 5 \end{bmatrix}$$

Thus $-2(110) + 3(75) = 5$, and multiplying by 9 yields a solution: $x = -18$, $y = 27$, since $110(-18) + 75(27) = 45$.

Alternate solution: The equation reduces to the congruence $35x \equiv 45 \pmod{75}$. This simplifies to $7x \equiv 9 \pmod{15}$, and multiplying both sides by -2 gives $x \equiv -3 \pmod{15}$. Thus $75y = 45 + 3(110) = 375$ and so $x = -3$, $y = 5$ is a solution.

Comment: The matrix computation (above) shows that $110(15) + 75(-22) = 0$, so adding any multiple of the vector $(15, -22)$ to the particular solution $(-18, 27)$ must also give you a solution. That is the motivation for part (b) of the problem.

(b) Show that if $x = m$ and $y = n$ is an integer solution to the equation in part (a), then so is $x = m + 15q$ and $y = n - 22q$, for any integer q.

Solution: If $110m + 75n = 45$, then $110(m + 15q) + 75(n - 22q) = 45 + 110(15)q + 75(-22)q = 45$, since $110(15) - 75(22) = 0$.

32. Solve the system of congruences $x \equiv 2 \pmod{9}$ $x \equiv 4 \pmod{10}$.

Solution: We can easily find a linear combination of 9 and 10 that equals 1, by just writing $(1)(10) + (-1)(9) = 1$. Using the method outlined in the proof of Theorem 1.3.6, the solution is $x \equiv (2)(1)(10) + (4)(-1)(9) = -16 \pmod{90}$.

Alternate solution: Convert the second congruence to the equation $x = 4 + 10q$ for some $q \in \mathbf{Z}$, and substitute for x in the second congruence. Then $4 + 10q \equiv 2 \pmod{9}$, which reduces to $q \equiv 7 \pmod{9}$. The solution is $x \equiv 4 + 10(7) \equiv 74 \pmod{90}$.

33. Solve the system of congruences $x \equiv 5 \pmod{25}$ $x \equiv 23 \pmod{32}$.

Solution: To solve $r(32) + s(25) = 1$ we will use the matrix method. $\begin{bmatrix} 1 & 0 & 32 \\ 0 & 1 & 25 \end{bmatrix} \rightsquigarrow$

$$\begin{bmatrix} 1 & -1 & 7 \\ 0 & 1 & 25 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 7 \\ -3 & 4 & 4 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 4 & -5 & 3 \\ -3 & 4 & 4 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 4 & -5 & 3 \\ -7 & 9 & 1 \end{bmatrix}$$ Thus

$(-7)(32) + (9)(25) = 1$, and so $x \equiv (5)(-7)(32) + (23)(9)(25) = 4025 \equiv 55 \pmod{800}$.

Alternate solution: Write $x = 23 + 32q$ for some $q \in \mathbf{Z}$, and substitute to get $23 + 32q \equiv 5 \pmod{25}$, which reduces to $7q \equiv 7 \pmod{25}$, so $q \equiv 1 \pmod{25}$. This gives $x \equiv 55 \pmod{800}$.

34. Solve the system of congruences $5x \equiv 14 \pmod{17}$ $3x \equiv 2 \pmod{13}$.

Solution: By trial and error, $7 \cdot 5 \equiv 1 \pmod{17}$ and $9 \cdot 3 \equiv 1 \pmod{13}$,

so $5x \equiv 14 \pmod{17}$; $35x \equiv 98 \pmod{17}$; $x \equiv 13 \pmod{17}$

and $3x \equiv 2 \pmod{13}$; $27x \equiv 18 \pmod{13}$; $x \equiv 5 \pmod{13}$.

Having reduced the system to the standard form, we can solve it in the usual way. We have $x = 13 + 17q$ for some $q \in \mathbf{Z}$, and then $13 + 17q \equiv 5 \pmod{13}$. This reduces to $4q \equiv 5 \pmod{13}$, so $40q \equiv 50 \pmod{13}$, or $q \equiv 11 \pmod{13}$. This leads to the answer, $x \equiv 13 + 17 \cdot 11 \equiv 200 \pmod{221}$.

35. Give integers a, b, m, n to provide an example of a system

$$x \equiv a \pmod{m} \qquad x \equiv b \pmod{n}$$

that has no solution.

Solution: In the example the integers m and n cannot be relatively prime. This is the clue to take $m = n = 2$, with $a = 1$ and $b = 0$.

36. Find the additive order of each of the following integers, module 20: 4, 5, 6, 7, and 8.

Note: The additive order of a modulo n is defined to be the smallest positive solution of the congruence $ax \equiv 0 \pmod{n}$.

Solution: To find the additive order of 4, we need to solve the congruence $4x \equiv 0 \pmod{20}$. Dividing each term by $\gcd(4, 20) = 4$, we obtain $x \equiv 0 \pmod{5}$, and then the smallest positive solution is $x = 5$. Thus 4 has additive order 5 modulo 20.

The additive order of 5 modulo 20 is 4, as shown by this solution of $4x \equiv 0 \pmod{20}$.

$5x \equiv 0 \pmod{20}$ $x \equiv 0 \pmod{4}$ $x = 4$.

The additive order of 6 modulo 20 is 10:

$6x \equiv 0 \pmod{20}$ $3x \equiv 0 \pmod{10}$ $x \equiv 0 \pmod{10}$ $x = 10$.

The additive order of 7 modulo 20 is 20:

$7x \equiv 0 \pmod{20}$ $x \equiv 0 \pmod{20}$ $x = 20$.

The additive order of 8 modulo 20 is 5:

$8x \equiv 0 \pmod{20}$ $2x \equiv 0 \pmod{5}$ $x \equiv 0 \pmod{5}$ $x = 5$.

37. (a) Compute the last digit in the decimal expansion of 4^{100}.

Solution: The last digit is the remainder when divided by 10. Thus we must compute the congruence class of $4^{100} \pmod{10}$. We have $4^2 \equiv 6 \pmod{10}$, and then $6^2 \equiv 6 \pmod{10}$. This shows that $4^{100} = (4^2)^{50} \equiv 6^{50} \equiv 6 \pmod{10}$, so the units digit of 4^{100} is 6.

(b) Is 4^{100} divisible by 3?

Solution: No, since $4^{100} \equiv 1^{100} \equiv 1 \pmod{3}$. Or you can write 2^{200} as the prime factorization, and then $\gcd(3, 2^{200}) = 1$.

38. Find all integers n for which $13 \mid 4(n^2+1)$.

Solution: This is equivalent to solving the congruence $4(n^2+1) \equiv 0 \pmod{13}$. Since $\gcd(4,13) = 1$, we can cancel 4, to get $n^2 \equiv -1 \pmod{13}$. Just computing the squares modulo 13 gives us $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 9$, $(\pm 4)^2 \equiv 3 \pmod{13}$, $(\pm 5)^2 \equiv -1 \pmod{13}$, and $(\pm 6)^2 \equiv -3 \pmod{13}$. We have done the computation for representatives of each congruence class, so the answer to the original question is $n \equiv \pm 5 \pmod{13}$. *Comment:* For example, if $n = 5$, then $13 \mid 4 \cdot 26$.

39. Prove that $10^{n+1} + 4 \cdot 10^n + 4$ is divisible by 9, for all positive integers n.

Comment: This could be proved by induction, but we can give a more elegant proof using congruences.

Solution: The proof consists of simply observing that $10^{n+1} + 4 \cdot 10^n + 4 \equiv 0 \pmod{9}$ since $10 \equiv 1 \pmod{9}$.

40. Prove that for any integer n, the number $n^3 + 5n$ is divisible by 6.

Solution: By Proposition 1.2.3 (c), it is enough to show that $n^3 + 5n \equiv 0 \pmod{2}$ and $n^3 + 5n \equiv 0 \pmod{3}$, reducing the question to just a few computations. Modulo 2, we have $0^3 + 5(0) \equiv 0 \pmod{2}$, and $1^3 + 5(1) = 6 \equiv 0 \pmod{2}$. Modulo 3, we have $0^3 + 5(0) \equiv 0 \pmod{3}$, $1^3 + 5(1) = 6 \equiv 0 \pmod{3}$, and $2^3 + 5(2) \equiv 8 + 10 \equiv 0 \pmod{3}$. Therefore $6 \mid n^3 + 5n$.

41. Use techniques of this section to prove that if m and n are odd integers, then $m^2 - n^2$ is divisible by 8. (Compare Problem 1.2.36.)

Solution: We need to show that if m and n are odd, then $m^2 - n^2 \equiv 0 \pmod{8}$. Modulo 8, any odd integer is congruent to either ± 1 or ± 3, and squaring any of these four values gives 1 (mod 8). Thus $m^2 - n^2 \equiv 1 - 1 \equiv 0 \pmod{8}$.

42. Prove that $4^{2n+1} - 7^{4n-2}$ is divisible by 15, for all positive integers n.

Solution: We have $4^2 \equiv 1 \pmod{15}$, so $4^{2n+1} = (4^2)^n \cdot 4 \equiv 4 \pmod{15}$. We also have $7^2 \equiv 4 \pmod{15}$, so $7^4 \equiv 1 \pmod{15}$, and thus $7^{4n-2} \equiv 7^2 \cdot (7^4)^{n-1} \equiv 4 \pmod{15}$. Therefore $4^{2n+1} - 7^{4n-2} \equiv 4 - 4 \equiv 0 \pmod{15}$.

Alternate solution: By Proposition 1.2.3 (c), it is enough to show that $4^{2n+1} - 7^{4n-2} \equiv 0 \pmod{3}$ and $4^{2n+1} - 7^{4n-2} \equiv 0 \pmod{5}$. We have $4^{2n+1} - 7^{4n-2} \equiv 1^{2n+1} - 1^{4n-2} \equiv 1 - 1 \equiv 0 \pmod{3}$ and $4^{2n+1} - 7^{4n-2} \equiv (-1)^{2n+1} - 2^{2(2n-1)} \equiv (-1)^{2n+1} - (2^2)^{2n-1} \equiv (-1)^{2n+1} - (-1)^{2n-1} \equiv -1 - (-1) \equiv 0 \pmod{5}$.

43. Prove that the fourth power of an integer can only have 0, 1, 5, or 6 as its units digit.

Solution: Since the question deals with the units digit of n^4, it is really asking to find $n^4 \pmod{10}$. All we need to do is to compute the fourth power of each congruence class modulo 10: $0^4 = 0$, $(\pm 1)^4 = 1$, $(\pm 2)^4 = 16 \equiv 6 \pmod{10}$, $(\pm 3)^4 = 81 \equiv 1 \pmod{10}$, $(\pm 4)^4 \equiv 6^2 \equiv 6 \pmod{10}$, and $5^4 \equiv 5^2 \equiv 5 \pmod{10}$. This shows that the only possible units digits for n^4 are 0, 1, 5, and 6.

ANSWERS AND HINTS

45. Solve the following congruences.
(a) $10x \equiv 5 \pmod{21}$ *Answer:* $x \equiv 11 \pmod{21}$
(b) $10x \equiv 5 \pmod{15}$ *Answer:* $x \equiv 2, 5, 8, 11, 14 \pmod{15}$
(c) $10x \equiv 4 \pmod{15}$ *Answer:* No solution
(d) $10x \equiv 4 \pmod{14}$ *Answer:* $x \equiv 6, 13 \pmod{14}$

47. Solve the following congruence. $20x \equiv 12 \pmod{72}$
Answer: $x \equiv 15, 33, 51, 69 \pmod{72}$

49. (a) Find the additive order of each of the following elements, by solving the appropriate congruences. 4, 5, 6 modulo 24
Answer: The congruence class of 4 has additive order 6, that of 5 has additive order 24, and that of 6 has additive order 4 (modulo 24).

53. Solve the following system of congruences: $x \equiv 11 \pmod{16}$ $x \equiv 18 \pmod{25}$
Answer: $x \equiv 43 \pmod{400}$

55. Solve the following system of congruences: $x \equiv 9 \pmod{25}$ $x \equiv 13 \pmod{18}$
Answer: $x \equiv -41 \equiv 409 \pmod{450}$

57. Solve this system: $2x \equiv 3 \pmod{7}$ $x \equiv 4 \pmod{6}$ $5x \equiv 50 \pmod{55}$
Answer: $x \equiv 208 \pmod{462}$

59. Use congruences to prove that $5^{2n} - 1$ is divisible by 24, for all positive integers n.
Solution: We have $5^{2n} = (5^2)^n \equiv 1^n \equiv 1 \pmod{24}$.

61. Prove that if $0 < n < m$, then $2^{2^n} + 1$ and $2^{2^m} + 1$ are relatively prime.
Hint: Write 2^{2^m} as a power of 2^{2^n}. If p is a common prime divisor, reduce modulo p.

1.4 Integers Modulo n

31. Find the multiplicative inverse of each nonzero element of $\mathbf{Z}_7$.

Solution: Since $6 \equiv -1 \pmod{7}$, the class $[6]_7$ is its own inverse. Furthermore, $2 \cdot 4 = 8 \equiv 1 \pmod{7}$, and $3 \cdot 5 = 15 \equiv 1 \pmod{7}$, so $[2]_7$ and $[4]_7$ are inverses of each other, and $[3]_7$ and $[5]_7$ are inverses of each other.

32. Find the multiplicative inverse of each nonzero element of $\mathbf{Z}_{13}$.

Comment: If $ab \equiv 1 \pmod{n}$, then $[a]_n$ and $[b]_n$ are inverses, as are $[-a]_n$ and $[-b]_n$. If $ab \equiv -1 \pmod{n}$, then $[a]_n$ and $[-b]_n$ are inverses, as are $[-a]_n$ and $[b]_n$. It is useful to list the integers with m with $m \equiv \pm 1 \pmod{n}$, and look at the various ways to factor them.

Solution: Note that 14, 27, and 40 are congruent to 1, while 12, 25, and 39 are congruent to -1. Factoring 14, we see that $[2]_{13}$ and $[7]_{13}$ are inverses. Factoring 12, we see that $[3]_{13}$ and $[-4]_{13}$ are inverses, as are the pairs $[4]_{13}$ and $[-3]_{13}$, and $[6]_{13}$

and $[-2]_{13}$. Factoring 40, we see that $[5]_{13}$ and $[8]_{13}$ are inverses. Here is the list of inverses: $[2]_{13}^{-1} = [7]_{13}$; $[3]_{13}^{-1} = [9]_{13}$; $[4]_{13}^{-1} = [10]_{13}$; $[5]_{13}^{-1} = [8]_{13}$; $[6]_{13}^{-1} = [11]_{13}$.

Since $[12]_{13}^{-1} = [-1]_{13}^{-1} = [-1]_{13} = [12]_{13}$, this answers the question for all of the nonzero elements of $\mathbf{Z}_{13}$.

33. Find the multiplicative order of each element of $\mathbf{Z}_7^\times$.

Solution: It helps to use Exercise 1.4.10 in the text, which shows that if $\gcd(a, n) = 1$, then the multiplicative order of $[a]_n$ is a divisor of $\varphi(n)$. In this problem, it follows that the possibilities for the multiplicative order of an element are the divisors of 6: 1, 2, 3 and 6.

We have $2^2 = 4 \pmod 7$, and $2^3 = 8 \equiv 1 \pmod 7$, so $[2]_7$ has multiplicative order 3.

We have $3^2 \equiv 2 \pmod 7$, $3^3 \equiv 3 \cdot 3^2 \equiv 3 \cdot 2 \equiv -1 \pmod 7$, and $3^6 \equiv (3^3)^2 \equiv (-1)^2 \equiv 1 \pmod 7$, so $[3]_7$ has multiplicative order 6. Actually, after seeing that $[3]_7$ does not have multiplicative order 2 or 3, we can conclude that it has multiplicative order 6, since that is the only possibility left.

We have $4^2 \equiv 2 \pmod 7$, $4^3 \equiv 4 \cdot 4^2 \equiv 4 \cdot 2 \equiv 1 \pmod 7$, so $[4]_7$ has multiplicative order 3.

We have $5^2 \equiv 4 \pmod 7$, $5^3 \equiv 5 \cdot 5^2 \equiv 5 \cdot 4 \equiv -1 \pmod 7$, so $[5]_7$ has multiplicative order 6. We could have done the calculations with -2, since $5 \equiv -2 \pmod 7$. This would have allowed us to use the calculations we had already made in the case of 2.

Finally, it is clear that $[6]_7$ has multiplicative order 2, since $[6]_7 = [-1]_7$.

34. Find the multiplicative order of each element of $\mathbf{Z}_9^\times$.

Solution: We have $\varphi(9) = 6$, so $[a]_9^6 = [1]_9$ for all $[a]_9 \in \mathbf{Z}_9^\times$, and the possible multiplicative orders are 1, 2, 3 and 6. The elements are $[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9$. We have $2^2 = 4$, $2^3 = 8$, $2^4 = 2 \cdot 8 \equiv 7 \pmod 9$, $2^5 \equiv 2 \cdot 7 \equiv 5 \pmod 9$, and $2^6 \equiv 1 \pmod 9$. This shows that $[2]_9$ has multiplicative order 6, and also shows that $\mathbf{Z}_9^\times$ is cyclic. We can use this information to shorten our calculations for the other elements, by expressing them as the various powers of $[2]_9$.

Since $[4]_9 = [2]_9^2$, it is easy to see that $[4]_9^3 = [1]_9$, while $[4]_9^2 \neq [1]_9$, so $[4]_9$ has multiplicative order 3.

The element $[8]_9 = [2]_9^3$ must have order 2. This also obviously follows from the fact that $[8]_9 = [-1]_9$.

We have $[7]_9 = [2]_9^4$, so $[7]_9^3 = ([2]_9^4)^3 = ([2]_9^6)^2 = [1]_9$, and it then follows that $[7]_9$ has multiplicative order 3.

The smallest positive power of $[5]_9 = [2]_9^5$ that will give us an exponent divisible by 6 is 30, so $[5]_9^6 = ([2]_9^5)^6 = ([2]_9^6)^5 = [1]_9^5 = [1]_9$ and no smaller exponent gives $[1]_9$. We conclude that $[5]_9$ has multiplicative order 6.

35. Find $[91]_{501}^{-1}$, if possible (in $\mathbf{Z}_{501}^\times$).

Solution: We need to use the Euclidean algorithm.

$$\begin{bmatrix} 1 & 0 & 501 \\ 0 & 1 & 91 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -5 & 46 \\ 0 & 1 & 91 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -5 & 46 \\ -1 & 6 & 45 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 2 & -11 & 1 \\ -1 & 6 & 45 \end{bmatrix}$$

Thus $501 \cdot 2 + 91(-11) = 1$, so $91(-11) \equiv 1 \pmod{501}$.

Answer: $[91]_{501}^{-1} = [-11]_{501} = [490]_{501}$.

36. Find $[3379]_{4061}^{-1}$, if possible (in $\mathbf{Z}_{4061}^{\times}$).

Solution: The inverse does not exist.

$$\begin{bmatrix} 1 & 0 & 4061 \\ 0 & 1 & 3379 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 682 \\ 0 & 1 & 3379 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 682 \\ -4 & 5 & 651 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 5 & -6 & 31 \\ -4 & 5 & 651 \end{bmatrix}$$

At the next step, $31 \mid 651$, and so $\gcd(4061, 3379) = 31$.

37. In $\mathbf{Z}_{20}$: find all units (list the multiplicative inverse of each); find all idempotent elements; find all nilpotent elements.

Comment: We know that $\mathbf{Z}_n$ has $\varphi(n)$ units. They occur in pairs, since $\gcd(a, n) = 1$ if and only if $\gcd(n - a, n) = 1$. This helps in checking your list.

Solution: The units of $\mathbf{Z}_{20}$ are the equivalence classes represented by 1, 3, 7, 9, 11, 13, 17, and 19. We have $[3]_{20}^{-1} = [7]_{20}$, $[9]_{20}^{-1} = [9]_{20}$, and $[11]_{20}^{-1} = [11]_{20}$ by trial and error, and then $[13]_{20}^{-1} = [-7]_{20}^{-1} = [-3]_{20} = [17]_{20}$, and $[19]_{20}^{-1} = [-1]_{20}^{-1} = [-1]_{20} = [19]_{20}$.

The idempotent elements of $\mathbf{Z}_{20}$ can be found by using trial and error. They are $[0]_{20}$, $[1]_{20}$, $[5]_{20}$, and $[16]_{20}$. If you want a more systematic approach, you can use the hint in Exercise 1.4.15 of the text: if $n = bc$, with $\gcd(b, c) = 1$, then any solution to the congruences $x \equiv 1 \pmod{b}$ and $x \equiv 0 \pmod{c}$ will be idempotent modulo n.

The nilpotent elements of $\mathbf{Z}_{20}$ can be found by using trial and error, or by using the result stated in Problem 1.4.41. They are $[0]_{20}$ and $[10]_{20}$.

38. Show that $\mathbf{Z}_{17}^{\times}$ is cyclic.

Comment: To show that $\mathbf{Z}_{17}^{\times}$ is cyclic, we need to find an element whose multiplicative order is 16. The solution just uses trial and error. It is known than if p is prime, then $\mathbf{Z}_p^{\times}$ is cyclic, but there is no known algorithm for actually finding the one element whose powers cover all of $\mathbf{Z}_p^{\times}$.

Solution: We begin by trying [2]. We have $[2]^2 = [4]$, $[2]^3 = [8]$, and $[2]^4 = [16] = [-1]$. Exercise 1.4.10 of the text shows that the multiplicative order of an element has to be a divisor of $\varphi(17) = 16$, so the next possibility to check is 8. Since $[2]^8 = [-1]^2 = [1]$, it follows that [2] has multiplicative order 8.

We next try [3]. We have $[3]^2 = [9]$, $[3]^4 = [81] = [-4]$, and $[3]^8 = [16] = [-1]$. The only divisor of 16 that is left to try is 16 itself, so [3] does in fact have multiplicative order 16, and we are done.

39. Show that $\mathbf{Z}_{35}^{\times}$ is not cyclic but that each element has the form $[8]_{35}^{i}[-4]_{35}^{j}$, for some positive integers i, j.

Solution: We first compute the powers of [8]: $[8]^2 = [-6]$, $[8]^3 = [8][-6] = [-13]$, and $[8]^4 = [-6]^2 = [1]$, so the multiplicative order of [8] is 4, and the powers we have listed represent the only possible values of $[8]^i$.

We next compute the powers of $[-4]$: $[-4]^2 = [16]$, $[-4]^3 = [-4][16] = [6]$, $[-4]^4 = [-4][6] = [11]$, $[-4]^5 = [-4][11] = [-9]$, and $[-4]^6 = [-4][-9] = [1]$, so the multiplicative order of $[-4]$ is 6.

There are 24 possible products of the form $[8]^i[-4]^j$, for $0 \leq i < 4$ and $0 \leq j < 6$. Are these all different? Suppose that $[8]^i[-4]^j = [8]^m[-4]^n$, for some $0 \leq i < 4$ and $0 \leq j < 6$ and $0 \leq m < 4$ and $0 \leq n < 6$. Then $[8]^{i-m} = [-4]^{n-j}$, and since the only power of $[8]$ that is equal to a power of $[-4]$ is $[1]$ (as shown by our computations), this forces $i = m$ and $n = j$.

We conclude that since there are 24 different elements of the form $[8]^i[-4]^j$, every element in $\mathbf{Z}_{35}$ must be of this form.

Finally, $([8]^i[-4]^j)^{12} = ([8]^4)^{3i}([-4]^6)^{2j} = [1]$, so no element of $\mathbf{Z}_{35}$ has multiplicative order 24, showing that $\mathbf{Z}_{35}$ is not cyclic.

40. Solve the equation $[x]_{11}^2 + [x]_{11} - [6]_{11} = [0]_{11}$.

Solution: We can factor $[x]^2 + [x] - [6] = ([x] + [3])([x] - [2])$. Corollary 1.4.6 implies that either $[x] + [3] = [0]$ or $[x] - [2] = [0]$, and so the only possible solutions are $[x] = [-3]$ and $[x] = [2]$. Substituting these values back into the equation shows that they are indeed solutions, so the answer is $[x] = [2]$ or $[x] = [-3]$.

41. Prove that $[a]_n$ is a nilpotent element of $\mathbf{Z}_n$ if and only if each prime divisor of n is a divisor of a.

Solution: First assume that each prime divisor of n is a divisor of a. If $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}$ is the prime factorization of n, then we must have $a = p_1^{\beta_1}p_2^{\beta_2}\cdots p_t^{\beta_t}d$, where $0 \leq \beta_j \leq \alpha_j$ for all j. If k is the smallest positive integer such that $k\beta_i \geq \alpha_i$ for all i, then $n \mid a^k$, and so $[a]_n^k = [0]_k$.

Conversely, if $[a]_n$ is nilpotent, with $[a]_n^k = [0]$, then $n \mid a^k$, so each prime divisor of n is a divisor of a^k. But if a prime p is a divisor of a^k, then it must be a divisor of a, and this completes the proof.

42. Show that if $n > 1$ is an odd integer, then $\varphi(2n) = \varphi(n)$.

Solution: Since n is odd, the prime 2 does not occur in its prime factorization. The formula in Proposition 1.4.8 shows that to compute $\varphi(2n)$ in terms of $\varphi(n)$ we need to add $2 \cdot (1 - \frac{1}{2})$, and this does not change the computation.

Alternate solution: Since n is odd, the integers n and 2 are relatively prime. Exercise 1.4.29 of the text states that if m, n are relatively prime positive integers, then $\varphi(mn) = \varphi(m)\varphi(n)$. It follows that $\varphi(2n) = \varphi(2)\varphi(n) = \varphi(n)$.

ANSWERS AND HINTS

43. Write out multiplication tables for the following sets.
(a) $\mathbf{Z}_9^\times$
Answer: This set is cyclic, and each element can be expressed as a power of 2. Writing out a table in the order $[1], [2], [4], [8], [7], [5]$ of consecutive powers of 2 means that

each row is just a shift of the one above it. Other orders are interesting too.

·	1	2	4	8	7	5
1	1	2	4	8	7	5
2	2	4	8	7	5	1
4	4	8	7	5	1	2
8	8	7	5	1	2	4
7	7	5	1	2	4	8
5	5	1	2	4	8	7

or

·	1	8	2	7	4	5
1	1	8	2	7	4	5
8	8	1	7	2	5	4
2	2	7	4	5	8	1
7	7	2	5	4	1	8
4	4	5	8	1	7	2
5	5	4	1	8	2	7

or

·	1	4	7	2	8	5
1	1	4	7	2	8	5
4	4	7	1	8	5	2
7	7	1	4	5	2	8
2	2	8	5	4	7	1
8	8	5	2	7	1	4
5	5	2	8	1	4	7

(b) $\mathbf{Z}_{10}^{\times}$

Answer:

·	1	3	9	7
1	1	3	9	7
3	3	9	7	1
9	9	7	1	3
7	7	1	3	9

or

·	1	−1	3	−3
1	1	−1	3	−3
−1	−1	1	−3	3
3	3	−3	−1	1
−3	−3	3	1	−1

The first table uses the fact that $\mathbf{Z}_{10}^{\times}$ is cyclic, and lists the elements as consecutive powers of 3. The second table shows a different pattern–compare this to the pattern in part (c), which differs in a crucial way along the main diagonal.

(c) $\mathbf{Z}_{12}^{\times}$

Answer:

·	1	−1	5	−5
1	1	−1	5	−5
−1	−1	1	−5	5
5	5	−5	1	−1
−5	−5	5	−1	1

(d) $\mathbf{Z}_{14}^{\times}$

Hint: Problem 47 shows that each element of $\mathbf{Z}_{14}^{\times}$ is a power of 3, so a quick way to write out the table is to use the order $[1], [3], [9], [13], [11], [5]$. Then the table will have the same pattern as the one in part (a).

44. Find the multiplicative inverses of the given elements (if possible).
(a) $[12]$ in $\mathbf{Z}_{15}$
Answer: There is no inverse, since 12 is not relatively prime to 15.
(c) $[7]$ in $\mathbf{Z}_{15}$
Answer: $[7]^{-1} = [13]$

45. Find the multiplicative orders of the following elements.
(b) $[5]$ and $[7]$ in $\mathbf{Z}_{17}^{\times}$
Answer: $[5]$ and $[7]$ both have multiplicative order 16

46. Find the multiplicative order of each element of the following sets.
(b) $\mathbf{Z}_{10}^{\times}$
Answer: $[3]$ and $[7] = [-3]$ have order 4; $[9] = [-1]$ has order 2; $[1]$ has order 1.

47. Is $\mathbf{Z}_{14}^{\times}$ cyclic?
Answer: Yes; $[3]$ has multiplicative order $6 = \varphi(14)$.

48. Is $\mathbf{Z}_{16}^{\times}$ cyclic?
Answer: No *Hint:* Check that each element has multiplicative order less than 8.

49. Is $\mathbf{Z}_{18}^{\times}$ cyclic?
Answer: Yes; [5] has multiplicative order $6 = \varphi(18)$.

50. Find all idempotent elements in the following sets.
(a) $\mathbf{Z}_{14}$
Hint: Exercise 1.4.15 in the text states that if $n = bc$, with $\gcd(b, c) = 1$, then any solution to the congruences $x \equiv 1 \pmod{b}$ and $x \equiv 0 \pmod{c}$ will be idempotent modulo n. First take $b = 7$, $c = 2$ and then $b = 2$, $c = 7$.

52. In $\mathbf{Z}_{24}$: find all units (list the multiplicative inverse of each); find all idempotent elements; find all nilpotent elements.
Answer: The units of $\mathbf{Z}_{24}$ are the equivalence classes represented by 1, 5, 7, 11, 13, 17, 19, and 23, and each element is its own inverse.
The idempotent elements are $[0]_{24}, [1]_{24}, [9]_{24}, [16]_{24}$.
The nilpotent elements are $[0]_{24}, [6]_{24}, [12]_{24}, [18]_{24}$.

53. Find $\{n \in \mathbf{Z}^+ \mid \varphi(n) = 2\}$ and $\{n \in \mathbf{Z}^+ \mid \varphi(n) = 4\}$.
Answer: $\{n \in \mathbf{Z}^+ \mid \varphi(n) = 2\} = \{3, 4, 6\}$ and $\{n \in \mathbf{Z}^+ \mid \varphi(n) = 4\} = \{5, 8, 10, 12\}$

Review Problems

1. Prove that if a, b, c are integers for which $b \mid a$ and $b \mid (a - c)$, then $b \mid c$.

   Solution: Assume that $b \mid a$ and $b \mid (a - c)$. Then by definition there exist integers k and q with $a = bq$ and $a - c = bk$. Since we need to show that b is a factor of c, we start by solving the second equation for c. Then $c = a - bk$, and we can substitute for a to get $c = bq - bk = b(q - k)$. This shows that c has b as a factor, and so $b \mid c$, as required.

2. Find $\gcd(7605, 5733)$, and express it as a linear combination of 7605 and 5733.

   Solution: Use the matrix form of the Euclidean algorithm:

$$\begin{bmatrix} 1 & 0 & 7605 \\ 0 & 1 & 5733 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 1872 \\ 0 & 1 & 5733 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 1872 \\ -3 & 4 & 117 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 49 & -65 & 0 \\ -3 & 4 & 117 \end{bmatrix}.$$

   Thus $\gcd(7605, 5733) = 117$, and $117 = (-3) \cdot 7605 + 4 \cdot 5733$.

3. Find the prime factorizations of 1275 and 495 and use them to find $\gcd(1275, 495)$.

   Solution: You can compare Problem 1.1.42, which was to be solved using the Euclidean algorithm. We can begin factoring 1275 by factoring out a 5. Continuing, we obtain $1275 = 5{\cdot}255 = 5^2{\cdot}51 = 3{\cdot}5^2{\cdot}17$. Next, we have $495 = 5{\cdot}99 = 5{\cdot}9{\cdot}11 = 3^2{\cdot}5{\cdot}11$. Thus $\gcd(1275, 495) = 3 \cdot 5$, while $\text{lcm}[1275, 495) = 3^2 \cdot 5^2 \cdot 11 \cdot 17$.

4. Find $\varphi(1275)$ and $\varphi(495)$.

Solution: We can use the prime factorizations found in Problem 3. By Proposition 1.4.8 we have $\varphi(1275) = 3 \cdot 5^2 \cdot 17 \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{16}{17} = 5 \cdot 2 \cdot 4 \cdot 16 = 640$ and $\varphi(495) = 3^2 \cdot 5 \cdot 11 \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{10}{11} = 3 \cdot 2 \cdot 4 \cdot 10 = 240$.

5. Solve the congruence $24x \equiv 168 \pmod{200}$.

   Solution: First we find that $\gcd(24, 200) = 8$, and $8 \mid 168$, so the congruence has a solution. The next step is to reduce the congruence by dividing each term by 8, which gives $24x \equiv 168 \pmod{200}$. To solve the congruence $3x \equiv 21 \pmod{25}$ we could find the multiplicative inverse of 3 modulo 25. Trial and error shows it to be -8, we can multiply both sides of the congruence by -8, and proceed with the solution.

$$\begin{array}{rcrl} 24x & \equiv & 168 & \pmod{200} \\ 3x & \equiv & 21 & \pmod{25} \\ -24x & \equiv & -168 & \pmod{25} \\ x & \equiv & 7 & \pmod{25} \end{array}$$

   The solution is $x \equiv 7, 32, 57, 82, 107, 132, 157, 182 \pmod{200}$.

6. Find the additive order of 168 modulo 200.

   Solution: According to the definition of the additive order of a number, we need to solve $168x \equiv 0 \pmod{200}$. Since $\gcd(168, 200) = 8$, we get $21x \equiv 0 \pmod{25}$. This leads to $x \equiv 0 \pmod{25}$, and therefore the the additive order of 168 is 25.

7. Solve the system of congruences $2x \equiv 9 \pmod{15}$ $x \equiv 8 \pmod{11}$.

   Solution: Write $x = 8 + 11q$ for some $q \in \mathbf{Z}$, and substitute to get $16 + 22q \equiv 9 \pmod{15}$, which reduces to $7q \equiv -7 \pmod{15}$, so $q \equiv -1 \pmod{15}$. This gives $x \equiv -3 \pmod{11 \cdot 15}$.

8. Find $[50]_{501}^{-1}$ and $[51]_{501}^{-1}$, if possible (in $\mathbf{Z}_{501}^{\times}$).

   Solution: We need to use the Euclidean algorithm.

$$\begin{bmatrix} 1 & 0 & 501 \\ 0 & 1 & 50 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -10 & 1 \\ 0 & 1 & 50 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -10 & 1 \\ -50 & 501 & 0 \end{bmatrix}$$

   Thus $[50]_{501}^{-1} = [-10]_{501} = [491]_{501}$.

$$\begin{bmatrix} 1 & 0 & 501 \\ 0 & 1 & 51 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -9 & 42 \\ 0 & 1 & 51 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -9 & 42 \\ -1 & 10 & 9 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 5 & -11 & 6 \\ -1 & 10 & 9 \end{bmatrix}$$

   Now we can see that the gcd is 3, so $[51]_{501}$ is not a unit in $\mathbf{Z}_{501}$.

9. List the elements of $\mathbf{Z}_{15}^{\times}$. For each element, find its multiplicative inverse, and find its multiplicative order.

   Solution: There should be 8 elements since $\varphi(15) = 8$. Exercise 1.4.10 of the text states that if $\gcd(a, n) = 1$ and $[a]$ has multiplicative order k in $\mathbf{Z}_n^{\times}$, then $k \mid \varphi(n)$. Thus the multiplicative order of any nontrivial element is 2, 4, or 8. The elements are [1], [2], [4], [7], [8], [11], [13], and [14].

Computing powers, we have $[2]^2 = [4]$, $[2]^3 = [8]$, and $[2]^4 = [1]$. This shows not only that the multiplicative order of $[2]$ is 4, but that the multiplicative order of $[4]$ is 2. The same computation shows that $[2]^{-1} = [8]$ and $[4]^{-1} = [4]$. We can also deduce that $[13] = [-2]$ has multiplicative order 4, that $[13]^{-1} = [-2]^{-1} = [-8] = [7]$, and that $[11]^{-1} = [-4]^{-1} = [-4] = [11]$.

Next, we have $[7]^2 = [4]$, so $[7]$ has multiplicative order 4 because $[7]^4 = [4]^2 = [1]$.

To compute the multiplicative order of $[8]$, we can rewrite it as $[2]^3$, and then it is clear that the first positive integer k with $([2]^3)^k = [1]$ is $k = 4$, since $3k$ must be a multiple of 4. (This can also be shown by rewriting $[8]$ as $[-7]$.) Similarly, $[11] = [-4]$ has multiplicative order 2, and $[13] = [-2]$ has multiplicative order 4.

10. Show that $3^n + 4^n - 1$ is divisible by 6, for any positive integer n.

Solution: We have $3^n + 4^n - 1 \equiv 1^n + 0^n - 1 \equiv 0 \pmod 2$ and $3^n + 4^n - 1 \equiv 0^n + 1^n - 1 \equiv 0 \pmod 3$. Since 2 and 3 are relatively prime, it follows that 6 is a divisor of $3^n + 4^n - 1$.

Chapter 2

Functions

2.1 Functions

21. The "Vertical Line Test" from calculus says that a curve in the xy-plane is the graph of a function of x if and only if no vertical line intersects the curve more than once. Explain why this agrees with Definition 2.1.1.

    Solution: We assume that the x-axis is the domain and the y-axis is the codomain of the function that is to be defined by the given curve. According to Definition 2.1.1, a subset of the plane defines a function if for each element x in the domain there is a unique element y in the codomain such that (x, y) belongs to the subset of the plane. If a vertical line intersects the curve in two distinct points, then there will be points (x_1, y_1) and (x_2, y_2) on the curve with $x_1 = x_2$ and $y_1 \neq y_2$. Thus if we apply Definition 2.1.1 to the given curve, the uniqueness part of the definition translates directly into the "vertical line test".

22. The "Horizontal Line Test" from calculus says that a function is one-to-one if and only if no horizontal line intersects its graph more than once. Explain why this agrees with Definition 2.1.4.

    Solution: If a horizontal line intersects the graph of the function more than once, then the points of intersection represent points (x_1, y_1) and (x_2, y_2) for which $x_1 \neq x_2$ but $y_1 = y_2$. According to Definition 2.1.4, a function is one-to-one if $f(x_1) = f(x_2)$ implies $x_1 = x_2$. Equivalently, if (x_1, y_1) and (x_2, y_2) lie on its graph, then we cannot have $y_1 = y_2$ while $x_1 \neq x_2$. In this context, the "horizontal line test" is exactly the same as the condition given in Definition 2.1.4.

23. In calculus the graph of an inverse function f^{-1} is obtained by reflecting the graph of f about the line $y = x$. Explain why this agrees with Definition 2.1.6.

    Solution: We first note that the reflection of a point (a, b) in the line $y = x$ is the point (b, a). This can be seen by observing that the line segment joining (a, b) and (b, a) has slope -1, which makes it perpendicular to the line $y = x$, and that this line segment intersects the line $y = x$ at the midpoint $((a+b)/2, (a+b)/2)$ of the segment.

If $f : \mathbf{R} \to \mathbf{R}$ has an inverse, and the point (x, y) lies on the graph of f, then $y = f(x)$, and so $f^{-1}(y) = f^{-1}(f(x)) = x$. This shows that the point (y, x) lies on the graph of f^{-1}. Conversely, if (y, x) lies on the graph of f^{-1}, then $x = f^{-1}(y)$, and therefore $y = f(f^{-1}(y)) = f(x)$, which shows that (x, y) lies on the graph of f.

On the other hand, suppose that the graph of the function g is defined by reflecting the graph of f in the line $y = x$. For any real number x, if $y = f(x)$ then we have $g(f(x)) = g(y) = x$ and for any real number y we have $f(g(y)) = f(x) = y$, where $x = g(y)$. This shows that $g = f^{-1}$, and so f has an inverse.

24. Show that the function $f : \mathbf{R}^2 \to \mathbf{R}^2$ defined by $f(x, y) = (x^3+y, y)$, for all $(x, y) \in \mathbf{R}^2$, is a one-to-one correspondence.

Solution: To show that f is one-to-one, suppose that $f(x_1, y_1) = f(x_2, y_2)$. Then $x_1^3 + y_1 = x_2^3 + y_2$ and $y_1 = y_2$, so it follows that $x_1^3 = x_2^3$ and therefore $x_1 = x_2$. Thus $(x_1, y_1) = (x_2, y_2)$.

To show that f is onto, suppose that $(a, b) \in \mathbf{R}^2$ is given. We need to solve the equation $f(x, y) = (a, b)$, which leads to two equations: $y = b$ and $x^3 + y = a$. Thus $x^3 = a - b$, and so $(x, y) = (\sqrt[3]{a - b}, b)$ gives us the desired solution.

25. Define $f : \mathbf{R} \to \mathbf{R}$ by $f(x) = x^3 + 3x - 5$, for all $x \in \mathbf{R}$. Is f a one-to-one function? Is f an onto function?

Hint: Use the derivative of f to show that f is a strictly increasing function.

Solution: Since $f'(x) = 3x^2 + 3 = 3(x^2 + 1)$, we have $f'(x) \geq 3$ for all x. If $x_1 < x_2$, then $f(x_1) < f(x_2)$, and so $x_1 \neq x_2$ implies $f(x_1) \neq f(x_2)$, showing that f is a one-to-one function.

We have $\lim_{x\to\infty} f(x) = \infty$ and $\lim_{x\to-\infty} f(x) = -\infty$. Since f is a continuous function, it follows that f must be an onto function.

26. Does the following formula define a function from $\mathbf{Q}$ to $\mathbf{Z}$? Set $f\left(\frac{m}{n}\right) = m$, where m, n are integers and $n \neq 0$.

Solution: We have $\frac{1}{2} = \frac{2}{4}$, but $f\left(\frac{1}{2}\right) = 1$ and $f\left(\frac{2}{4}\right) = 2$. The definition of a function requires that if $x_1 = x_2$, then $f(x_1) = f(x_2)$, so f does not define a function.

27. Define the formulas $f : \mathbf{Z}_{12} \to \mathbf{Z}_8$ by $f([x]_{12}) = [2x]_8$, for all $[x]_{12} \in \mathbf{Z}_{12}$, and $g : \mathbf{Z}_{12} \to \mathbf{Z}_8$ by $g([x]_{12}) = [3x]_8$, for all $[x]_{12} \in \mathbf{Z}_{12}$. Show that f defines a function, but g does not.

Solution: We must show that if $[x_1]_{12} = [x_2]_{12}$, then $f([x_1]_{12}) = f([x_2]_{12})$. If $[x_1]_{12} = [x_2]_{12}$, then $12 \mid (x_1 - x_2)$, so multiplying by 2 gives us $24 \mid (2x_1 - 2x_2)$, and it follows that $8 \mid (2x_1 - 2x_2)$, which shows that $[2x_1]_8 = [x_2]_8$.

On the other hand, $[0]_{12} = [12]_{12}$, but but $g([0]_{12}) = [0]_8$, while $g([12]_{12}) = [36]_8 = [4]_8$. Therefore the formula g does not produce a well-defined function from $\mathbf{Z}_{12}$ to $\mathbf{Z}_8$.

Comment: Exercise 2.1.11 in the text gives the complete answer. It states that if $m, n, k \in \mathbf{Z}^+$, then the formula $f([x]_n) = [mx]_k$ defines a function from $\mathbf{Z}_n$ to $\mathbf{Z}_k$ if and only if $k \mid mn$. Thus in this problem f is a well-defined function since $8 \mid 2 \cdot 12$, but g is not a well-defined function since $8 \nmid 3 \cdot 12$.

28. Let a be a fixed element of $\mathbf{Z}_{17}^\times$. Define the function $\theta : \mathbf{Z}_{17}^\times \to \mathbf{Z}_{17}^\times$ by $\theta(x) = ax$, for all $x \in \mathbf{Z}_{17}^\times$. Is θ one-to-one? Is θ onto? If possible, find the inverse function θ^{-1}.

Solution: Since a has an inverse in $\mathbf{Z}_{17}^\times$, we can define $\psi : \mathbf{Z}_{17}^\times \to \mathbf{Z}_{17}^\times$ by $\psi(x) = a^{-1}x$, for all $x \in \mathbf{Z}_{17}^\times$. Then $\psi(\theta(x)) = \psi(ax) = a^{-1}(ax) = (a^{-1}a)x = x$ and $\theta(\psi(x)) = \theta(a^{-1}x) = a(a^{-1}x) = (aa^{-1})x = x$, which shows that $\psi = \theta^{-1}$. This implies that θ is one-to-one and onto.

29. For integers m, n, b with $n > 1$, define $f : \mathbf{Z}_n \to \mathbf{Z}_n$ by $f([x]_n) = [mx + b]_n$.

(a) Show that f is a well-defined function.

Solution: If $x_1 \equiv x_2 \pmod{n}$, then it is clear that $mx_1 + b \equiv mx_2 + b \pmod{n}$.

(b) Prove that f is a one-to-one correspondence if and only if $\gcd(m, n) = 1$.

Solution: First assume that f is a one-to-one correspondence. Then f is onto, and so $f([x]_n) = [1+b]_n$ has a solution. But then $mx+b \equiv 1+b \pmod{n}$, so $mx \equiv 1 \pmod{n}$, which implies that $\gcd(m, n) = 1$.

You can also give a proof using the fact that f is one-to-one, but it takes more work since we don't have any result that states that being able to cancel m for all possible integers guarantees that $\gcd(m, n) = 1$.

Conversely, suppose that $\gcd(m, n) = 1$. Then $f([x_1]_n) = f([x_2]_n)$ implies $[mx_1 + b]_n = [mx_2 + b]_n$, so $[mx_1]_n = [mx_2]_n$. Since $\gcd(m, n) = 1$, the element $[m]_n$ has a multiplicative inverse $[m]_n^{-1}$, and multiplying by it gives $[x_1]_n = [x_2]_n$. Because $\mathbf{Z}_n$ is a finite set and f maps $\mathbf{Z}_n$ into $\mathbf{Z}_n$, Proposition 2.1.8 shows that f is also onto.

(c) If $\gcd(m, n) = 1$, find the inverse function f^{-1}.

Solution: You can use the calculus algorithm to find the inverse: $[y]_n = [m]_n[x]_n + [b]_n$ so interchange x and y and solve. We get $[x]_n = [m]_n[y]_n + [b]_n$, so $[m]_n[y]_n = [x]_n - [b]_n$, and then we can multiply by $[m]_n^{-1}$, which exists since $\gcd(m, n) = 1$. We get $[y]_n = [m]_n^{-1}[x]_n - [m]_n^{-1}[b]_n$ as the formula for the inverse.

Check: $f(f^{-1}([x]_n)) = f([m]_n^{-1}[x]_n - [m]_n^{-1}[b]_n) = [m]_n([m]_n^{-1}[x]_n - [m]_n^{-1}[b]_n) + [b]_n = [m]_n[m]_n^{-1}[x]_n - [m[_n[m]_n^{-1}[b]_n + [b]_n = [x]_n$

$f^{-1}(f([x]_n)) = f^{-1}([m]_n[x]_n + [b]_n) = f^{-1}([m]_n[x]_n + [b]_n) =$

$= [m]_n^{-1}([m]_n[x]_n + [b]_n) - [m]_n^{-1}[b]_n) = [x]_n + [m]_n^{-1}[b]_n) - [m]_n^{-1}[b]_n = [x]_n.$

Alternate solution: You can keep secret how you found the formula for the inverse, and just check that $f \circ f^{-1}$ and $f^{-1} \circ f$ are the identity functions.

30. Let $f : S \to T$ be a function, and let A, B be subsets of S. Prove the following:

(a) If $A \subseteq B$, then $f(A) \subseteq f(B)$.

Solution: If $t \in f(A)$, then $t = f(a)$ for some $a \in A$. Since $A \subseteq B$, we have $a \in B$, and thus $t \in f(B)$.

(b) $f(A \cup B) = f(A) \cup f(B)$

Solution: To check equality of the given sets, we need to show that $f(A \cup B) \subseteq f(A) \cup f(B)$ and that $f(A) \cup f(B) \subseteq f(A \cup B)$.

First, let $t \in f(A \cup B)$. Then $t = f(s)$ for some $s \in A \cup B$, so either $s \in A$, in which case $t \in f(A)$, or else $s \in B$, in which case $t \in f(B)$. Thus $t \in f(A) \cup f(B)$, and so we have shown that $f(A \cup B) \subseteq f(A) \cup f(B)$.

Next, let $t \in f(A) \cup f(B)$. Then either $t \in f(A)$, in which case $t = f(a)$ for some $a \in A$, or else $t \in f(B)$, in which case $t = f(b)$ for some $b \in B$. Since $t = f(s)$, where either $s = a \in A$ or $s = b \in B$, it follows that $t \in f(A \cup B)$, showing that $f(A) \cup f(B) \subseteq f(A \cup B)$.

(c) $f(A \cap B) \subseteq f(A) \cap f(B)$

Solution: Let $t \in f(A \cap B)$. Then $t = f(s)$, for some $s \in A \cap B$. Since $s \in A$ and $s \in B$, it follows that $t \in f(A) \cap f(B)$.

31. Let $f : S \to T$ be a function. Prove that f is a one-to-one function if and only if $f(A \cap B) = f(A) \cap f(B)$ for all subsets A, B of S.

Solution: First, suppose that f is a one-to-one function. Problem 30 (c) shows that $f(A \cap B) \subseteq f(A) \cap f(B)$, so we only need to show that $f(A) \cap f(B) \subseteq f(A \cap B)$. If $t \in f(A) \cap f(B)$, then $t = f(a)$ for some $a \in A$ and $t = f(b)$ for some $b \in B$. But we must have $a = b$ since f is one-to-one, and it follows that $t \in f(A \cap B)$.

Conversely, suppose that the given condition holds and that $f(x_1) = f(x_2)$ for elements $x_1 \neq x_2$ in S. Let $A = \{x_1\}$ and $B = \{x_2\}$. Then $A \cap B = \emptyset$, but $f(A) \cap f(B) = \{f(x_1\}$, so $f(A \cap B) \neq f(A) \cap f(B)$, a contradiction. We conclude that f must be a one-to-one function.

32. Let $f : S \to T$ be a function, and let X, Y be subsets of T. Prove the following:

(a) If $X \subseteq Y$, then $f^{-1}(X) \subseteq f^{-1}(Y)$.

Solution: Let $s \in f^{-1}(X)$. Then $f(s) \in X$, so $f(x) \in Y$ since $X \subseteq Y$, which shows that $s \in f^{-1}(Y)$.

(b) $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$

Solution: Let $s \in f^{-1}(X \cup Y)$. Then $f(s) \in X \cup Y$, so either $f(s) \in X$ or $f(s) \in Y$. In the first case $s \in f^{-1}(X)$, and in the second case $s \in f^{-1}(Y)$, showing that $s \in f^{-1}(X) \cup f^{-1}(Y)$.

Let $s \in f^{-1}(X) \cup f^{-1}(Y)$. Then either $s \in f^{-1}(X)$, in which case $f(s) \in X$, or else $s \in f^{-1}(Y)$, in which case $f(s) \in Y$. Thus $f(s) \in X$ or $f(s) \in Y$, showing that $s \in f^{-1}(X \cup Y)$. Since both inclusions hold, we have equality of the given sets.

(c) $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$

Solution: Let $s \in f^{-1}(X \cap Y)$. Then $f(x) \in X \cap Y$, so $f(s) \in X$ and $f(s) \in Y$, which shows that $s \in f^{-1}(X) \cap f^{-1}(Y)$.

On the other hand, let $s \in f^{-1}(X) \cap f^{-1}(Y)$. Then $f(s) \in X$ and $f(s) \in Y$, so $f(x) \in X \cap Y$ and therefore $s \in f^{-1}(X \cap Y)$.

33. Let A be an $n \times n$ matrix with entries in $\mathbf{R}$. Define a linear transformation $L : \mathbf{R}^n \to \mathbf{R}^n$ by $L(\mathbf{x}) = A\mathbf{x}$, for all $\mathbf{x} \in \mathbf{R}^n$.

(a) Show that L is an invertible function if and only if $\det(A) \neq 0$.

Solution: I need to assume that you know that a square matrix A is invertible if and only if $\det(A) \neq 0$.

First, if L has an inverse, then it can also be described by multiplication by a matrix B, which must satisfy the conditions $BA = I$, and $AB = I$, where I is the $n \times n$ identity matrix. Thus A is an invertible matrix, and so $\det(A) \neq 0$.

On the other hand, if $\det(A) \neq 0$, then A is invertible, and so L has an inverse, defined by $L^{-1}(\mathbf{x}) = A^{-1}\mathbf{x}$, for all $\mathbf{x} \in \mathbf{R}^n$.

(b) Show that if L is either one-to-one or onto, then it is invertible.

Solution: The *rank* of the matrix A is the dimension of the column space of A, and the column space is the image of the transformation L, so L is onto if and only if A has rank n.

On the other hand, the *nullity* of A is the dimension of the solution space of the equation $A\mathbf{x} = \mathbf{0}$, and L is one-to-one if and only if the nullity of A is zero, since $A\mathbf{x}_1 = A\mathbf{x}_2$ if and only if $A(\mathbf{x}_1 - \mathbf{x}_2) = \mathbf{0}$.

To prove part (b) we need to use the rank–nullity theorem, which states that if A is an $n \times n$ matrix, then the rank of A plus the nullity of A is n. Since the matrix A is invertible if and only if it has rank n, it follows that L is invertible if and only if L is onto, and then the rank–nullity theorem shows that this happens if and only if L is one-to-one.

34. Let A be an $m \times n$ matrix with entries in $\mathbf{R}$, and assume that $m > n$. Define a linear transformation $L : \mathbf{R}^n \to \mathbf{R}^m$ by $L(\mathbf{x}) = A\mathbf{x}$, for all $\mathbf{x} \in \mathbf{R}^n$. Show that L is a one-to-one function if $\det(A^TA) \neq 0$, where A^T is the transpose of A.

Solution: If $\det(A^TA) \neq 0$, then A^TA is an invertible matrix. If we define $K : \mathbf{R}^m \to \mathbf{R}^n$ by $K(\mathbf{x}) = (A^TA)^{-1}A^T\mathbf{x}$, for all $\mathbf{x} \in \mathbf{R}^m$, then KL is the identity function on $\mathbf{R}^m$. Exercise 2.1.18 in the text states that a function $f : A \to B$ is one-to-one if and only if there exists a function $g : B \to A$ such that $g \circ f = 1_A$. Our construction of the function K allows us to conclude (by Exercise 2.1.18) that L is one-to-one.

Comment: There is a stronger result that depends on knowing a little more linear algebra. In some linear algebra courses it is proved that $\det(A^TA)$ gives the n-dimensional "content" of the parallelepiped defined by the column vectors of A. This content is nonzero if and only if the vectors are linearly independent, and so $\det(A^TA) \neq 0$ if and only if the column vectors of A are linearly independent. According to the rank–nullity theorem, this happens if and only if the nullity of A is zero. In other words, L is a one-to-one linear transformation if and only if $\det(A^TA) \neq 0$.

35. Let A be an $n \times n$ matrix with entries in $\mathbf{R}$. Define a linear transformation $L : \mathbf{R}^n \to \mathbf{R}^n$ by $L(\mathbf{x}) = A\mathbf{x}$, for all $\mathbf{x} \in \mathbf{R}^n$. Prove that L is one-to-one if and only if no eigenvalue of A is equal to zero.

Note: A vector $\mathbf{x}$ is called an **eigenvector** of A if it is nonzero and there exists a scalar λ such a that $A\mathbf{x} = \lambda\mathbf{x}$, and in this case λ is called an **eigenvalue** of A.

Solution: As noted in the solution to Problem 33, $A\mathbf{x}_1 = A\mathbf{x}_2$ if and only if $A(\mathbf{x}_1 - \mathbf{x}_2) = \mathbf{0}$, and so L is one-to-one if and only if $A\mathbf{x} \neq \mathbf{0}$ for all nonzero vectors $\mathbf{x}$. This is equivalent to the statement that there is no nonzero vector $\mathbf{x}$ for which $A\mathbf{x} = 0 \cdot \mathbf{x}$, which translates into the given statement about eigenvalues of A.

ANSWERS AND HINTS

36. In each of the following parts, determine whether the given function is one-to-one and whether it is onto.
(a) $f : \mathbf{Z}_{12} \to \mathbf{Z}_{12}$; $f([x]_{12}) = [7x + 3]_{12}$, for all $[x]_{12} \in \mathbf{Z}_{12}$
Answer: The function is both one-to-one and onto.
(c) $f : \mathbf{Z}_{12} \to \mathbf{Z}_{12}$; $f([x]_{12}) = [x]_{12}^2$, for all $[x]_{12} \in \mathbf{Z}_{12}$
Answer: The function is neither one-to-one nor onto.
(e) $f : \mathbf{Z}_{12}^\times \to \mathbf{Z}_{12}^\times$; $f([x]_{12}) = [x]_{12}^2$, for all $[x]_{12} \in \mathbf{Z}_{12}^\times$
Answer: The function is neither one-to-one nor onto.
(f) $f : \mathbf{Z}_{12}^\times \to \mathbf{Z}_{12}^\times$; $f([x]_{12}) = [x]_{12}^3$, for all $[x]_{12} \in \mathbf{Z}_{12}^\times$
Answer: The function is both one-to-one and onto.

37. For each one-to-one and onto function in Problem 36, find the inverse of the function.
Answer: In both (a) and (f) the function is its own inverse.

39. Define $f : \mathbf{Z}_{10} \to \mathbf{Z}_{11}^\times$ by $f([m]_{10}) = [2]_{11}^m$, for all $[m]_{10} \in \mathbf{Z}_{10}$.
(b) Is f one-to-one and onto? *Answer:* Yes.

40. Define $f : \mathbf{Z}_8 \to \mathbf{Z}_{16}^\times$ by $f([m]_8) = [3]_{16}^m$, for all $[m]_8 \in \mathbf{Z}_8$.
(b) Is f one-to-one and onto? *Answer:* No.

42. Consider the function $f : \mathbf{Z}_{10} \to \mathbf{Z}_{10}$ defined by $f([x]_{10}) = [3x + 4]_{10}$. Show that f is one-to-one and onto by computing all values of the function. Then find a formula of the type $g([x]_{10}) = [mx + b]_{10}$ that gives the inverse of f.
Hint: The inverse of f is given by $g([x]_{10}) = [7x + 2]_{10}$.

2.2 Equivalence Relations

13. For the function $f : \mathbf{R} \to \mathbf{R}$ defined by $f(x) = x^2$, for all $x \in \mathbf{R}$, describe the equivalence relation $\sim_f$ on $\mathbf{R}$ that is determined by f.

Solution: The equivalence relation determined by f is defined by setting $a \sim_f b$ if $f(a) = f(b)$, so $a \sim b$ if and only if $a^2 = b^2$. Probably a better way to understand $\sim_f$ is to note that $a \sim_f b$ if and only if $|a| = |b|$.

14. (a) Define the function $f : \mathbf{Z}_{12} \to \mathbf{Z}_{18}$ by setting $f([x]_{12}) = [12x]_{18}$. Find the image $f(\mathbf{Z}_{12})$ of f and the factor set $\mathbf{Z}_{12}/f$ of $\mathbf{Z}_{12}$ determined by f and exhibit the one-to-one correspondence between them.

Solution: It follows from Exercise 2.1.11 that f is a function. (That exercise shows that $f : \mathbf{Z}_n \to \mathbf{Z}_k$ defined by $f([x]_n) = [mx]_k$ is a function if and only if $k \mid mn$.)

We have $f(\mathbf{Z}_{12}) = \{[0]_{18}, [6]_{18}, [12]_{18}\}$. Furthermore, $f([n]_{12}) = f([m]_{12})$ if and only if $[12n]_{18} = [12m]_{18}$ if and only if $18|12(n-m)$ if and only if $3|(n-m)$. Hence $[n]_{12} \sim [m]_{12}$ if and only if $n \equiv m \pmod 3$. Thus $\mathbf{Z}_{12}/f = \{[[0]_{12}, [[1]_{12}, [[2]_{12}]\}$, where $[[0]_{12}] = \{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}$, $[[1]_{12}] = \{[1]_{12}, [4]_{12}, [7]_{12}, [10]_{12}\}$, and $[[2]_{12}] = \{[2]_{12}, [5]_{12}, [8]_{12}, [11]_{12}\}$. Furthermore, $\bar{f} : \mathbf{Z}_{12}/f \to f(\mathbf{Z}_{12})$ is given by $\bar{f}([[n]_{12}]) = f([n]_{12}) = [12n]_{18}$. Hence $\bar{f}([[0]_{12}]) = [0]_{18}$, $\bar{f}([[1]_{12}]) = [12]_{18}$, $\bar{f}([[2]_{12}]) = [6]_{18}$.

(b) Define the formula $f : \mathbf{Z}_{12} \to \mathbf{Z}_{12}$ by $f([x]_{12}) = [x]_{12}^2$, for all $[x]_{12} \in \mathbf{Z}_{12}$. Show that the formula f defines a function. Find the image $f(\mathbf{Z}_{12})$ of f and the factor set $\mathbf{Z}_{12}/f$ of $\mathbf{Z}_{12}$ determined by f and exhibit the one-to-one correspondence between them.

Solution: The formula for f is well-defined since if $[x_1]_{12} = [x_2]_{12}$, then $x_1 \equiv x_2 \pmod{12}$, and so $x_1^2 \equiv x_2^2 \pmod{12}$, which shows that $f([x_1]_{12}) = f([x_2]_{12})$.

To compute the image of f we have $f([0]_{12}) = [0]_{12}^2 = [0]_{12}$, $f([\pm 1]_{12}) = [\pm 1]_{12}^2 = [1]_{12}$, $f([\pm 2]_{12}) = [\pm 2]_{12}^2 = [4]_{12}$, $f([\pm 3]_{12}) = [\pm 3]_{12}^2 = [9]_{12}$, $f([\pm 4]_{12}) = [\pm 4]_{12}^2 = [4]_{12}$, $f([\pm 5]_{12}) = [\pm 5]_{12}^2 = [1]_{12}$, and $f([\pm 6]_{12}) = [6]_{12}^2 = [0]_{12}$. Thus the image of f is $f(\mathbf{Z}_{12}) = \{[0]_{12}, [1]_{12}, [4]_{12}, [9]_{12}\}$.

The equivalence classes in $\mathbf{Z}_{12}/f$ that correspond to these elements are, respectively,

$\{[0]_{12}, [6]_{12}\}$, $\{[\pm 1]_{12}, [\pm 5]_{12}\}$, $\{[\pm 2]_{12}, [\pm 4]_{12}\}$, $\{[\pm 3]_{12}\}$.

15. For the linear transformation $L : \mathbf{R}^3 \to \mathbf{R}^3$ defined by

$$L(x, y, z) = (x + y + z, x + y + z, x + y + z) ,$$

for all $(x, y, z) \in \mathbf{R}^3$, give a geometric description of the partition of $\mathbf{R}^3$ that is determined by L.

Solution: Since $(a_1, a_2, a_3) \sim_L (b_1, b_2, b_3)$ if $L(a_1, a_2, a_3) = L(b_1, b_2, b_3)$, it follows from the definition of L that $(a_1, a_2, a_3) \sim_L (b_1, b_2, b_3)$ if and only if $a_1+a_2+a_3 = b_1+b_2+b_3$. For example, $\{(x, y, z) \mid L(x, y, z) = (0, 0, 0)\}$ is the plane through the origin whose equation is $x+y+z = 0$, with normal vector $(1, 1, 1)$. The other subsets in the partition of $\mathbf{R}^3$ defined by L are planes parallel to this one. Thus the partition consists of the planes perpendicular to the vector $(1, 1, 1)$.

16. For each of the following relations on the given set, determine which of the three conditions of Definition 2.2.1 hold.

(a) For $a, b \in \mathbf{Z}$, define $a \sim b$ if $a + b$ is even.

Solution: We first check the reflexive law. Given $a \in \mathbf{Z}$, it follows that $a + a$ is even, regardless of whether a is odd or even. Thus $a \sim a$, and the reflexive law holds.

We next check the symmetric law. Suppose that $a, b \in \mathbf{Z}$ are given, with $a \sim b$. Then $a+b$ is even, and so $b+a$ is even, showing that $b \sim a$. Thus the symmetric law holds.

Finally, we will check the transitive law. Let $a, b, c \in \mathbf{Z}$, with $a \sim b$ and $b \sim c$. Then $a+b$ and $b+c$ are even, and since $2b$ is even, we also have that $c-b = (b+c)-2b$ is even. The sum $a+c = (a+b)+(c-b)$ is even, showing that $a \sim c$, and so the transitive law holds.

(b) For $a, b \in \mathbf{Z}$, define $a \sim b$ if $a+b$ is odd.

Solution: The reflexive law does not hold, since $0+0$ is not odd, and thus 0 is not equivalent to itself.

The symmetric law holds, since $a+b = b+a$.

The transitive law does not hold. For example: $0 \sim 1$ and $1 \sim 2$, but $0 \sim 2$ is false.

(c) On $\mathbf{R}^\times$, define $a \sim b$ if $\dfrac{a}{b} \in \mathbf{Q}$.

Solution: Let $a, b, c \in \mathbf{R}^\times$. We have $a \sim a$ since $\dfrac{a}{a} = 1 \in \mathbf{Q}$. If $a \sim b$, then $\dfrac{a}{b} \in \mathbf{Q}$, and it follows that $\dfrac{b}{a} \in \mathbf{Q}$, so $b \sim a$. If $a \sim b$ and $b \sim c$, then $\dfrac{a}{b} \in \mathbf{Q}$ and $\dfrac{b}{c} \in \mathbf{Q}$, so $\dfrac{a}{c} = \dfrac{a}{b} \cdot \dfrac{b}{c} \in \mathbf{Q}$, and thus $a \sim c$. Therefore $\sim$ is an equivalence relation.

(d) On $\mathbf{R}^\times$, define $a \sim b$ if $\dfrac{a}{b} \in \mathbf{Z}$.

Solution: Let $a, b, c \in \mathbf{R}^\times$. We have $a \sim a$ since $\dfrac{a}{a} = 1 \in \mathbf{Z}$. The reflexive law does *not* hold, since $2 \sim 1$ but $1 \sim 2$ is false because $\dfrac{1}{2} \notin \mathbf{Z}$. The transitive law holds, as shown in part (c), since the product of two integers is an integer.

17. On the set $\{(a, b)\}$ of all ordered pairs of positive integers, define $(x_1, y_1) \sim (x_2, y_2)$ if $x_1 y_2 = x_2 y_1$. Show that this defines an equivalence relation.

Solution: We first show that the reflexive law holds. Given an ordered pair (a, b), we have $ab = ba$, and so $(a, b) \sim (a, b)$.

We next check the symmetric law. Given (a_1, b_1) and (a_2, b_2) with $(a_1, b_1) \sim (a_2, b_2)$, we have $a_1 b_2 = a_2 b_1$, and so $a_2 b_1 = a_1 b_2$, which shows that $(a_2, b_2) \sim (a_1, b_1)$.

Finally, we verify the transitive law. Given (a_1, b_1), (a_2, b_2), and (a_3, b_3) with $(a_1, b_1) \sim (a_2, b_2)$ and $(a_2, b_2) \sim (a_3, b_3)$, we have the equations $a_1 b_2 = a_2 b_1$ and $a_2 b_3 = a_3 b_2$. If we multiply the first equation by b_3 and the second equation by b_1, we get $a_1 b_2 b_3 = a_2 b_1 b_3 = a_3 b_1 b_2$. Since $b_2 \neq 0$ we can cancel to obtain $a_1 b_3 = a_3 b_1$, showing that $(a_1, b_1) \sim (a_3, b_3)$.

18. On the set $\mathbf{R}^2$, define $(x_1, y_1) \sim (x_2, y_2)$ if $x_1 y_1 = x_2 y_2$. Show that $\sim$ is an equivalence relation, and give a geometric description of the equivalence classes of $\sim$.

Solution: For any $(a, b) \in \mathbf{R}^2$, we have $(a, b) \sim (a, b)$ since $ab = ab$, which shows that $\sim$ is reflexive. If $(a, b) \sim (c, d)$, then $ab = cd$, and so $cd = ab$, which implies that $(c, d) \sim (a, b)$, and so $\sim$ is symmetric. If $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, then

$ab = cd$ and $cd = ef$. The transitive law for equality implies that $ab = ef$, and therefore $(a, b) \sim (e, f)$, so $\sim$ is transitive. We conclude that $\sim$ is an equivalence relation.

Given any $(a, b) \in \mathbf{R}^2$, the equivalence class of (a, b) is $\{(x, y) \mid xy = ab\}$. If $a = 0$ or $b = 0$, this set is the union of the x-axis and the y-axis. If $ab \neq 0$, then solving for y yields the equation $y = \dfrac{ab}{x}$ of a hyperbola. Thus the equivalence classes of $\sim$ consist of all hyperbolas of the form $y = \dfrac{k}{x}$, where k can be any nonzero real number, together with the "degenerate" hyperbola consisting of the two axes.

19. On $\mathbf{C}$, define $z_1 \sim z_2$ if $|z_1| = |z_2|$. Show that $\sim$ is an equivalence relation, and find the equivalence classes of $\sim$.

Solution: The reflexive, symmetric, and transitive laws can be easily verified since $\sim$ is defined in terms of an equality, and equality is itself an equivalence relation. In the complex plane, the equivalence classes are concentric circles, with center at the origin.

Alternate solution: Define $f : \mathbf{C} \to \mathbf{R}$ by $f(z) = |z|$, for all $z \in \mathbf{C}$. That is, $f(a+bi) = \sqrt{a^2 + b^2}$, for all complex numbers $a + bi$. The given relation is $\sim_f$, which we know to be an equivalence relation.

20. Let $\mathbf{u}$ be a fixed vector in $\mathbf{R}^3$, and assume that $\mathbf{u}$ has length 1. For vectors $\mathbf{v}$ and $\mathbf{w}$, define $\mathbf{v} \sim \mathbf{w}$ if $\mathbf{v} \cdot \mathbf{u} = \mathbf{w} \cdot \mathbf{u}$, where $\cdot$ denotes the standard dot product. Show that $\sim$ is an equivalence relation, and give a geometric description of the equivalence classes of $\sim$.

Solution: The reflexive, symmetric, and transitive laws for the relation $\sim$ really depend on equality, and can easily be verified. Since $\mathbf{u}$ has length 1, the scalar $\mathbf{v} \cdot \mathbf{u}$ represents the length of the projection of $\mathbf{v}$ onto the line determined by $\mathbf{u}$. Thus two vectors are equivalent if and only if they lie in the same plane perpendicular to $\mathbf{u}$. For example, the plane through the origin perpendicular to $\mathbf{u}$ is $\{\mathbf{v} \mid \mathbf{v} \cdot \mathbf{u} = 0\}$. It follows that the equivalence classes of $\sim$ are the planes in $\mathbf{R}^3$ that are perpendicular to $\mathbf{u}$.

21. Let $f : S \to T$ be a function. Given an equivalence relation $\simeq$ on T, define $\sim$ on S by setting $x_1 \sim x_2$ if $f(x_1) \simeq f(x_2)$, for all $x_1, x_2 \in S$. Prove that $\sim$ is an equivalence relation on S.

Solution: Given $a \in S$, we have $f(a) \simeq f(a)$, since $\simeq$ is reflexive, and therefore $a \sim a$.

If $a \sim b$ for $a, b \in S$, then $f(a) \simeq f(b)$, and so $f(b) \simeq f(a)$ since $\simeq$ is symmetric. This implies that $b \sim a$.

If $a \sim b$ and $b \sim c$ for $a, b, c \in S$, then $f(a) \simeq f(b)$ and $f(b) \simeq f(c)$, which implies that $f(a) \simeq f(c)$, since $\simeq$ is transitive. It follows that $a \sim c$.

We have shown that $\sim$ is reflexive, symmetric, and transitive, so it is an equivalence relation.

Comment: If the equivalence relation $\simeq$ on T is ordinary equality, then the corresponding equivalence relation on S (as defined in the problem) is $\sim_f$.

22. Let $f : S \to T$ be an onto function. Let $\{P_\alpha\}_{\alpha \in I}$ be a partition of T. Prove that $\mathcal{P} = \{f^{-1}(P_\alpha) \mid \alpha \in I\}$ is a partition of S.

Solution: Since f is an onto function, and each set P_α is nonempty, it follows that each set $f^{-1}(P_\alpha)$ is nonempty. For any element $s \in S$, the image $f(s)$ belongs to some set P_α, and then $s \in f^{-1}(P_\alpha)$. Finally, for any indices $\alpha \neq \beta$, it follows from Problem 2.1.32 (c) that $f^{-1}(P_\alpha) \cap f^{-1}(P_\beta) = f^{-1}(P_\alpha \cap (P_\beta) = f^{-1}(\emptyset) = \emptyset$. This shows that $\mathcal{P}$ is a partition of S.

ANSWERS AND HINTS

23. Define $f : \mathbf{Z}_8 \to \mathbf{Z}_{12}$ by $f([x]_8) = [3x]_{12}$, for all $[x]_8 \in \mathbf{Z}_8$.
(b) Find the image $f(\mathbf{Z}_8)$ and the set of equivalence classes $\mathbf{Z}_8/f$ defined by f, and exhibit the one-to-one correspondence between these sets.
Answer: The image of f is the subset $\{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}$. The corresponding preimages, in order, are the sets $\{[0]_8, [4]_8\}$, $\{[1]_8, [5]_8\}$, $\{[2]_8, [6]_8\}$, $\{[3]_8, [7]_8\}$, and these make up the factor set $\mathbf{Z}_8/f$.

25. For $[x]_{15}$, let $f([x]_{15}) = [3x]_5^3$.
(b) Find $f(\mathbf{Z}_{15}^\times)$ and $\mathbf{Z}_{15}^\times/f$ and exhibit the one-to-one correspondence between them.
Answer: Since $f(\mathbf{Z}_{15}^\times) = \{[1]_5, [2]_5, [-2]_5, [-1]_5\} = \mathbf{Z}_5^\times$, the corresponding preimages, in order, are $\{[2]_{15}, [7]_{15}\}$, $\{[1]_{15}, [-4]_{15}\}$, $\{[-1]_{15}, [4]_{15}\}$, $\{[-2]_{15}, [-7]_{15}\}$, and these make up the factor set $\mathbf{Z}_{15}^\times/f$.

26. For each of the following relations on $\mathbf{R}$, determine which of the three conditions of Definition 2.2.1 hold.
(a) Define $a \sim b$ if $b = a^2$. *Answer:* None of the conditions hold.
(d) Define $a \sim b$ if $b = a + q\pi$, for some $q \in \mathbf{Q}^+$.
Answer: Only the transitive law holds.

27. For each of the following relations on the given set, determine which of the three conditions of Definition 2.2.1 hold.
(a) For $(x_1, y_1), (x_2, y_2) \in \mathbf{R}^2$, define $(x_1, y_1) \sim (x_2, y_2)$ if $2(y_1 - x_1) = 3(y_2 - x_2)$.
Answer: All three conditions hold.
(c) Let P be the set of all people living in North America. For $p, q \in P$, define $p \sim q$ if p is the sister of q.
Answer: None of the three conditions hold.

30. Let $\sim$ be an equivalence relation on the set S. Show that $[a] = [b]$ if and only if $a \sim b$.
Hint: You can give a direct proof (which uses all three properties of an equivalence relation) or you can use part of the proof of Theorem 2.2.5 in **Abstract Algebra**.

2.3 Permutations

17. For the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 6 & 9 & 2 & 4 & 8 & 1 & 3 \end{pmatrix}$, write σ as a product of disjoint cycles. What is the order of σ? Write σ as a product of transpositions. Is σ an even permutation? Compute σ^{-1}.

Solution: Starting with 1, we have $\sigma(1) = 7$, $\sigma^2(1) = \sigma(7) = 8$, and $\sigma^3(1) = \sigma(8) = 1$, so the first cycle is $(1, 7, 8)$. The smallest number not in this cycle is 2, and starting with 2 we get the cycle $(2, \sigma(2)) = (2, 5)$. Continuing, we get $\sigma = (1, 7, 8)(2, 5)(3, 6, 4, 9)$. By Proposition 2.3.8, σ has order 12, since $\text{lcm}[3, 2, 4] = 12$.

To write σ as a product of transpositions, we can simply write $(1, 7, 8)(2, 5)(3, 6, 4, 9) = (1, 7)(7, 8)(2, 5)(3, 6)(6, 4)(4, 9)$. Since σ can be expressed as the product of 6 transpositions, it is an even permutation.

Finally, we have $\sigma^{-1} = (1, 8, 7)(2, 5)(3, 9, 4, 6)$. (Note that since the cycles are disjoint they commute with each other, and so here the order of the cycles is not important.)

18. For the permutations $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 1 & 8 & 3 & 6 & 4 & 7 & 9 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 4 & 7 & 2 & 6 & 8 & 9 & 3 \end{pmatrix}$, write each of these permutations as a product of disjoint cycles: σ, τ, $\sigma\tau$, $\sigma\tau\sigma^{-1}$, σ^{-1}, τ^{-1}, $\tau\sigma$, $\tau\sigma\tau^{-1}$.

Solution: $\sigma = (1, 2, 5, 3)(4, 8, 7)$; $\tau = (2, 5)(3, 4, 7, 8, 9)$; $\sigma\tau = (1, 2, 3, 8, 9)$;

$\sigma\tau\sigma^{-1} = (1, 8, 4, 7, 9)(3, 5)$; $\sigma^{-1} = (1, 3, 5, 2)(4, 7, 8)$; $\tau^{-1} = (2, 5)(3, 9, 8, 7, 4)$;

$\tau\sigma = (1, 5, 4, 9, 3)$; $\tau\sigma\tau^{-1} = (1, 5, 2, 4)(7, 9, 8)$.

19. Let $\sigma = (2, 4, 9, 7,)(6, 4, 2, 5, 9)(1, 6)(3, 8, 6) \in S_9$. Write σ as a product of disjoint cycles. What is the order of σ? Compute σ^{-1}.

Solution: We have $\sigma = (1, 9, 6, 3, 8)(2, 5, 7)$, so it has order $15 = \text{lcm}[5, 3]$, and $\sigma^{-1} = (1, 8, 3, 6, 9)(2, 7, 5)$.

20. Compute the order of $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 2 & 11 & 4 & 6 & 8 & 9 & 10 & 1 & 3 & 5 \end{pmatrix}$. For $\sigma = (3, 8, 7)$, compute the order of $\sigma\tau\sigma^{-1}$.

Solution: Since $\tau = (1, 7, 9)(3, 11, 5, 6, 8, 10)$, it has order $6 = \text{lcm}[3, 6]$. Then $\sigma\tau\sigma^{-1} = (3, 8, 7)(1, 7, 9)(3, 11, 5, 6, 8, 10)(3, 7, 8) = (1, 3, 9)(8, 11, 5, 6, 7, 10)$, so the cycle structure of $\sigma\tau\sigma^{-1}$ is the same as that of τ, and thus $\sigma\tau\sigma^{-1}$ has order 6.

21. Prove that if $\tau \in S_n$ is a permutation with order m, then $\sigma\tau\sigma^{-1}$ has order m, for any permutation $\sigma \in S_n$.

Solution: Assume that $\tau \in S_n$ has order m. It follows from the identity $(\sigma\tau\sigma^{-1})^k = \sigma\tau^k\sigma^{-1}$ that $(\sigma\tau\sigma^{-1})^m = \sigma\tau^m\sigma^{-1} = \sigma(1)\sigma^{-1} = (1)$. On the other hand, the order of $\sigma\tau\sigma^{-1}$ cannot be less than n, since $(\sigma\tau\sigma^{-1})^k = (1)$ implies $\sigma\tau^k\sigma^{-1} = (1)$, and then $\tau^k = \sigma^{-1}\sigma = (1)$.

22. Show that S_{10} has elements of order 10, 12, and 14, but not 11 or 13.

Solution: The element $(1, 2)(3, 4, 5, 6, 7)$ has order 10, the element $(1, 2, 3)(4, 5, 6, 7)$ has order 12, and $(1, 2)(3, 4, 5, 6, 7, 8, 9)$ has order 14. On the other hand, since 11 and 13 are prime, any element of order 11 or 13 would have to be a cycle, and there are no cycles of that length in S_{10}.

23. Let S be a set, and let $X \subseteq S$. Let $G = \{\sigma \in \mathrm{Sym}(S) \mid \sigma(X) = X\}$. Prove that G is a group of permutations.

Solution: If $\sigma, \tau \in G$, then $\sigma\tau(X) = \sigma(\tau(X)) = \sigma(X) = X$, which shows that $\sigma\tau \in G$. It is clear that $1_S(X) = X$, and thus $1_S \in G$. Finally, if $\sigma \in G$, then $\sigma^{-1}(X) = \sigma^{-1}(\sigma(X)) = X$, which shows that $\sigma^{-1} \in G$.

24. Let G be a group of permutations, with $G \subseteq \mathrm{Sym}(S)$, for the set S. Let τ be a fixed permutation in $\mathrm{Sym}(S)$. Prove that

$$\tau G \tau^{-1} = \{\sigma \in \mathrm{Sym}(S) \mid \sigma = \tau\gamma\tau^{-1} \text{ for some } \gamma \in G\}$$

is a group of permutations.

Solution: If $\sigma_1, \sigma_2 \in \tau G \tau^{-1}$, then we can write $\sigma_1 = \tau\gamma_1\tau^{-1}$ and $\sigma_2 = \tau\gamma_2\tau^{-1}$ for some $\gamma_1, \gamma_2 \in G$. Then $\sigma_1\sigma_2 = \tau\gamma_1\tau^{-1}\tau\gamma_2\tau^{-1} = \tau(\gamma_1\gamma_2)\tau^{-1}$ belongs to $\tau G\tau^{-1}$ since $\gamma_1\gamma_2 \in G$. We have $1_S = \tau\tau^{-1} = \tau 1_S \tau^{-1}$, and so $1_S \in \tau G\tau^{-1}$. If $\sigma = \tau\gamma\tau^{-1}$, then $\sigma^{-1} = (\tau\gamma\tau^{-1})^{-1} = (\tau^{-1})^{-1}\gamma^{-1}\tau^{-1} = \tau\gamma^{-1}\tau^{-1}$, which shows that $\sigma^{-1} \in \tau G\tau^{-1}$ since $\gamma^{-1} \in G$.

ANSWERS AND HINTS

25. Consider the following permutations in S_7.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 6 & 1 & 7 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 5 & 7 & 4 & 6 & 3 \end{pmatrix}$$

Compute the following products.

Answer: (a) $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 6 & 7 & 4 & 1 & 5 \end{pmatrix}$

Answer: (c) $\sigma\tau\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 2 & 7 & 6 & 4 & 5 \end{pmatrix}$

26. Using the permutations σ and τ from Problem 25, write each of the permutations $\sigma\tau$, $\tau\sigma$, $\tau^2\sigma$, σ^{-1}, $\sigma\tau\sigma^{-1}$, $\tau\sigma\tau^{-1}$ and $\tau^{-1}\sigma\tau$ as a product of disjoint cycles. Write σ and τ as products of transpositions.

Answers: $\sigma = (1,3,5,6) = (1,3)(3,5)(5,6)$ $\tau = (1,2)(3,5,4,7) = (1,2)(3,5)(5,4)(4,7)$
$\sigma\tau = (1,2,3,6)(4,7,5)$ $\sigma\tau\sigma^{-1} = (2,3)(4,7,5,6)$ $\tau^{-1}\sigma\tau = (2,7,3,6)$

28. Let $\sigma = (3,6,8)(1,9,4,3,2,7,6,8,5)(2,3,9,7) \in S_9$.
(b) Is σ an even permutation or an odd permutation? *Answer:* Odd
(c) What is the order of σ in S_9? *Answer:* 12

29. Let $\sigma = (2,3,9,6)(7,3,2,5,9)(1,7)(4,8,7) \in S_9$.
(b) Is σ an even permutation or an odd permutation? *Answer:* Even
(c) What is the order of σ in S_9? *Answer:* 15

Review Problems

1. For the function $f : \mathbf{Z}_{16} \to \mathbf{Z}_{16}$ defined by $f([x]_{16}) = [x^2]_{16}$, for all $[x]_{16} \in \mathbf{Z}_{16}$, describe the equivalence relation $\sim_f$ on $\mathbf{Z}_{16}$ that is determined by f.

   Solution: We begin by computing the image of f. We have $[0^2]_{16} = [0]_{16}$, $[(\pm 1)^2]_{16} = [1]_{16}$, $[(\pm 2)^2]_{16} = [4]_{16}$, $[(\pm 3)^2]_{16} = [9]_{16}$, $[(\pm 4)^2]_{16} = [16]_{16} = [0]_{16}$, $[(\pm 5)^2]_{16} = [25]_{16} = [9]_{16}$, $[(\pm 6)^2]_{16} = [36]_{16} = [4]_{16}$, $[(\pm 7)^2]_{16} = [49]_{16} = [1]_{16}$, and $[8^2]_{16} = [64]_{16} = [0]_{16}$. Thus the image of f is the set $\{[0]_{16}, [1]_{16}, [4]_{16}, [9]_{16}\}$. The equivalence classes that correspond to these elements are (in order)

   $\{[0]_{16}, [4]_{16}, [8]_{16}, [12]_{16}\}$, $\{[1]_{16}, [7]_{16}, [9]_{16}, [15]_{16}\}$,

   $\{[2]_{16}, [6]_{16}, [10]_{16}, [14]_{16}\}$, and $\{[3]_{16}, [5]_{16}, [11]_{16}, [13]_{16}\}$.

2. Define $f : \mathbf{Z}_7 \to \mathbf{Z}_7$ by $f([x]_7) = [x^3 + 3x - 5]_7$, for all $[x]_7 \in \mathbf{Z}_7$. Is f a one-to-one correspondence?

   Solution: We need to calculate the values of the function. We have $f([0]_7) = [-5]_7 = [2]_7$, $f([1]_7) = [1^3 + 3 \cdot 1 - 5]_7 = [-1]_7 = [6]_7$, $f([-1]_7) = [(-1)^3 + 3 \cdot (-1) - 5]_7 = [-9]_7 = [5]_7$, $f([2]_7) = [2^3 + 3 \cdot 2 - 5]_7 = [9]_7 = [2]_7$. Since $f([2]_7) = f([0]_7)$, the function is not a one-to-one correspondence.

   Just out of curiosity we will find the remaining values. We have $f([-2]_7) = [(-2)^3 + 3 \cdot (-2) - 5]_7 = [-19]_7 = [2]_7$, $f([3]_7) = [3^3 + 3 \cdot 3 - 5]_7 = [31]_7 = [3]_7$, and $f([-3]_7) = [(-3)^3 + 3 \cdot (-3) - 5]_7 = [-41]_7 = [1]_7$.

3. On the set $\mathbf{Q}$ of rational numbers, define $x \sim y$ if $x - y$ is an integer. Show that $\sim$ is an equivalence relation.

   Solution: If $x \in \mathbf{Q}$, then $x \sim x$ since $x - x = 0$ is an integer. If $x, y \in \mathbf{Q}$ and $x \sim y$, then $x - y \in \mathbf{Z}$, so $y - x = -(x - y) \in \mathbf{Z}$, and therefore $y \sim x$. If $x, y, z \in \mathbf{Q}$ with $x \sim y$ and $y \sim z$, then $x - y$ and $y - z$ are integers, so the sum $x - z = (x - y) + (y - z)$ is an integer, showing that $x \sim z$.

4. In S_{10}, let $\alpha = (1, 3, 5, 7, 9)$, $\beta = (1, 2, 6)$, and $\gamma = (1, 2, 5, 3)$. For $\sigma = \alpha\beta\gamma$, write σ as a product of disjoint cycles, and use this to find its order and its inverse. Is σ even or odd?

   Solution: We have $\sigma = (1, 6, 3, 2, 7, 9)$, so σ has order 6, and

   $\sigma^{-1} = (1, 9, 7, 2, 3, 6)$. Since σ has length 6, it can be written as a product of 5 transpositions, so it is an odd permutation.

5. Define the function $\phi : \mathbf{Z}_{17}^{\times} \to \mathbf{Z}_{17}^{\times}$ by $\phi(x) = x^{-1}$, for all $x \in \mathbf{Z}_{17}^{\times}$. Is ϕ one to one? Is ϕ onto? If possible, find the inverse function ϕ^{-1}.

   Solution: For all $x \in \mathbf{Z}_{17}^{\times}$ we have $\phi(\phi(x)) = \phi(x^{-1}) = (x^{-1})^{-1} = x$, so $\phi = \phi^{-1}$, which also shows that ϕ is one-to-one and onto.

6. (a) Let α be a fixed element of S_n. Show that $\phi_\alpha : S_n \to S_n$ defined by $\phi_\alpha(\sigma) = \alpha\sigma\alpha^{-1}$, for all $\sigma \in S_n$, is a one-to-one and onto function.

   Solution: If $\phi_\alpha(\sigma) = \phi_\alpha(\tau)$, for $\sigma, \tau \in S_n$, then $\alpha\sigma\alpha^{-1} = \alpha\tau\alpha^{-1}$. We can multiply on the left by α^{-1} and on the right by α, to get $\sigma = \tau$, so ϕ_α is one-to-one. Finally, given $\tau \in S_n$, we have $\phi_\alpha(\sigma) = \tau$ for $\sigma = \alpha^{-1}\tau\alpha$, and so ϕ_α is onto.

   Alternate solution: To show that ϕ_α is one-to-one and onto you could also show that it has an inverse function. A short computation shows that $(\phi_\alpha)^{-1} = \phi_{\alpha^{-1}}$.

   (b) In S_3, let $\alpha = (1, 2)$. Compute ϕ_α.

   Solution: Since $(1, 2)$ is its own inverse, direct computations show that

   $\phi_\alpha((1)) = (1)$, $\phi_\alpha((1, 2)) = (1, 2)$, $\phi_\alpha((1, 3)) = (2, 3)$, $\phi_\alpha((2, 3)) = (1, 3)$,

   $\phi_\alpha((1, 2, 3)) = (1, 3, 2)$, and $\phi_\alpha((1, 3, 2)) = (1, 2, 3)$.

7. Let S be the set of all $n \times n$ matrices with real entries. For $A, B \in S$, define $A \sim B$ if there exists an invertible matrix P such that $B = PAP^{-1}$. Prove that $\sim$ is an equivalence relation.

   Comment: When multiplying matrices, be careful not to mix up the sides, because matrices don't necessarily satisfy the commutative law. If they did, similarity would be the same as equality. Review your linear algebra textbook if you need to.

   Solution: Let A be any $n \times n$ matrix. Since $A = IAI^{-1}$ for the identity matrix I, it follows that $A \sim A$. (You could use $P = A$ instead of $P = I$.)

   Let A, B be $n \times n$ matrices with $A \sim B$. Then there exists an invertible matrix P with $B = PAP^{-1}$. To solve for A, multiply on the left by P^{-1} and on the right by P. So we get $P^{-1}BP = A$. To put this in the right form, note that $P = (P^{-1})^{-1}$. Then we have $P^{-1}B(P^{-1})^{-1} = A$ and so $B \sim A$.

   Suppose that A, B, C are $n \times n$ matrices with $A \sim B$ and $B \sim C$. Then there exist invertible matrices P and Q with $B = PAP^{-1}$ and $C = QBQ^{-1}$. (Don't make the mistake of assuming that you can use P in both places.) Substituting for B in the second equation, $C = Q(PAP^{-1})Q^{-1} = (QP)A(QP)^{-1}$, and thus $A \sim C$.

   We have verified that the reflexive, symmetric, and transitive properties hold, so $\sim$ is an equivalence relation.

8. Show that S_n contains $n(n-1)/2$ transpositions.

   Solution: In constructing a transposition (a, b), we have n choices for a and $n - 1$ choices for b. But since in cycle notation we have $(b, a) = (a, b)$, we have really only constructed $n(n-1)/2$ *different* transpositions.

Chapter 3

Groups

3.1 Definition of a Group

25. Use the dot product to define a multiplication on $\mathbf{R}^3$. Does this make $\mathbf{R}^3$ into a group?

    Solution: The dot product of two vectors is a scalar, not a vector. This means that the dot product does not even define a binary operation on the set of vectors in $\mathbf{R}^3$.

26. For vectors (x_1, y_1, z_1) and (x_2, y_2, z_2) in $\mathbf{R}^3$, the cross product is defined by

$$(x_1, y_1, z_1) \times (x_2, y_2, z_2) = (y_1 z_2 - z_1 y_2,\ z_1 x_2 - x_1 z_2,\ x_1 y_2 - y_1 x_2)\ .$$

    Is $\mathbf{R}^3$ a group under this multiplication?

    Solution: The cross product of the zero vector and any other vector is the zero vector, so the cross product cannot be used to make the set of all vectors in $\mathbf{R}^3$ into a group.

    Even if we were to exclude the zero vector we would still have problems. The cross product of two nonzero vectors defines a vector that is perpendicular to each of the given vectors. This means that the operation could not have an identity element, again making it impossible to define a group structure.

27. On the set $G = \mathbf{Q}^\times$ of nonzero rational numbers, define a new multiplication by $a * b = \dfrac{ab}{2}$, for all $a, b \in G$. Show that G is a group under this multiplication.

    Solution: If a and b are nonzero rational numbers, then ab is a nonzero rational number, and so is $\dfrac{ab}{2}$, showing that the operation is closed on the set G. The operation is associative since

$$a * (b * c) = a * \left(\frac{bc}{2}\right) = \frac{a\left(\frac{bc}{2}\right)}{2} = \frac{a(bc)}{4}$$

    and

$$(a * b) * c = \left(\frac{ab}{2}\right) * c = \frac{\left(\frac{ab}{2}\right) c}{2} = \frac{(ab)c}{4}\ .$$

Check that the number 2 acts as the multiplicative identity, and if a is nonzero, then $4/a$ is a nonzero rational number that serves as the multiplicative inverse of a.

28. Write out the multiplication table for $\mathbf{Z}_{18}^{\times}$.

Solution: $\mathbf{Z}_{18}^{\times} = \{[1]_{18}, [5]_{18}, [7]_{18}, [11]_{18}, [13]_{18}, [17]_{18}\}$. We will write m for $[m]_{18}$.

$\cdot$	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

Comment: Rewriting the table, with the elements in a slightly different order, gives a different picture of the group.

$\cdot$	1	5	7	17	13	11
1	1	5	7	17	13	11
5	5	7	17	13	11	1
7	7	17	13	11	1	5
17	17	13	11	1	5	7
13	13	11	1	5	7	17
11	11	1	5	7	17	13

Each element in the group is a power of 5, and the second table shows what happens when we arrange the elements in order, as successive powers of 5.

29. Write out the multiplication table for $\mathbf{Z}_{15}^{\times}$.

Solution: $\mathbf{Z}_{15}^{\times} = \{[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15}\}$. We will write the elements as $\{1, 2, 4, 7, -7, -4, -2, -1\}$.

$\cdot$	1	-1	2	-2	4	-4	7	-7
1	1	-1	2	-2	4	-4	7	-7
-1	-1	1	-2	2	-4	4	-7	7
2	2	-2	4	-4	-7	7	-1	1
-2	-2	2	-4	4	7	-7	1	-1
4	4	-4	-7	7	1	-1	-2	2
-4	-4	4	7	-7	-1	1	2	-2
7	7	-7	-1	1	-2	2	4	-4
-7	-7	7	1	-1	2	-2	-4	4

Comment: Notice how much easier it is to use the representatives $\{\pm 1, \pm 2, \pm 4, \pm 7\}$ when listing the congruence classes in the group.

30. Let G be a group, and suppose that a and b are any elements of G. Show that if $(ab)^2 = a^2b^2$, then $ba = ab$.

Solution: Assume that a and b are elements of G for which $(ab)^2 = a^2b^2$. Expanding this equation gives us

$$(ab)(ab) = a^2b^2 \ .$$

Since G is a group, both a and b have inverses, denoted by a^{-1} and b^{-1}, respectively. Multiplication in G is well-defined, so we can multiply both sides of the equation on the left by a^{-1} without destroying the equality.

If we are to be precise about using the associative law, we have to include the following steps.

$$\begin{aligned} a^{-1}((ab)(ab)) &= a^{-1}(a^2b^2) \\ (a^{-1}(ab))(ab) &= (a^{-1}a^2)b^2 \\ ((a^{-1}a)b))(ab) &= ((a^{-1}a)a)b^2 \\ (eb)(ab) &= (ea)b^2 \\ b(ab) &= ab^2 \end{aligned}$$

The next step is to multiply on the right by b^{-1}. The associative law for multiplication essentially says that parentheses don't matter, so we don't really need to include all of the steps we showed before.

$$\begin{aligned} b(ab)b^{-1} &= (ab^2)b^{-1} \\ (ba)(bb^{-1}) &= (ab)(bb^{-1}) \\ ba &= ab \end{aligned}$$

This completes the proof, since we have shown that if $(ab)^2 = a^2b^2$, then $ba = ab$.

31. Let G be a group, and suppose that a and b are any elements of G. Show that $(aba^{-1})^n = ab^na^{-1}$, for any positive integer n.

Solution: To give a careful proof we need to use induction. The statement for $n = 1$ is simply that $aba^{-1} = aba^{-1}$, which is certainly true. Now assume that the result holds for $n = k$. Using this induction hypothesis, we have the following calculation.

$$\begin{aligned} (aba^{-1})^{k+1} &= (aba^{-1})^k(aba^{-1}) \\ &= (ab^ka^{-1})(aba^{-1}) \\ &= (ab^k)(a^{-1}a)(ba^{-1}) \\ &= (ab^k)(ba^{-1}) \\ &= ab^{k+1}a^{-1} \end{aligned}$$

Thus the statement holds for $n = k+1$. The principle of mathematical induction now guarantees that $(aba^{-1})^n = ab^na^{-1}$ for all positive integers n.

32. In Definition 3.1.4, replace condition (iii) with the condition that there exists $e \in G$ such that $e \cdot a = a$ for all $a \in G$, and replace condition (iv) with the condition that for each $a \in G$ there exists $a' \in G$ with $a' \cdot a = e$. Prove that these weaker conditions (given only on the left) still imply that G is a group.

Solution: Assume that the two replacement conditions hold. Note the $e \cdot e = e$, and that the associative law holds.

We will first show that $a \cdot e = a$, for all $a \in G$. Let a' be an element in G with $a' \cdot a = e$. Then

$$a' \cdot (a \cdot e) = (a' \cdot a) \cdot e = e \cdot e = e = a' \cdot a \ ,$$

and since there exists an element $a'' \in G$ with $a'' \cdot a' = e$, we can cancel a' from the left of the above equation, to get $a \cdot e = a$. This shows that e is a multiplicative identity for G, and so the original condition (iii) is satisfied.

We also have the equation

$$a' \cdot (a \cdot a') = (a' \cdot a) \cdot a' = e \cdot a' = a' = a' \cdot e \ ,$$

and then (as above) we can cancel a' to get $a \cdot a' = e$, which shows that a' is indeed the multiplicative inverse of a. Thus the original condition (iv) holds, and so G is a group under the given operation.

33. Problem 32 shows that in the definition of a group it is sufficient to require the existence of a left identity element and the existence of left inverses. Give an example to show that it is *not* sufficient to require the existence of a left identity element together with the existence of *right* inverses.

Solution: On the set G of nonzero real numbers, define the operation $a * b = |a|b$, for all $a, b \in G$. Then $a * b \neq 0$ if $a \neq 0$ and $b \neq 0$, so we have defined a binary operation on G. The operation is associative since $a * (b * c) = a * (|b|c) = |a||b|c = |ab|c$ and $(a * b) * c = (|a|b) * c = ||a|b|c = |ab|c$. The number 1 is a left identity element, since $1 * a = |1|a = a$ for all $a \in G$. There is no right identity element, since the two equations $1 * x = 1$ and $(-1) * x = -1$ lead to $x = 1$ and $x = -1$, which have no simultaneous solution in G. Finally, $1/|a|$ is a right inverse for any $a \in G$, but the equation $x * a = |x|a = 1$ has no solution for $a = -1$, so -1 has no left inverse.

In summary, we have shown that G is not a group, even though it has a left identity element and right inverses.

34. Let F be the set of all **fractional linear transformations** of the complex plane. That is, F is the set of all functions $f(z) : \mathbf{C} \to \mathbf{C}$ of the form $f(z) = \dfrac{az + b}{cz + d}$, where the coefficients a, b, c, d are integers with $ad - bc = 1$. Show that F forms a group if we take the operation to be composition of functions.

Solution: We first need to check that composition of functions defines a binary operation on F, so we need to check the closure axiom in Definition 3.1.4. Let

$f_1(z) = \dfrac{a_1z + b_1}{c_1z + d_1}$, and $f_2(z) = \dfrac{a_2z + b_2}{c_2z + d_2}$, with $a_1d_1 - b_1c_1 = 1$ and $a_2d_2 - b_2c_2 = 1$. Then for any complex number z we have

$$\begin{aligned} f_2 \circ f_1(z) &= f_2(f_1(z)) = \frac{a_2 f_z(z) + b_2}{c_2 f_z(z) + d_2} \\ &= \frac{a_2\left(\frac{a_1z+b_1}{c_1z+d_1}\right) + b_2}{c_2\left(\frac{a_1z+b_1}{c_1z+d_1}\right) + d_2} \\ &= \frac{a_2(a_1z + b_1) + b_2(c_1z + d_1)}{c_2(a_1z + b_1) + d_2(c_1z + d_1)} \\ &= \frac{(a_2a_1 + b_2c_1)z + (a_2b_1 + b_2d_1)}{(c_2a_1 + d_2c_1)z + (c_2b_1 + d_2d_1)} . \end{aligned}$$

You can see that verifying all of the axioms is going to be painful. We need a better way to look at the entire situation, so let's look at the following matrix product.

$$\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} = \begin{bmatrix} a_2a_1 + b_2c_1 & a_2b_1 + b_2d_1 \\ c_2a_1 + d_2c_1 & c_2b_1 + d_2d_2 \end{bmatrix}$$

If we associate with the fractional linear transformations $f_2(z) = \dfrac{a_2z + b_2}{c_2z + d_2}$ and $f_1(z) = \dfrac{a_1z + b_1}{c_1z + d_1}$ the matrices $\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ and $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$, respectively, then we can see that composition of two fractional linear transformations corresponds to the product of the two associated matrices. Furthermore, the condition that $ad - bc = 1$ for a fractional linear transformation corresponds to the condition that the determinant of the associated matrix is equal to 1. All of this means that it is fair to use what we already know about matrix multiplication. The proof that the determinant of a product is the product of the determinants can be used to show that in the composition $f_2 \circ f_1$ we will still have the required condition on the coefficients that we calculated.

Composition of functions is associative, by Proposition 2.1.3. The identity function will serve as an identity element for F, and we only need to check that it can be written in the correct form, as a fractional linear transformation. This can be shown by choosing coefficients $a = 1$, $b = 0$, $c = 0$, and $d = 1$. Finally, we can use the formula for the inverse of a 2×2 matrix with determinant 1 to find an inverse function for $f(z) = \dfrac{az + b}{cz + d}$. This gives $f^{-1}(z) = \dfrac{dz - b}{-cz + a}$, and completes the proof that F forms a group under composition of functions.

35. Let $G = \{x \in \mathbf{R} \mid x > 1\}$ be the set of all real numbers greater than 1. For $x, y \in G$, define $x * y = xy - x - y + 2$.

(a) Show that the operation $*$ is closed on G.

Solution: If $a, b \in G$, then $a > 1$ and $b > 1$, so $b-1 > 0$, and therefore $a(b-1) > (b-1)$. It follows immediately that $ab - a - b + 2 > 1$.

(b) Show that the associative law holds for $*$.

Solution: For $a, b, c \in G$, we have

$$\begin{aligned} a*(b*c) &= a*(bc-b-c+2) \\ &= a(bc-b-c+2)-a-(bc-b-c+2)+2 \\ &= abc-ab-ac-bc+a+b+c\,. \end{aligned}$$

On the other hand, we have

$$\begin{aligned} (a*b)*c &= (ab-a-b+2)*c \\ &= (ab-a-b+2)c-(ab-a-b+2)-c+2 \\ &= abc-ab-ac-bc+a+b+c\,. \end{aligned}$$

Thus $a*(b*c) = (a*b)*c$.

(c) Show that 2 is the identity element for the operation $*$.

Comment: The given operation is commutative since $x*y = xy-x-y+2 = yx-y-x+2 = y*x$.

Solution: Since $*$ commutative, the one computation $2*y = 2y-2-y+2 = y$ suffices to show that 2 is the identity element.

(d) Show that for element $a \in G$ there exists an inverse $a^{-1} \in G$.

Solution: Given any $a \in G$, we need to solve $a*y = 2$. This gives us the equation $ay-a-y+2 = 2$, which has the solution $y = a/(a-1)$. This solution belongs to G since $a > a-1$ implies $a/(a-1) > 1$. Finally, $a*(a/a-1) = a^2/(a-1)-a-a/(a-1)+2 = (a^2-a^2+a-a)/(a-1)+2 = 2$.

ANSWERS AND HINTS

36. For each binary operation $*$ given below, determine whether or not $*$ defines a group structure on the given set. If not, list the group axioms that fail to hold.
(a) Define $*$ on $\mathbf{Z}$ by $a*b = \min\{a,b\}$.
Answer: The operation is associative, but has no identity element.
(b) Define $*$ on $\mathbf{Z}^+$ by $a*b = \min\{a,b\}$.
Answer: The operation is associative, and 1 is an identity element, but no other element has an inverse.
(c) Define $*$ on $\mathbf{Z}^+$ by $a*b = \max\{a,b\}$.
Answer: (c) The operation is associative, but has no identity element.

37. For each binary operation $*$ given below, determine whether or not $*$ defines a group structure on the given set. If not, list the group axioms that fail to hold.
(a) Define $*$ on $\mathbf{R}$ by $x*y = x+y-1$.
Answer: The set $\mathbf{R}$ is a group under this operation.
(b) Define $*$ on $\mathbf{R}^\times$ by $x*y = xy+1$.
Answer: The operation is not a binary operation (since closure fails).

(c) Define $*$ on $\mathbf{Q}^+$ by $x * y = \dfrac{1}{x} + \dfrac{1}{y}$.

Answer: This binary operation is not associative, and there is no identity element.

39. For each binary operation $*$ given below, determine whether or not $*$ defines a group structure on the given set. If not, list the group axioms that fail to hold.

(a) Use matrix multiplication to define $*$ on $\left\{ \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} \middle| x, y \in \mathbf{R} \right\}$.

Answer: The operation is associative, and there is an identity element on the left, but not on the right.

(b) Define $*$ on $\mathbf{R}^2$ by $(x_1, y_1) * (x_2, y_2) = (x_1 x_2, y_1 x_2 + y_2)$.

Answer: The set $\mathbf{R}^2$ is a group under this operation.

Hint: If you don't want to grind out the details, you can try to convert the vectors into 2×2 matrices in such a way that the operation becomes matrix multiplication, and then you don't need to check associativity.

44. Let G be a group, with operation $\cdot$. Define a new operation on G by setting $x * y = y$, for $x, y \in G$. Determine which group axioms hold for this operation.

Answer: This defines an associative binary operation with a left identity element but no right identity element. Since there is no identity, we need not discuss inverses.

3.2 Subgroups

28. In $\mathbf{Z}_n$, show that if $\gcd(a, n) = d$, then $\langle [a]_n \rangle = \langle [d]_n \rangle$.

Note: This result is very useful when you are trying to find cyclic subgroups of $\mathbf{Z}_n$.

Solution: We need to show that $\langle [a]_n \rangle \subseteq \langle [d]_n \rangle$ and $\langle [d]_n \rangle \subseteq \langle [a]_n \rangle$.

First, to show that $\langle [a]_n \rangle \subseteq \langle [d]_n \rangle$, note that $a = dq$ for some $q \in \mathbf{Z}$, since d is a divisor of a. Then $[a]_n = q[d]_n$, which shows that $[a]_n \in \langle [d]_n \rangle$ by applying Proposition 3.2.6 (b).

To show that $\langle [d]_n \rangle \subseteq \langle [a]_n \rangle$, recall that we can write $d = ma + nq$ for some $m, q \in \mathbf{Z}$, since the greatest common divisor of a and n can be written as a linear combination of a and n. Then $d \equiv ma \pmod{n}$, and so $[d]_n = m[a]_n \in \langle [a]_n \rangle$.

29. Find all cyclic subgroups of $\mathbf{Z}_{12}$.

Solution: We need to find $\langle [a] \rangle$ for all congruence classes $[a] \in \mathbf{Z}_{12}$.

$\langle [1] \rangle = \mathbf{Z}_{12}$

$\langle [2] \rangle = \{[0], [2], [4], [6], [8], [10]\}$

$\langle [3] \rangle = \{[0], [3], [6], [9]\}$

$\langle [4] \rangle = \{[0], [4], [8]\}$

$\langle [5] \rangle = \{[0], [5], [10], [3], [8], [1], [6], [11], [4], [9], [2], [7]\}$.

At this point we should have used Problem 28, which guarantees that $\langle [5] \rangle = \langle [1] \rangle = \mathbf{Z}_{12}$ since $\gcd(5, 12) = 1$.

$\langle [6] \rangle = \{[0], [6]\}$

Now, to save time in the calculations, we will use Problem 28. The remaining elements generate subgroups that we have already found. In fact, you can see that the subgroups of $\mathbf{Z}_{12}$ correspond to the divisors of 12.

$\langle [7] \rangle = \langle [1] \rangle = \mathbf{Z}_{12}$ since $\gcd(7, 12) = 1$.

$\langle [8] \rangle = \langle [4] \rangle$ since $\gcd(8, 12) = 4$.

$\langle [9] \rangle = \langle [3] \rangle$ since $\gcd(9, 12) = 3$.

$\langle [10] \rangle = \langle [2] \rangle$ since $\gcd(10, 12) = 2$.

$\langle [11] \rangle = \langle [1] \rangle = \mathbf{Z}_{12}$, since $\gcd(11, 12) = 1$.

30. Find all cyclic subgroups of $\mathbf{Z}_{24}^{\times}$.

Solution: You can check that $x^2 = 1$ for all elements of the group. Thus each nonzero element generates a subgroup of order 2, including just the element itself and the identity element [1].

31. In $\mathbf{Z}_{20}^{\times}$, find two subgroups of order 4, one that is cyclic and one that is not cyclic.

Solution: To find a cyclic subgroup of order 4, we need to check the orders of elements in $\mathbf{Z}_{20}^{\times} = \{\pm[1], \pm[3], \pm[7], \pm[9]\}$. It is natural to begin with [3], which turns out to have order 4, and so $H = \langle [3] \rangle$ is a cyclic subgroup of order 4.

The element $[9] = [3]^2$ has order 2. Since $9^2 \equiv 1 \pmod{20}$, the subset $K = \{\pm[1], \pm[9]\}$ is closed under multiplication. Since H is a finite, nonempty subset of a known group, Corollary 3.2.4 implies that it is a subgroup. Since no element of H has order four, it is not cyclic.

32. (a) Find the cyclic subgroup of S_7 generated by the element $(1, 2, 3)(5, 7)$.

Solution: We have

$((1, 2, 3)(5, 7))^2 = (1, 3, 2)$,

$((1, 2, 3)(5, 7))^3 = (5, 7)$,

$((1, 2, 3)(5, 7))^4 = (1, 2, 3)$,

$((1, 2, 3)(5, 7))^5 = (1, 3, 2)(5, 7)$,

$((1, 2, 3)(5, 7))^6 = (1)$.

These elements, together with $(1, 2, 3)(5, 7)$, form the cyclic subgroup generated by $(1, 2, 3)(5, 7)$.

(b) Find a subgroup of S_7 that contains 12 elements. You do not have to list all of the elements if you can explain why there must be 12, and why they must form a subgroup.

Solution: We only need to find an element of order 12, since it will generate a cyclic subgroup with 12 elements. Since the order of a product of disjoint cycles is the least common multiple of their lengths, the element $(1, 2, 3, 4)(5, 6, 7)$ has order 12.

33. Let G be an abelian group, and let n be a fixed positive integer. Show that

$$N = \{g \in G \mid g = a^n \text{ for some } a \in G\}$$

is a subgroup of G.

Solution: We will use Proposition 3.2.2.

(i) Suppose that g_1 and g_2 belong to N. Then there must exist elements a_1 and a_2 in G with $g_1 = a_1^n$ and $g_2 = a_2^n$, and so $g_1g_2 = a_1^n a_2^n = (a_1a_2)^n$. The last equality holds since G is abelian.

(ii) The identity element e belongs to N since it can always be written in the form $e = e^n$.

(iii) If $g \in N$, with $g = a^n$, then $g^{-1} = (a^n)^{-1} = (a^{-1})^n$, and so g^{-1} has the right form to belong to N.

34. Let K be the following subset of $\mathrm{GL}_2(\mathbf{R})$.

$$K = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbf{R}) \middle| \, d = a, \;\; c = -2b \right\}$$

Show that K is a subgroup of $\mathrm{GL}_2(\mathbf{R})$.

Solution: We will use the compact condition given in Corollary 3.2.3, and so we first note that K is nonempty because it contains the identity matrix. The elements of K have the standard form $\begin{bmatrix} a & b \\ -2b & a \end{bmatrix}$, with nonzero determinant. Given two elements of K, we have the following product, which has a nonzero determinant.

$$\begin{bmatrix} a_1 & b_1 \\ -2b_1 & a_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ -2b_2 & a_2 \end{bmatrix}^{-1} = \begin{bmatrix} a_1 & b_1 \\ -2b_1 & a_1 \end{bmatrix} \frac{1}{a_2^2 + 2b_2^2} \begin{bmatrix} a_2 & -b_2 \\ -2b_2 & a_2 \end{bmatrix}$$

$$= \frac{1}{a_2^2 + 2b_2^2} \begin{bmatrix} a_1a_2 + 2b_1b_2 & -a_1b_2 + b_1a_2 \\ -2b_1a_2 + 2a_1b_2 & 2b_1b_2 + a_1a_2 \end{bmatrix}$$

$$= \frac{1}{a_2^2 + 2b_2^2} \begin{bmatrix} a_1a_2 + 2b_1b_2 & -a_1b_2 + b_1a_2 \\ -2(-a_1b_2 + b_1a_2) & a_1a_2 + 2b_1b_2 \end{bmatrix}$$

The product belongs to K, showing that K is a subgroup of $\mathrm{GL}_2(\mathbf{R})$.

Comment: We've used the form for the inverse of a 2×2 matrix given in Section 3.1.

35. In $G = \mathbf{Z}_{21}^{\times}$, show that $H = \{[x]_{21} \mid x \equiv 1 \pmod 3\}$ and $K = \{[x]_{21} \mid x \equiv 1 \pmod 7\}$ are subgroups of G.

Solution: The subset H is finite and nonempty (it certainly contains [1]), so by Corollary 3.2.4 it is enough to show that H is closed under multiplication. If $[x]$ and $[y]$ belong to H, then $x \equiv 1 \pmod 3$ and $y \equiv 1 \pmod 3$, so it follows that $xy \equiv 1 \pmod 3$, and therefore $[x] \cdot [y] = [xy]$ belongs to H.

A similar argument shows that K is a subgroup of $\mathbf{Z}_{21}^{\times}$.

36. Suppose that p is a prime number of the form $p = 2^n + 1$.

(a) Show that in $\mathbf{Z}_p^\times$ the order of $[2]_p$ is $2n$.

Solution: Since $2^n + 1 = p$, we have $2^n \equiv -1 \pmod{p}$, and squaring this yields $2^{2n} \equiv 1 \pmod{p}$. Thus the order of $[2]$ is a divisor of $2n$, and for any proper divisor k of $2n$ we have $k \leq n$, so $2^k \not\equiv 1 \pmod{p}$ since $2^k - 1 < 2^n + 1 = p$, and hence $2^k - 1$ cannot be divisible by p. This shows that $[2]$ has order $2n$.

(b) Use part (a) to prove that n must be a power of 2.

Solution: The order of $[2]$ is a divisor of $|\mathbf{Z}_p^\times| = p - 1 = 2^n$, so by part (a) this implies that n is a divisor of 2^{n-1}, and therefore n is a power of 2.

Comment: Part (b) gives a group theoretic proof of Exercise 1.2.23 in the text, which states that if $n \in \mathbf{Z}^+$ and $2^n + 1$ is prime, then n is a power of 2.

37. In the multiplicative group $\mathbf{C}^\times$ of complex numbers, find the order of the elements $-\dfrac{\sqrt{2}}{2} + \dfrac{\sqrt{2}}{2}i$ and $-\dfrac{\sqrt{2}}{2} - \dfrac{\sqrt{2}}{2}i$.

Solution: It is probably easiest to change these complex numbers from rectangular coordinates into polar coordinates. Each has magnitude 1, and you can check that $-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i = \cos(3\pi/4) + i\sin(3\pi/4)$ and $-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i = \cos(5\pi/4) + i\sin(5\pi/4)$. Since $8(\frac{3\pi}{4}) = 6\pi$, it follows from DeMoivre's theorem on powers of complex numbers that $(\cos(3\pi/4) + i\sin(3\pi/4))^8 = \cos(6\pi) + i\sin(6\pi) = 1$. Thus $-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ has order 8 in $\mathbf{C}^\times$. A similar argument shows that $-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$ also has order 8.

38. In the group $G = \mathrm{GL}_2(\mathbf{R})$ of invertible 2×2 matrices with real entries, show that

$$H = \left\{ \left[\begin{array}{cc} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{array} \right] \middle| \, \theta \in \mathbf{R} \right\}$$

is a subgroup of G.

Solution: We have $H \subseteq G$ since each element of H has determinant 1.

Closure: To show that H is closed under multiplication we need to use the familiar trig identities for the sine and cosine of the sum of two angles.

$$\left[\begin{array}{cc} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{array} \right] \left[\begin{array}{cc} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{array} \right]$$

$$= \left[\begin{array}{cc} \cos\theta\cos\phi - \sin\theta\sin\phi & -\cos\theta\sin\phi - \sin\theta\cos\phi \\ \sin\theta\cos\phi + \cos\theta\sin\phi & -\sin\theta\sin\phi + \cos\theta\cos\phi \end{array} \right]$$

$$= \left[\begin{array}{cc} \cos\theta\cos\phi - \sin\theta\sin\phi & -(\sin\theta\cos\phi + \cos\theta\sin\phi) \\ \sin\theta\cos\phi + \cos\theta\sin\phi & \cos\theta\cos\phi - \sin\theta\sin\phi \end{array} \right]$$

$$= \left[\begin{array}{cc} \cos(\theta+\phi) & -\sin(\theta+\phi) \\ \sin(\theta+\phi) & \cos(\theta+\phi) \end{array} \right] \in H.$$

Identity: To see that the identity matrix is in the set, let $\theta = 0$.

Existence of inverses: $\left[\begin{array}{cc} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{array} \right]^{-1} = \left[\begin{array}{cc} \cos(-\theta) & -\sin(-\theta) \\ \sin(-\theta) & \cos(-\theta) \end{array} \right] \in H.$

39. Compute the centralizer in $\mathrm{GL}_2(\mathbf{R})$ of the matrix $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$.

Solution: Let $A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$, and suppose that $X = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ belongs to the centralizer of A in $\mathrm{GL}_2(\mathbf{R})$. Then we must have $XA = AX$, so doing this calculation shows that $\begin{bmatrix} 2a+b & a+b \\ 2c+d & c+d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 2a+c & 2b+d \\ a+c & b+d \end{bmatrix}$. Equating corresponding entries shows that we must have $2a + b = 2a + c$, $a + b = 2b + d$, $2c + d = a + c$, and $c + d = b + d$. The first and last equations imply that $b = c$, while the second and third equations imply that $a = b + d = c + d$, or $d = a - b$. On the other hand, any matrix of this form commutes with A, so the centralizer in $\mathrm{GL}_2(\mathbf{R})$ of the matrix $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ is the subgroup $\left\{ \begin{bmatrix} a & b \\ b & a-b \end{bmatrix} \middle| a, b \in \mathbf{R} \text{ and } ab \neq a^2 - b^2 \right\}$.

40. Prove that any infinite group has infinitely many subgroups.

Solution: First note that if a has infinite order, then $\langle a \rangle$ has infinitely many subgroups, one for each positive integer n, namely $\langle a^n \rangle$. Suppose that G has only finitely many subgroups. Then it certainly has only finitely many cyclic subgroups. Each element of G generates a finite cyclic subgroup, so G is contained in the union of a finite number of finite sets, and therefore it must be finite.

ANSWERS AND HINTS

41. Let G be a group, and let $a \in G$, with $a \neq e$. Prove or disprove these statements.
(a) The element a has order 2 if and only if $a^2 = e$.
(b) The element a has order 3 if and only if $a^3 = e$.
(c) The element a has order 4 if and only if $a^4 = e$.
Hint: Statements (a) and (b) are true, but (c) is false.

43. Is $\{(x, y) \in \mathbf{R}^2 \mid y = x^2\}$ a subgroup of $\mathbf{R}^2$?
Answer: No, since the closure property does not hold.

44. Is $\{(x, y) \in \mathbf{R}^2 \mid x, y \in \mathbf{Z}\}$ a subgroup of $\mathbf{R}^2$?
Answer: Yes.

51. Let G be a group, with a subgroup $H \subseteq G$. Define $N(H) = \{g \in G \mid gHg^{-1} = H\}$. Show that $N(H)$ is a subgroup of G that contains H.
Hint: To show that $N(H)$ is closed under formation of inverses, you must show that $gHg^{-1} = H$ implies $g^{-1}Hg = H$.

53. In each of the groups O, P, Q in the tables in Section 3.1 of the *Study Guide*, find the centralizers $C(a)$ and $C(ab)$.
Answer: The group O is abelian, so $C(a) = O$ and $C(ab) = O$. In both groups P and Q, we have $C(a) = \langle a \rangle$ and $C(ab) = \{e, ab, a^2, a^3b\}$.

58. (a) Characterize the elements of $\mathrm{GL}_2(\mathbf{R})$ that have order 2.
Answer: Case 1: If $\det(A) = 1$, then $A = \pm I_2$.
Case 2: If $\det(A) = -1$, then $A = \begin{bmatrix} a & b \\ c & -a \end{bmatrix}$, with $a^2 + bc = 1$.
(b) Which of the elements in part (a) are upper triangular?
Answer: $\pm I_2$ and matrices of the form $\begin{bmatrix} 1 & b \\ 0 & -1 \end{bmatrix}$ or $\begin{bmatrix} -1 & b \\ 0 & 1 \end{bmatrix}$
(c) Is $\{A \in \mathrm{GL}_2(\mathbf{R}) \mid A^2 = I\}$ a subgroup of $\mathrm{GL}_2(\mathbf{R})$?
(d) Does the set of upper triangular matrices in $\{A \in \mathrm{GL}_2(\mathbf{R}) \mid A^2 = I\}$ form a subgroup of $\mathrm{GL}_2(\mathbf{R})$?
Answer: The answer to both (c) and (d) is no.

59. (a) Characterize the elements of order 3 in $\mathrm{GL}_2(\mathbf{R})$ that have the form $\begin{bmatrix} a & b \\ c & 0 \end{bmatrix}$.
Show that there are infinitely many such elements.
Answer: These elements have the form $\begin{bmatrix} -1 & b \\ -\frac{1}{b} & 0 \end{bmatrix}$, for any nonzero $b \in \mathbf{R}$.

61. In $\mathrm{GL}_2(\mathbf{R})$, let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, which has infinite order, and let $B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Find the order of B, and find the order of AB.
Answer: B has order 4, and AB has order 3.

64. (a) Find the cyclic subgroup of S_6 generated by the element $(1, 2, 3)(4, 5, 6)$.
(b) Find the smallest subgroup of S_6 that contains $(1, 2, 3)$ and $(4, 5, 6)$.
Answer: The subgroup in part (a) has order 3; the one in part (b) has order 9.

3.3 Constructing Examples

From this point on, if the modulus n is fixed throughout the problem, we will write a rather than $[a]_n$ for elements of $\mathbf{Z}_n$.

19. Show that $\mathbf{Z}_5 \times \mathbf{Z}_3$ is a cyclic group, and list all of the generators of the group.

Solution: By Proposition 3.3.4 (b), the order of an element $([a]_5, [b]_3)$ in $\mathbf{Z}_5 \times \mathbf{Z}_3$ is the least common multiple of the orders of the components. Since $[1]_5, [2]_5, [3]_5, [4]_5$ have order 5 in $\mathbf{Z}_5$ and $[1]_3, [2]_3$ have order 3 in $\mathbf{Z}_3$, the element $([a]_5, [b]_3)$ is a generator if and only if $[a]_5 \neq [0]_5$ and $[b]_3 \neq [0]_3$. There are 8 such elements, which can easily be listed.

Comment: The other 7 elements in the group will have at least one component equal to zero. There are 4 elements of order 5 (with $[0]_3$ as the second component) and 2 elements of order 3 (with $[0]_5$ as the first component). Adding the identity element to the list accounts for all 15 elements of $\mathbf{Z}_5 \times \mathbf{Z}_3$.

20. Find the order of the element $([9]_{12}, [15]_{18})$ in the group $\mathbf{Z}_{12} \times \mathbf{Z}_{18}$.

Solution: Since $\gcd(9, 12) = 3$, we have $o([9]_{12}) = o([3]_{12}) = 4$. Similarly, $o([15]_{18}) = o([3]_{18}) = 6$. Thus the order of $([9]_{12}, [15]_{18})$ is $\mathrm{lcm}[4, 6] = 12$.

21. Find two groups G_1 and G_2 whose direct product $G_1 \times G_2$ has a subgroup that is not of the form $H_1 \times H_2$, for subgroups $H_1 \subseteq G_1$ and $H_2 \subseteq G_2$.

Solution: In $\mathbf{Z}_2 \times \mathbf{Z}_2$, the element $(1,1)$ has order 2, so it generates a cyclic subgroup that does not have the required form.

22. In the group $G = \mathbf{Z}_{36}^{\times}$, let $H = \{[x] \mid x \equiv 1 \pmod 4\}$ and $K = \{[y] \mid y \equiv 1 \pmod 9\}$. Show that H and K are subgroups of G, and find the subgroup HK.

Solution: It can be shown (as in Problem 3.2.35) that the given subsets are subgroups. A short computation shows that $H = \{1, 5, 13, 17, 25, 29\}$ and $K = \{1, 19\}$. Since $x \cdot 1 \neq x \cdot 19$ for $x \in G$, the set HK must contain 12 elements, and so $HK = G$ since $G = \mathbf{Z}_{36}^{\times}$ has $\varphi(36) = 36 \cdot \frac{1}{2} \cdot \frac{2}{3} = 12$ elements.

23. Let F be a field, and let H be the subset of $\mathrm{GL}_2(F)$ consisting of all invertible upper triangular matrices. Show that H is a subgroup of $\mathrm{GL}_2(F)$.

Solution: Since $\begin{bmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} \\ 0 & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} + a_{12}b_{22} \\ 0 & a_{22}b_{22} \end{bmatrix}$, and $a_{11}a_{22} \neq 0$ and $b_{11}b_{22} \neq 0$ together imply that $(a_{11}b_{11})(a_{22}b_{22}) \neq 0$, it follows that H is closed under multiplication. It is also closed under formation of inverses, since $\begin{bmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{bmatrix}^{-1} = \begin{bmatrix} a_{11}^{-1} & -a_{11}^{-1}a_{12}a_{22}^{-1} \\ 0 & a_{22}^{-1} \end{bmatrix}$. The identity matrix is certainly in H.

Comment: This comment is directed to the readers who remember some linear algebra. We will prove a more general result.

Proposition: For a field F, the set H of upper triangular matrices in $\mathrm{GL}_n(F)$ is a subgroup of $\mathrm{GL}_n(F)$.

Proof: Of course, the identity matrix is upper triangular, so it belongs to H.

Suppose that $A = [a_{ij}]$ and $B = [b_{ij}]$ belong to H. This condition is expressed by that fact that $a_{ij} = 0$ if $i > j$ and $b_{ij} = 0$ if $i > j$. The entries of the product matrix $[c_{ij}] = [a_{ij}][b_{ij}]$ are given by the formula $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$. Now look at c_{ij} when $i > j$. Since $a_{ik} = 0$ for all $k < i$ and $b_{kj} = 0$ for all $k > j$, we must have $a_{ik}b_{kj} = 0$ for all $1 \leq k \leq n$ because $i > j$. This argument shows that the set of upper triangular matrices in $\mathrm{GL}_n(F)$ is closed under multiplication.

Finally, we need to show that the inverse of an upper triangular matrix is again upper triangular. Recall that $A^{-1} = \dfrac{1}{\det(A)} \operatorname{adj}(A)$, where $\operatorname{adj}(A)$ is the adjoint of A, and that $\operatorname{adj}(A)$ is the transpose of the matrix of cofactors of A. It can then be checked that the adjoint of an upper triangular matrix is again upper triangular.

Second proof: We will use induction (which doesn't require using the adjoint). If an invertible matrix has the block form $\begin{bmatrix} A & B \\ 0 & C \end{bmatrix}$, then A and C must be invertible matrices, and a direct calculation shows that $\begin{bmatrix} A & B \\ 0 & C \end{bmatrix}^{-1} = \begin{bmatrix} A^{-1} & -A^{-1}BC^{-1} \\ 0 & C^{-1} \end{bmatrix}$. The induction begins with the 2×2 case proved above. Now suppose that $[a_{ij}]$ is

an $n \times n$ upper triangular matrix. We can write $[a_{ij}] = \begin{bmatrix} A & X \\ 0 & a_{nn} \end{bmatrix}$, where A is an $(n-1) \times (n-1)$ upper triangular matrix, and X is an $(n-1) \times 1$ column. Given the induction hypothesis that the inverse of an $(n-1) \times (n-1)$ upper triangular matrix is again upper triangular, it is clear that $[a_{ij}]^{-1} = \begin{bmatrix} A^{-1} & -A^{-1}Xa_{nn}^{-1} \\ 0 & a_{nn}^{-1} \end{bmatrix}$ is also upper triangular.

24. Let p be a prime number.

(a) Show that the order of the general linear group $\mathrm{GL}_2(\mathbf{Z}_p)$ is $(p^2-1)(p^2-p)$.

Hint: Count the number of ways to construct two linearly independent rows.

Solution: We need to count the number of ways in which an invertible 2×2 matrix can be constructed with entries in $\mathbf{Z}_p$. This is done by noting that we need 2 linearly independent rows. The first row can be any nonzero vector, so there are p^2-1 choices.

There are p^2 possibilities for the second row, but to be linearly independent of the first row, it cannot be a scalar multiple of that row. Since we have p possible scalars, we need to omit the p multiples of the first row. Therefore the total number of ways to construct a second row independent of the first is $p^2 - p$.

(b) Show that the subgroup of $\mathrm{GL}_2(\mathbf{Z}_p)$ consisting of all invertible upper triangular matrices has order $(p-1)^2 p$.

Solution: An upper triangular 2×2 matrix has nonzero determinant if and only if the elements on the main diagonal are nonzero. There are $(p-1)^2$ choices for these entries. Since the third entry can be any element of $\mathbf{Z}_p$, there are p choices for this entry.

25. Find the order of the element $A = \begin{bmatrix} i & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -i \end{bmatrix}$ in the group $\mathrm{GL}_3(\mathbf{C})$.

Solution: For any diagonal 3×3 matrix we have

$$\begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix}^n = \begin{bmatrix} a^n & 0 & 0 \\ 0 & b^n & 0 \\ 0 & 0 & c^n \end{bmatrix},$$

It follows immediately that the order of A is the least common multiple of the orders of the diagonal entries i, -1, and $-i$. Thus $o(A) = 4$.

26. Let G be the subgroup of $\mathrm{GL}_2(\mathbf{R})$ defined by

$$G = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| \, m \neq 0 \right\}.$$

Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$. Find the centralizers $C(A)$ and $C(B)$, and show that $C(A) \cap C(B) = Z(G)$, where $Z(G)$ is the center of G.

Solution: Suppose that $X = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$ belongs to $C(A)$ in G. Then we must have $XA = AX$, and doing this calculation shows that

$$\begin{bmatrix} m & m+b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} m & b+1 \\ 0 & 1 \end{bmatrix}.$$

Equating corresponding entries shows that we must have $m+b = b+1$, and so $m = 1$. On the other hand, any matrix of this form commutes with A, and so

$$C(A) = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \middle| b \in \mathbf{R} \right\}.$$

Now suppose that $X = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$ belongs to $C(B)$. Then $XB = BX$, and so

$$\begin{bmatrix} -m & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -m & -b \\ 0 & 1 \end{bmatrix}.$$

Equating corresponding entries shows that we must have $b = 0$, and so

$$C(B) = \left\{ \begin{bmatrix} m & 0 \\ 0 & 1 \end{bmatrix} \middle| 0 \neq m \in \mathbf{R} \right\}.$$

This shows that $C(A) \cap C(B)$ is the identity matrix, and since any element in the center of G must belong to $C(A) \cap C(B)$, our calculations show that the center of G is the trivial subgroup, containing only the identity element.

27. Compute the centralizer in $\mathrm{GL}_2(\mathbf{Z}_3)$ of the matrix $\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$.

Solution: Let $A = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$, and suppose that $X = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ belongs to the centralizer of A in $\mathrm{GL}_2(\mathbf{Z}_3)$. Then $XA = AX$, and so $\begin{bmatrix} a & -a+b \\ c & -c+d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a-c & b-d \\ c & d \end{bmatrix}$. Equating corresponding entries shows that we must have $a = a - c$, $-a + b = b - d$, and $-c + d = d$. The first equation implies that $c = 0$, while the second equation implies that $a = d$. It follows that the centralizer in $\mathrm{GL}_2(\mathbf{Z}_3)$ of the matrix $\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$ is the subgroup $H = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \middle| a, b \in \mathbf{Z}_3 \text{ and } a \neq 0 \right\}$. Note that the modulus 3 has played no role here.

Comment: The centralizer contains 6 elements, while it follows from Problem 24 that $\mathrm{GL}_2(\mathbf{Z}_3)$ has $(3^2-1)(3^2-3) = 48$ elements. $H = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, a = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, a^2 = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, b = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, ab = \begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix}, a^2b = \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix} \right\}$

Note that the multiplication table for H will look like that of S_3, since it has order 6 and is not abelian ($ab \neq ba$). (See Exercises 15-16 in the text.)

28. Compute the centralizer in $\mathrm{GL}_2(\mathbf{Z}_3)$ of the matrix $\begin{bmatrix} 1 & -1 \\ -1 & 0 \end{bmatrix}$.

Solution: Let $A = \begin{bmatrix} 1 & -1 \\ -1 & 0 \end{bmatrix}$, and suppose that $X = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ belongs to the centralizer of A in $\mathrm{GL}_2(\mathbf{Z}_3)$. Then $XA = AX$, and so $\begin{bmatrix} a-b & -a \\ c-d & -c \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & -1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a-c & b-d \\ -a & -b \end{bmatrix}$. Equating corresponding entries shows that we must have $a-b = a-c$, $-a = b-d$, $c-d = -a$, and $-c = -b$. The first equation implies that $c = b$, while the second equation implies that $d = a+b$. It follows that the centralizer in $\mathrm{GL}_2(\mathbf{Z}_3)$ of the matrix $\begin{bmatrix} 1 & -1 \\ -1 & 0 \end{bmatrix}$ is the subgroup $\left\{ \begin{bmatrix} a & b \\ b & a+b \end{bmatrix} \middle| a, b \in \mathbf{Z}_3 \text{ and } a \neq 0 \text{ or } b \neq 0 \right\}$.

Comment: In this case the centralizer contains 8 of the 48 elements in $\mathrm{GL}_2(\mathbf{Z}_3)$. $H = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ -1 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix} \right\}$ Note that H is cyclic, as given above.

29. Let H be the following subset of the group $G = \mathrm{GL}_2(\mathbf{Z}_5)$.

$$H = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \in \mathrm{GL}_2(\mathbf{Z}_5) \middle| m, b \in \mathbf{Z}_5,\ m = \pm 1 \right\}$$

(a) Show that H is a subgroup of G with 10 elements.

Solution: Since in the matrix $\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$ there are two choices for m and 5 choices for b, we will have a total of 10 elements. The set is closed under multiplication since $\begin{bmatrix} \pm 1 & b \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \pm 1 & c \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \pm 1 & b \pm c \\ 0 & 1 \end{bmatrix}$, and it is certainly nonempty, and so it is a subgroup since the group is finite.

(b) Show that if we let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$, then $BA = A^{-1}B$.

Solution: We have $BA = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}$ and

$A^{-1}B = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}$.

(c) Show that every element of H can be written uniquely in the form A^iB^j, where $0 \leq i < 5$ and $0 \leq j < 2$.

Solution: Since $\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b+c \\ 0 & 1 \end{bmatrix}$, the cyclic subgroup generated by A consists of all matrices of the form $\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$. Multiplying on the right by B will create 5 additional elements, giving all of the elements in H.

30. Let H and K be subgroups of the group G. Prove that HK is a subgroup of G if and only if $KH \subseteq HK$.

Note: This result strengthens Proposition 3.3.2.

Solution: First assume that HK is a subgroup of G. If $k \in K$ and $h \in H$, then we have $k = ek \in HK$ and $h = he \in HK$, so the product kh must belong to HK. This shows that $KH \subseteq HK$.

Conversely, suppose that $KH \subseteq HK$. It is clear that $e = ee \in HK$ since H and K are subgroups. To show closure, let $g_1, g_2 \in HK$. Then there exist elements $h_1, h_2 \in H$ and $k_1, k_2 \in K$ with $g_1 = h_1k_1$ and $g_2 = h_2k_2$. Since $k_1h_2 \in KH$, by assumption there exist $k_1' \in K$ and $h_2' \in H$ with $k_1h_2 = h_2'k_1'$. Thus $g_1g_2 = h_1k_1h_2k_2 = h_1h_2'k_1'k_2 \in HK$ since both H and K are closed under multiplication. Finally, $(g_1)^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in HK$ since $k_1^{-1} \in K$ and $h_1^{-1} \in H$ and $KH \subseteq HK$.

ANSWERS AND HINTS

31. What is the order of $([15]_{24}, [25]_{30})$ in the group $\mathbf{Z}_{24} \times \mathbf{Z}_{30}$? What is the largest possible order of an element in $\mathbf{Z}_{24} \times \mathbf{Z}_{30}$?
Answer: The element $([15]_{24}, [25]_{30})$ has order $\text{lcm}[8, 6] = 24$. The largest possible order of an element in $\mathbf{Z}_{24} \times \mathbf{Z}_{30}$ is $\text{lcm}[24, 30] = 120$,

32. Find the order of each element of the group $\mathbf{Z}_4 \times \mathbf{Z}_4^\times$.
Answer: $(0, 1)$ has order one; $(2, 1), (0, 2), (2, 2)$ have order two; the remaining 4 elements have order four.

33. Check the order of each element of the quaternion group in Example 3.3.7 by using the matrix form of the element.
Answer: Order 2: $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ Order 4: $\pm\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \pm\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \pm\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$

35. Let $G = \mathbf{Z}_{10}^\times \times \mathbf{Z}_{10}^\times$.
(a) If $H = \langle(3, 3)\rangle$ and $K = \langle(3, 7)\rangle$, list the elements of HK.
Answer: $HK = \{(1, 1), (3, 3), (9, 9), (7, 7), (3, 7), (9, 1), (7, 3), (1, 9)\}$
(b) If $H = \langle(3, 3)\rangle$ and $K = \langle(1, 3)\rangle$, list the elements of HK.
Answer: $HK = G$.

37. In $G = \mathbf{Z}_{15}^\times$, find subgroups H and K with $|H| = 4$, $|K| = 2$, $HK = G$, and $H \cap K = \{1\}$.
Answer: Answer: Let $H = \langle 2\rangle$ and $K = \langle -1\rangle$.

41. Find the orders of $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ and $\begin{bmatrix} 1 & 2 \\ 4 & 3 \end{bmatrix}$ in $\text{GL}_2(\mathbf{Z}_5)$.
Answer: The first matrix has order 8; the second matrix is not in $\text{GL}_2(\mathbf{Z}_5)$.

42. Let $K = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \in \text{GL}_2(\mathbf{Z}_5) \middle| m, b \in \mathbf{Z}_5,\ m \neq 0 \right\}$.
(b) Show, by finding the order of each element in K, that K has elements of order 2 and 5, but no element of order 10.

Answer: The 4 elements of the form $\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$, with $b \neq 0$, each have order 5; the 5 elements $\begin{bmatrix} 4 & b \\ 0 & 1 \end{bmatrix}$ each have order 2; the 10 elements $\begin{bmatrix} 2 & b \\ 0 & 1 \end{bmatrix}$ or $\begin{bmatrix} 3 & b \\ 0 & 1 \end{bmatrix}$ each have order 4.

45. Find the cyclic subgroup of $\mathrm{GL}_4(\mathbf{Z}_2)$ generated by $\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$.

Answer: $\left\langle \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \right\}$

47. List the orthogonal matrices in $\mathrm{GL}_2(\mathbf{Z}_3)$ and find the order of each one.

Answer: Case 1: $\pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ have determinant 1.

Case 2: $\pm \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \pm \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ have determinant -1.

The symmetric orthogonal matrices have order 2 (except for I_2), and the remaining two matrices have order 4.

3.4 Isomorphisms

29. Show that $\mathbf{Z}_{17}^{\times}$ is isomorphic to $\mathbf{Z}_{16}$.

Comment: The introduction to Section 3.2 in the *Study Guide* shows that the element $[3]_{17}$ is a generator for $\mathbf{Z}_{17}^{\times}$. This provides the clue as to how to define the isomorphism we need, since $\mathbf{Z}_{16}$ is also a cyclic group (with generator $[1]_{16}$), and Proposition 3.4.3 (a) implies that any isomorphism between cyclic groups must map a generator to a generator.

Solution: Define $\phi : \mathbf{Z}_{16} \to \mathbf{Z}_{17}^{\times}$ by setting $\phi([1]_{16}) = [3]_{17}$, $\phi([2]_{16}) = [3]_{17}^2$, etc. The general formula is $\phi([n]_{16}) = [3]_{17}^n$, for all $[n]_{16} \in \mathbf{Z}_{16}$. Since ϕ is defined by using a representative n of the equivalence class $[n]_{16}$, we have to show that the formula for ϕ does not depend on the particular representative that is chosen. If $k \equiv m \pmod{16}$, then it follows from Proposition 3.2.8 (c) that $[3]_{17}^k = [3]_{17}^m$ since $[3]_{17}$ has order 16 in $\mathbf{Z}_{17}^{\times}$. Therefore $\phi([k]_{16}) = \phi([m]_{16})$, and so ϕ *is* a well-defined function.

Proposition 3.2.8 (c) shows that $\phi([k]_{16}) = \phi([m]_{16})$ only if $k \equiv m \pmod{16}$, and so ϕ is a one-to-one function. Then because both $\mathbf{Z}_{16}$ and $\mathbf{Z}_{17}^{\times}$ have 16 elements, it follows from Proposition 2.1.8 that ϕ is also an onto function. For any elements $[n]_{16}$ and

$[m]_{16}$ in $\mathbf{Z}_{16}$, we first compute what happens if we combine $[n]_{16}$ and $[m]_{16}$ using the operation in $\mathbf{Z}_{16}$, and then substitute the result into the function ϕ:

$$\phi([n]_{16} + [m]_{16}) = \phi([n+m]_{16}) = [3]_{17}^{n+m} .$$

Next, we first apply the function ϕ to the two elements, $[n]_{16}$ and $[m]_{16}$, and then combine the results using the operation in $\mathbf{Z}_{17}^{\times}$:

$$\phi([n]_{16}) \cdot \phi([m]_{16}) = [3]_{17}^{n}[3]_{17}^{m} = [3]_{17}^{n+m} .$$

Thus $\phi([n]_{16} + [m]_{16}) = \phi([n]_{16}) \cdot \phi([m]_{16})$, and this completes the proof that ϕ is a group isomorphism.

30. Is $\mathbf{Z}_{16}^{\times}$ isomorphic to $\mathbf{Z}_4 \times \mathbf{Z}_2$?

Comment: The positive integers less than 16 and relatively prime to 16 are 1, 3, 5, 7, 9, 11, 13, 15, so we can write $\mathbf{Z}_{16}^{\times} = \{\pm 1, \pm 3, \pm 5, \pm 7\}$. Since $\mathbf{Z}_4 \times \mathbf{Z}_2$ also has 8 elements, we can't eliminate the possibility of an isomorphism just by using a counting argument.

We might next check to see if the two groups have the same number of elements having the same orders. In the multiplicative group $\mathbf{Z}_{16}^{\times}$, easy calculations show that -1, 7, and -7 have order 2, while ± 3 and ± 5 all have order 4. In the additive group $\mathbf{Z}_4 \times \mathbf{Z}_2$, the elements $(2,0)$, $(2,1)$, and $(0,1)$ have order 2, while $(1,0)$, $(1,1)$, $(3,0)$, and $(3,1)$ have order 4. Again, we can't eliminate the possibility of an isomorphism. But now we *do* have some idea of what a correspondence might look like.

Let's focus on the elements $(1,0)$ and $(0,1)$ in $\mathbf{Z}_4 \times \mathbf{Z}_2$. We need an element of order 4 in $\mathbf{Z}_{16}^{\times}$ to correspond to $(1,0)$, so we might choose 3 as a possibility. The powers of 3 are $1, 3, 9, 11$, or $\langle 3 \rangle = \{1, 3, -7, -5\}$. Since the elements of $\mathbf{Z}_4 \times \mathbf{Z}_2$ are formed by adding $(0,1)$ to the multiples of $(1,0)$, we need to look for an element that can be multiplied by the elements of $\langle 3 \rangle$ to give $\mathbf{Z}_{16}^{\times}$. An easy choice is -1. Now we are ready to use an "exponential" function to actually provide the isomorphism. In the solution we will be more formal, and keep track of the moduli in the domain and codomain of the isomorphism.

Solution: Define $\phi : \mathbf{Z}_4 \times \mathbf{Z}_2 \to \mathbf{Z}_{16}^{\times}$ by setting $\phi(([n]_4, [m]_2)) = [3]_{16}^{n}[-1]_{16}^{m}$. You can quickly check that the function is well-defined since $[3]_{16}$ has order 4 and $[-1]_{16}$ has order 2. Taking $n = 0, 1, 2, 3$ and $m = 0$ and then $n = 0, 1, 2, 3$ and $m = 1$ gives us the elements $[1]_{16}$, $[3]_{16}$, $[-7]_{16}$, $[-5]_{16}$, $[-1]_{16}$, $[-3]_{16}$, $[7]_{16}$, $[5]_{16}$, respectively, and shows that ϕ is one-to-one and onto. Finally, ϕ is an isomorphism because

$$\phi(([n_1]_4, [m_1]_2) + ([n_2]_4, [m_2]_2)) = \phi(([n_1 + n_2]_4, [m_1 + m_2]_2)) = [3]_{16}^{n_1+n_2}[-1]_{16}^{m_1+m_2}$$

$$\phi(([n_1]_4, [m_1]_2))\phi(([n_2]_4, [m_2]_2)) = [3]_{16}^{n_1}[-1]_{16}^{m_1}[3]_{16}^{n_2}[-1]_{16}^{m_2} = [3]_{16}^{n_1+n_2}[-1]_{16}^{m_1+m_2}.$$

31. Prove that $\mathbf{Z}_{24}^{\times}$ is not isomorphic to $\mathbf{Z}_{16}^{\times}$.

Solution: First note that $|\mathbf{Z}_{24}^{\times}| = |\mathbf{Z}_{16}^{\times}| = 8$, so we cannot rule out the existence of an isomorphism on the grounds of size alone. Exercise 3.4.21 in the text shows that $\mathbf{Z}_{24}^{\times}$ is isomorphic to $\mathbf{Z}_8^{\times} \times \mathbf{Z}_3^{\times}$. (This can be proved using the function defined in

Proposition 3.4.5.) We have seen that every nontrivial element of $\mathbf{Z}_8^\times$ has order 2, as does every nontrivial element of $\mathbf{Z}_3^\times$. It follows from Proposition 3.3.4 (b) that every nontrivial element of $\mathbf{Z}_{24}^\times$ has order 2. Problem 30 shows that $\mathbf{Z}_{16}^\times$ has elements of order 4, and so the two groups cannot be isomorphic by Proposition 3.4.3 (a).

32. Let $\phi : \mathbf{R}^\times \to \mathbf{R}^\times$ be defined by $\phi(x) = x^3$, for all $x \in \mathbf{R}$. Show that ϕ is a group isomorphism.

Solution: The function ϕ preserves multiplication in $\mathbf{R}^\times$ since for all $a, b \in \mathbf{R}^\times$ we have $\phi(ab) = (ab)^3 = a^3b^3 = \phi(a)\phi(b)$. The function is one-to-one and onto since for each $y \in \mathbf{R}^\times$ the equation $\phi(x) = y$ has the unique solution $x = \sqrt[3]{y}$.

33. Let G_1, G_2, H_1, H_2 be groups, and suppose that $\theta_1 : G_1 \to H_1$ and $\theta_2 : G_2 \to H_2$ are group isomorphisms. Define $\phi : G_1 \times G_2 \to H_1 \times H_2$ by $\phi(x_1, x_2) = (\theta_1(x_1), \theta_2(x_2))$, for all $(x_1, x_2) \in G_1 \times G_2$. Prove that ϕ is a group isomorphism.

Solution: If $(y_1, y_2) \in H_1 \times H_2$, then since θ_1 is an isomorphism there is a unique element $x_1 \in G_1$ with $y_1 = \theta_1(x_1)$. Similarly, since θ_2 is an isomorphism there is a unique element $x_2 \in G_2$ with $y_2 = \theta_2(x_2)$. Thus there is a unique element $(x_1, x_2) \in G_1 \times G_2$ such that $(y_1, y_2) = \phi(x_1, x_2)$, and so ϕ is one-to-one and onto.

Given (a_1, a_2) and (b_1, b_2) in $G_1 \times G_2$, we have

$$\begin{aligned} \phi((a_1, a_2) \cdot (b_1, b_2)) &= \phi((a_1b_1, a_2b_2)) = (\theta_1(a_1b_1), \theta_2(a_2b_2)) \\ &= (\theta_1(a_1)\theta_1(b_1), \theta_2(a_2)\theta_2(b_2)) \end{aligned}$$

$$\begin{aligned} \phi((a_1, a_2)) \cdot \phi((b_1, b_2)) &= (\theta_1(a_1), \theta_2(a_2)) \cdot (\theta_1(b_1), \theta_2(b_2)) \\ &= (\theta_1(a_1)\theta_1(b_1), \theta_2(a_2)\theta_2(b_2)) \end{aligned}$$

and so $\phi : G_1 \times G_2 \to H_1 \times H_2$ is a group isomorphism.

34. Prove that the group $\mathbf{Z}_7^\times \times \mathbf{Z}_{11}^\times$ is isomorphic to the group $\mathbf{Z}_6 \times \mathbf{Z}_{10}$.

Solution: You can check that $\mathbf{Z}_7^\times$ is cyclic of order 6, generated by $[3]_7$, and that $\mathbf{Z}_{11}^\times$ is cyclic of order 10, generated by $[2]_{11}$. Just as in Problem 29, you can show that $\theta_1 : \mathbf{Z}_6 \to \mathbf{Z}_7^\times$ defined by $\theta_1([n]_6) = [3]_7^n$ and $\theta_2 : \mathbf{Z}_{10} \to \mathbf{Z}_{11}^\times$ defined by $\theta_2([m]_{10}) = [2]_{11}^m$ are group isomorphisms. It then follows from Problem 33 that $\phi : \mathbf{Z}_6 \times \mathbf{Z}_{10} \to \mathbf{Z}_7^\times \times \mathbf{Z}_{11}^\times$ defined by $\phi(([n]_6, [m]_{10})) = ([3]_7^n, [2]_{11}^m)$, for all $[n]_6 \in \mathbf{Z}_6$ and all $[m]_{10} \in \mathbf{Z}_{10}$, is a group isomorphism.

35. Define $\phi : \mathbf{Z}_{30} \times \mathbf{Z}_2 \to \mathbf{Z}_{10} \times \mathbf{Z}_6$ by $\phi([n]_{30}, [m]_2) = ([n]_{10}, [4n + 3m]_6)$, First prove that ϕ is a well-defined function, and then prove that ϕ is a group isomorphism.

Solution: If $([n]_{30}, [m]_2)$ and $([k]_{30}, [j]_2)$ are equal elements of $\mathbf{Z}_{30} \times \mathbf{Z}_2$, then $30 \mid n-k$ and $2 \mid m-j$. It follows that $10 \mid n-k$, and so $[n]_{10} = [k]_{10}$. Furthermore, $30 \mid 4(n-k)$, so $6 \mid 4(n-k)$, and then $6 \mid 3(m-j)$, which together imply that $6 \mid (4n+3m)-(4k+3j)$, showing that $[4n + 3m]_6 = [4k + 3j]_6$. Thus $([n]_{10}, [4n + 3m]_6) = ([k]_{10}, [4k + 3j]_6)$, which shows that the formula for ϕ *does* yield a well-defined function.

For any elements $([a]_{30}, [c]_2)$ and $([b]_{30}, [d]_2)$ we have

$$\begin{aligned}\phi(([a]_{30}, [c]_2) + ([b]_{30}, [d]_2)) &= \phi(([a+b]_{30}, [c+d]_2)) \\ &= ([a+b]_{10}, [4(a+b)+3(c+d)]_2) \\ &= ([a+b]_{10}, [4a+4b+3c+3d]_2)\end{aligned}$$

$$\begin{aligned}\phi(([a]_{30}, [c]_2)) + \phi(([b]_{30}, [d]_2)) &= ([a]_{10}, [4a+3c]_2) + ([b]_{10}, [4b+3d]_2) \\ &= ([a+b]_{10}, [4a+3c+4b+3d]_2) \\ &= ([a+b]_{10}, [4a+4b+3c+3d]_2)\end{aligned}$$

and so ϕ respects the operations in the two groups.

To show that ϕ is one-to-one, suppose that $\phi([n]_{30}, [m]_2) = \phi([r]_{30}, [s]_2)$. Then $([n]_{10}, [4n+3m]_6) = ([r]_{10}, [4r+3s]_6)$, so $10 \mid (n-r)$ and $6 \mid (4(n-r)+3(m-s)$. Then $2 \mid 4(n-r)$, so we must have $2 \mid 3(m-s)$, which implies that $2 \mid (m-s)$ and therefore $[m]_2 = [s]_2$. Furthermore, $3 \mid 3(m-s)$ implies that $3 \mid 4(n-r)$, and therefore $3 \mid (n-r)$. Since $\gcd(10, 3) = 1$, we obtain $30 \mid (n-r)$, and so $[n]_{30} = [r]_{30}$. We conclude that ϕ is a one-to-one function.

Since the groups both have 60 elements, it follows that ϕ must also be an onto function. We have therefore checked all of the necessary conditions, so we can conclude that ϕ is a group isomorphism.

Comment: We can use Proposition 3.4.4 to give a different proof that ϕ is one-to-one. If $\phi([n]_{30}, [m]_2) = ([0]_{10}, [0]_6)$, then $([n]_{10}, [4n+3m]_6) = ([0]_{10}, [0]_6)$, so $10 \mid n$, say $n = 10q$, for some $q \in \mathbf{Z}$, and $6 \mid (4n+3m)$, or $6 \mid (40q+3m)$. It follows that $2 \mid (40q+3m)$ and $3 \mid (40q+3m)$, and therefore $2 \mid 3m$ since $2 \mid 40q$, and $3 \mid 40q$ since $3 \mid 3m$. Then since 2 and 3 are prime numbers, it follows that $2 \mid m$, so $[m]_2 = [0]_2$, and $3 \mid q$, so $[n]_{30} = [10q]_{30} = [0]_{30}$. We have now shown that if $\phi([n]_{30}, [m]_2) = ([0]_{10}, [0]_6)$, then $([n]_{30}, [m]_2) = ([0]_{30}, [0]_2)$, and so the condition in Proposition 3.4.4 is satisfied.

36. Let G be a group, and let H be a subgroup of G. Prove that if a is any element of G, then the subset

$$aHa^{-1} = \{g \in G \mid g = aha^{-1} \text{ for some } h \in H\}$$

is a subgroup of G that is isomorphic to H.

Solution: By Exercise 3.4.15 in the text, the function $\phi : G \to G$ defined by $\phi(x) = axa^{-1}$, for all $x \in G$, is a group isomorphism. By Exercise 3.4.17 the image under ϕ of any subgroup of G is again a subgroup of G, so $aHa^{-1} = \phi(H)$ is a subgroup of G. It is then clear that the function $\theta : H \to aHa^{-1}$ defined by $\theta(x) = axa^{-1}$ is an isomorphism.

Comment: The solution to Problem 3.2.50 shows directly that aHa^{-1} is a subgroup, but the above proof is much more conceptual in nature.

37. Let G, G_1, G_2 be groups. Prove that if $G_1 \times G_2$ is isomorphic to G, then there are subgroups H and K in G such that $H \cap K = \{e\}$, $HK = G$, and $hk = kh$ for all $h \in H$ and $k \in K$.

Solution: Suppose that $\phi : G_1 \times G_2 \to G$ is an isomorphism. Exercise 3.3.11 in the text shows that in $G_1 \times G_2$ the subgroups $H^* = \{(x_1, x_2) \mid x_2 = e\}$ and $K^* = \{(x_1, x_2) \mid x_1 = e\}$ have the properties we are looking for. Let $H = \phi(H^*)$ and $K = \phi(K^*)$ be the images in G of H^* and K^*, respectively. Exercise 3.4.17 shows that any isomorphism will map a subgroup of the domain to a subgroup of the codomain. Thus H and K are subgroups of G, so we only need to show that $H \cap K = \{e\}$, $HK = G$, and $hk = kh$ for all $h \in H$ and $k \in K$.

Let $y \in G$, with $y = \phi(x)$, for $x \in G_1 \times G_2$. If $y \in H \cap K$, then $y \in H$, and so $x \in H^*$. Since $y \in K$ as well, we must also have $x \in K^*$, so $x \in H^* \cap K^*$, and therefore $x = (e_1, e_2)$, where e_1 and e_2 are the respective identity elements in G_1 and G_2. Thus $y = \phi((e_1, e_2)) = e$, showing that $H \cap K = \{e\}$. Since y is any element of G, and we can write $x = h^*k^*$ for some $h^* \in H^*$ and some $k^* \in K^*$, it follows that $y = \phi(h^*k^*) = \phi(h^*)\phi(k^*)$, and thus $G = HK$. It is clear that ϕ preserves the fact that elements of H^* and K^* commute. We conclude that H and K satisfy the desired conditions.

38. Let G be an abelian group with subgroups H and K. Prove that if $HK = G$ and $H \cap K = \{e\}$, then $G \cong H \times K$.

Solution: We claim that $\phi : H \times K \to G$ defined by $\phi(h, k) = hk$, for all $(h, k) \in H \times K$, is a group isomorphism. First, for all $(h_1, k_1), (h_2, k_2) \in H \times K$ we have

$$\phi((h_1, k_1)(h_2, k_2)) = \phi((h_1h_2, k_1k_2)) = h_1h_2k_1k_2 \ .$$

On the other hand,

$$\phi((h_1, k_1))\phi((h_2, k_2)) = h_1k_1h_2k_2 = h_1h_2k_1k_2$$

since by assumption $k_1h_2 = h_2k_1$.

Since $HK = G$, it is clear that ϕ is onto. Finally, if $\phi((h, k)) = e$ for $(h, k) \in H \times K$, then $hk = e$ implies $h = k^{-1} \in H \cap K$, and so $h = e$ and $k = e$, which shows, using Proposition 3.4.4, that ϕ is one-to-one.

39. Show that for any prime number p, the subgroup of diagonal matrices in $\mathrm{GL}_2(\mathbf{Z}_p)$ is isomorphic to $\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$.

Solution: Since each matrix in $\mathrm{GL}_2(\mathbf{Z}_p)$ has nonzero determinant, it is clear that the mapping $\phi : \mathbf{Z}_p^\times \times \mathbf{Z}_p^\times \to \mathrm{GL}_2(\mathbf{Z}_p)$ defined by $\phi(x_1, x_2) = \begin{bmatrix} x_1 & 0 \\ 0 & x_2 \end{bmatrix}$, for each $(x_1, x_2) \in \mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$, is one-to-one and maps $\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$ onto the subgroup of diagonal matrices. This mapping respects the operations in the two groups, since for

$(a_1, a_2), (b_1, b_2) \in \mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$ we have

$$\begin{aligned} \phi((a_1, a_2)(b_1, b_2)) &= \phi((a_1b_1, a_2b_2)) \\ &= \begin{bmatrix} a_1b_1 & 0 \\ 0 & a_2b_2 \end{bmatrix} = \begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix} \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix} \\ &= \phi((a_1, a_2))\phi((b_1, b_2)) \, . \end{aligned}$$

Thus ϕ is the desired isomorphism.

40. (a) In the group $G = \mathrm{GL}_2(\mathbf{R})$ of invertible 2×2 matrices with real entries, show that

$$H = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in \mathrm{GL}_2(\mathbf{R}) \middle| \, a_{11} = 1, \; a_{21} = 0, \; a_{22} = 1 \right\}$$

is a subgroup of G.

Solution: Closure: $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}$.

Identity: The identity matrix has the correct form.

Existence of inverses: $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -a \\ 0 & 1 \end{bmatrix} \in H$.

(b) Show that H is isomorphic to the group $\mathbf{R}$ of all real numbers, under addition.

Solution: Define $\phi : \mathbf{R} \to H$ by $\phi(x) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$, for all $x \in \mathbf{R}$. You can easily check that ϕ is an isomorphism. (The computation necessary to show that ϕ preserves the respective operations is the same computation we used to show that H is closed.)

41. Let G be the subgroup of $\mathrm{GL}_2(\mathbf{R})$ defined by

$$G = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| \, m \neq 0 \right\} \, .$$

Show that G is not isomorphic to the direct product $\mathbf{R}^\times \times \mathbf{R}$.

Solution: Our approach is to try to find an algebraic property that would be preserved by any isomorphism but which is satisfied by only one of the two groups in question. By Proposition 3.4.3 (b), if one of the groups is abelian but the other is not, then the groups cannot be isomorphic.

The direct product $\mathbf{R}^\times \times \mathbf{R}$ is an abelian group, since each factor is abelian. On the other hand, G is not abelian, since $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}$ but $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}$. Thus the two groups cannot be isomorphic.

42. Let H be the following subgroup of group $G = \mathrm{GL}_2(\mathbf{Z}_3)$.

$$H = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \in \mathrm{GL}_2(\mathbf{Z}_3) \middle| \, m, b \in \mathbf{Z}_3, \; m \neq 0 \right\}$$

Show that H is isomorphic to the symmetric group S_3.

Solution: This group is small enough that we can just compare its multiplication table to that of S_3, as given in Table 3.3.3. Remember that constructing an isomorphism is the same as constructing a one-to-one correspondence between the elements of the group, such that all entries in the respective group tables also have the same one-to-one correspondence.

In this case we can explain how this can be done, without actually writing out the multiplication table. Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$. Then just as in Problem 3.3.29, we can show that $BA = A^{-1}B$, and that each element of H can be written uniquely in the form A^iB^j, where $0 \leq i < 3$ and $0 \leq j < 2$. This information should make it plausible that the function $\phi : S_3 \to H$ defined by $\phi(a^ib^j) = A^iB^j$, for all $0 \leq i < 3$ and $0 \leq j < 2$, gives a one-to-one correspondence between the elements of the groups which also produces multiplication tables that have exactly the same pattern.

ANSWERS AND HINTS

43. Let a, b be elements of a group G, with $o(b) = 2$ and $ba = a^2b$. Find $o(a)$.
Answer: Either $a = e$, and $o(a) = 1$, or $o(a) = 3$.

44. How many different isomorphisms are there from $\mathbf{Z}_6$ onto $\mathbf{Z}_2 \times \mathbf{Z}_3$?
Answer: There are two, since $\mathbf{Z}_2 \times \mathbf{Z}_3$ has two generators.

45. How many different isomorphisms are there from $\mathbf{Z}_{12}$ onto $\mathbf{Z}_4 \times \mathbf{Z}_3$?
Answer: There are exactly four different isomorphisms from $\mathbf{Z}_{12}$ onto $\mathbf{Z}_4 \times \mathbf{Z}_3$.

46. Is $\mathbf{Z}_{24}^{\times}$ isomorphic to $\mathbf{Z}_{30}^{\times}$? Give a complete explanation for your answer.
Answer: The two groups are *not* isomorphic, since in one (but not the other) every nontrivial element has order 2.

54. On $\mathbf{R}$, define a new operation by $x * y = x + y - 1$. Show that the group $G = (\mathbf{R}, *)$ is isomorphic to $(\mathbf{R}, +)$. *Note:* The group G is defined in Problem 3.1.37 (a).
Hint: Define $\phi : G \to \mathbf{R}$ by $\phi(x) = x - 1$, for all $x \in G$.

55. Show that the group $\mathbf{Q}$ is not isomorphic to the group $\mathbf{Q}^+$.
Hint: Suppose $\phi : \mathbf{Q} \to \mathbf{Q}^+$ is an isomorphism with $\phi(a) = 2$. Show that this would imply that $\sqrt{2} \in \mathbf{Q}^+$.

59. Let G be a finite abelian group, and let n be a positive integer. Define a function $\phi : G \to G$ by $\phi(g) = g^n$, for all $g \in G$. Find necessary and sufficient conditions to guarantee that ϕ is a group isomorphism.
Answer: The function ϕ is one-to-one if and only if G has no nontrivial element whose order is a divisor of n.

3.5 Cyclic Groups

21. Show that the three groups $\mathbf{Z}_6$, $\mathbf{Z}_9^\times$, and $\mathbf{Z}_{18}^\times$ are isomorphic to each other.

Solution: First, we have $|\mathbf{Z}_9^\times| = 6$, and $|\mathbf{Z}_{18}^\times| = 6$. In $\mathbf{Z}_9^\times$, $2^2 = 4$, $2^3 = 8 \not\equiv 1$, and so $[2]_9$ must have order 6, showing that $\mathbf{Z}_9^\times$ is cyclic of order 6. Our theorems tell us that $\mathbf{Z}_9^\times \cong \mathbf{Z}_6$. In $\mathbf{Z}_{18}^\times$, we have $5^2 \equiv 7$, $5^3 \equiv 17 \not\equiv 1$, and so $[5]_{18}$ must have order 6, showing that $\mathbf{Z}_{18}^\times$ is cyclic of order 6. Our theorems tell us that $\mathbf{Z}_{18}^\times \cong \mathbf{Z}_6$. Thus all three groups are isomorphic.

22. Is $\mathbf{Z}_{20}^\times$ cyclic?

Solution: We have $\mathbf{Z}_{20}^\times = \{\pm 1, \pm 3, \pm 7, \pm 9\}$. Direct calculations show that -1 and ± 9 have order 2, while ± 3 and ± 7 have order 4. Therefore $\mathbf{Z}_{20}^\times$ is not cyclic, since it has no element of order 8.

Alternate Solution: Exercise 3.4.21 in the text states that if m and n are relatively prime positive integers, then $\mathbf{Z}_{mn}^\times \cong \mathbf{Z}_m^\times \times \mathbf{Z}_n^\times$. Note that this can be proved by using the function $\phi : \mathbf{Z}_{mn}^\times \to \mathbf{Z}_m^\times \times \mathbf{Z}_n^\times$ defined by setting $\phi([x]_{mn}) = ([x]_m, [x]_n)$.

Thus we can simplify the given problem by noting that $\mathbf{Z}_{20}^\times \cong \mathbf{Z}_4^\times \times \mathbf{Z}_5^\times$. Since $\mathbf{Z}_4^\times$ has order 2 and $\mathbf{Z}_5^\times$ has order 4, by Proposition 3.3.4 (b) the elements of $\mathbf{Z}_{20}^\times$ can have order 1, 2, or 4, but not 8, which shows that $\mathbf{Z}_{20}^\times$ is not a cyclic group.

23. Is $\mathbf{Z}_{50}^\times$ cyclic?

Solution: We have $\varphi(50) = 20$, and so the possible orders of elements of $\mathbf{Z}_{50}^\times$ are $1, 2, 4, 5, 10, 20$. Calculating these powers of 3 gives $3^2 = 9$, $3^4 = (3^2)^2 = 81 \equiv 31$, $3^5 = 93 \equiv -7$, and $3^{10} = (3^5)^2 = (-7)^2 = 49$. Thus 3 must have order 20, and so $\mathbf{Z}_{50}^\times$ is a cyclic group.

24. Is $\mathbf{Z}_4 \times \mathbf{Z}_{10}$ isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_{20}$?

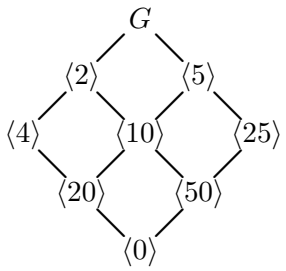
Solution: It follows from Theorem 3.5.5 that $\mathbf{Z}_{10} \cong \mathbf{Z}_2 \times \mathbf{Z}_5$, and that $\mathbf{Z}_{20} \cong \mathbf{Z}_4 \times \mathbf{Z}_5$. It then follows from Problem 3.4.33 that $\mathbf{Z}_4 \times \mathbf{Z}_{10} \cong \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_5$, and $\mathbf{Z}_2 \times \mathbf{Z}_{20} \cong \mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_5$. Finally, it is possible to show that the obvious mapping from $\mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_5$ onto $\mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_5$ is an isomorphism. Therefore $\mathbf{Z}_4 \times \mathbf{Z}_{10} \cong \mathbf{Z}_2 \times \mathbf{Z}_{20}$.

25. Is $\mathbf{Z}_4 \times \mathbf{Z}_{15}$ isomorphic to $\mathbf{Z}_6 \times \mathbf{Z}_{10}$?

Solution: As in Problem 24, $\mathbf{Z}_4 \times \mathbf{Z}_{15} \cong \mathbf{Z}_4 \times \mathbf{Z}_3 \times \mathbf{Z}_5$, and $\mathbf{Z}_6 \times \mathbf{Z}_{10} \cong \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_2 \times \mathbf{Z}_5$. The two groups are not isomorphic since the first has an element of order 4, while the second has none.

26. Give the lattice diagram of subgroups of $\mathbf{Z}_{100}$.

Solution: The subgroups correspond to the divisors of 100, and are given in the following diagram, where $G = \mathbf{Z}_{100}$.



Here $\langle n \rangle$ is the set of all multiples of $[n]_{100}$ in $\mathbf{Z}_{100}$.

27. Find all generators of the cyclic group $\mathbf{Z}_{28}$.

    Solution: By Corollary 3.5.4 (a), the generators correspond to the numbers less than 28 and relatively prime to 28. The Euler φ-function allows us to compute how many there are: $\varphi(28) = \frac{1}{2} \cdot \frac{6}{7} \cdot 28 = 12$. The list of generators is $\{\pm 1, \pm 3, \pm 5, \pm 9, \pm 11, \pm 13\}$.

28. In $\mathbf{Z}_{30}$, find the order of the subgroup $\langle 18 \rangle$; find the order of $\langle 24 \rangle$.

    Solution: Using Proposition 3.5.3, we first find $\gcd(18, 30) = 6$. Then $\langle 18 \rangle = \langle 6 \rangle$, and so the subgroup has $30/6 = 5$ elements.

    Similarly, $\langle 24 \rangle = \langle 6 \rangle$, and so we actually have $\langle 24 \rangle = \langle 18 \rangle$, and $|\langle 24 \rangle| = 5$.

29. In $\mathbf{Z}_{45}$ find all elements of order 15.

    Solution: Since $\frac{45}{15} = 3$, it follows that $[3]$ has order 15, and that $|\langle 3 \rangle| = 15$. If $[a]$ is another elements of order 15, then $\gcd(a, 45) = 3$ by Proposition 3.5.3, and $[a] \in \langle [3] \rangle$. The easiest way to find these elements is to remember that $\langle [3] \rangle$ is cyclic of order 15 and therefore isomorphic to $\mathbf{Z}_{15}$. The generators of $\mathbf{Z}_{15}$ correspond to the integers $1, 2, 4, 7, 8, 11, 13, 14$ that are relatively prime to 15, and so the elements of order 15 in $\mathbf{Z}_{45}$ correspond to these multiples of 3. Answer: the elements of order 15 in $\mathbf{Z}_{45}$ are $[3], [6], [12], [21], [24], [33], [39], [42]$.

30. Prove that if G_1 and G_2 are groups of order 7 and 11, respectively, then the direct product $G_1 \times G_2$ is a cyclic group.

    Solution: Since 7 and 11 are primes, the groups are cyclic. If a has order 7 in G_1 and b has order 11 in G_2, then (a, b) has order $\text{lcm}[7, 11] = 77$ in $G_1 \times G_2$. Thus $G_1 \times G_2$ is cyclic since it has an element whose order is equal to the order of the group.

31. Show that any cyclic group of even order has exactly one element of order 2.

    Solution: If G is cyclic of order $2n$, for some positive integer n, then it follows from Theorem 3.5.2 that G is isomorphic to $\mathbf{Z}_{2n}$. Since isomorphisms preserve orders of elements, we only need to answer the question in $\mathbf{Z}_{2n}$. In that group, the elements of order 2 are the nonzero solutions to the congruence $2x \equiv 0 \pmod{2n}$, and since the congruence can be rewritten as $x \equiv 0 \pmod{n}$, we see that $[n]_{2n}$ is the only element of order 2 in $\mathbf{Z}_{2n}$.

32. Use the the result in Problem 31 to show that the multiplicative groups $\mathbf{Z}_{15}^{\times}$ and $\mathbf{Z}_{21}^{\times}$ are not cyclic groups.

Solution: In $\mathbf{Z}_{15}^{\times}$, both $[-1]_{15}$ and $[4]_{15}$ are easily checked to have order 2.

In $\mathbf{Z}_{21}^{\times}$, we have $[8]_{21}^2 = [64]_{21} = [1]_{21}$, and so $[8]_{21}$ and $[-1]_{21}$ have order 2.

33. Prove that if p and q are different odd primes, then $\mathbf{Z}_{pq}^{\times}$ is not a cyclic group.

Solution: We know that $[-1]_{pq}$ has order 2, so by Problem 31 it is enough to find one other element of order 2. The Chinese remainder theorem (Theorem 1.3.6) states that the system of congruences $x \equiv 1 \pmod{p}$ and $x \equiv -1 \pmod{q}$ has a solution $[a]_{pq}$, since p and q are relatively prime. Because p is an odd prime, $[-1]_{pq}$ is not a solution, so $[a]_{pq} \neq [-1]_{pq}$. But $a^2 \equiv 1 \pmod{p}$ and $a^2 \equiv 1 \pmod{q}$, so $a^2 \equiv 1 \pmod{pq}$ since p and q are relatively prime. Thus $[a]_{pq}$ has order 2.

34. Find all cyclic subgroups of the quaternion group. Use this information to show that the quaternion group cannot be isomorphic to the subgroup of S_4 generated by $(1,2,3,4)$ and $(1,3)$.

Solution: The quaternion group $Q = \{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ is defined in Section 3.3. The elements satisfy the following identities:

$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$ and $\mathbf{ij} = \mathbf{k}$, $\mathbf{jk} = \mathbf{i}$, $\mathbf{ki} = \mathbf{j}$, $\mathbf{ji} = -\mathbf{k}$, $\mathbf{kj} = -\mathbf{i}$, $\mathbf{ik} = -\mathbf{j}$.

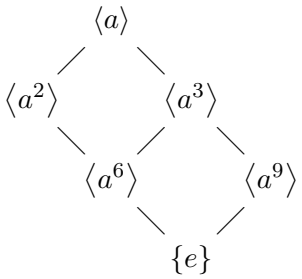
The cyclic subgroups $\langle -1\rangle = \{\pm 1\}$, $\langle \pm\mathbf{i}\rangle = \{\pm 1, \pm\mathbf{i}\}$, $\langle \pm\mathbf{j}\rangle = \{\pm 1, \pm\mathbf{j}\}$, and $\langle \pm\mathbf{k}\rangle = \{\pm 1, \pm\mathbf{k}\}$ can be found by using the given identities. For example, $\mathbf{i}^2 = -1$, $\mathbf{i}^3 = \mathbf{i}^2\mathbf{i} = -\mathbf{i}$, and $\mathbf{i}^4 = \mathbf{i}^2\mathbf{i}^2 = (-1)^2 = 1$.

In S_4, let $(1,2,3,4) = a$ and $(1,3) = b$. Since a is a cycle of length 4, it has order 4, with $a^2 = (1,3)(2,4)$ and $a^3 = a^{-1} = (1,4,3,2)$. To find the subgroup generated by a and b, we have $ab = (1,2,3,4)(1,3) = (1,4)(2,3)$, $a^2b = (1,3)(2,4)(1,3) = (2,4)$, and $a^3b = (1,4,3,2)(1,3) = (1,2)(3,4)$. On the other side, we have $ba = (1,3)(1,2,3,4) = (1,2)(3,4) = a^3b$, $ba^2 = (1,3)(1,3)(2,4) = (2,4) = a^2b$, and $ba^3 = (1,3)(1,4,3,2) = (1,4)(2,3) = ab$. This shows that the subgroup generated by a and b consists of the 8 elements $\{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$. Furthermore, from the cycle structures of the elements we can see that the only cyclic subgroup of order 4 is the one generated by a (and a^3). In any isomorphism, cyclic subgroups would correspond to cyclic subgroups, and so it is impossible for this group to be isomorphic to the quaternion group, which has 3 cyclic subgroups of order 4.

ANSWERS AND HINTS

35. Let G be a cyclic group of order 25, written multiplicatively, with $G = \langle a\rangle$. Find all elements of G that have order 5.
Answer: The elements $a^5, a^{10}, a^{15}, a^{20}$ have order 5.

36. Let G be a group with an element $a \in G$ with $o(a) = 18$. Find all subgroups of $\langle a\rangle$.



38. Give an example of an infinite group in which every element has finite order.
Answer: One possibility it to let G be the subgroup of elements of finite order in $\mathbf{C}^\times$, the set of all nth roots of unity, for all $n > 0$.

43. Let $D = \left\{ \left[\begin{array}{ccc} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{array} \right] \middle| \, a, b, c \in \mathbf{Z}_2 \right\}$. Note that D is a group by Problem 3.3.44.
(a) Find the number of elements of order 4 in D. Use this and the fact that D is nonabelian to guess which of the groups O, P, or Q (from Section 3.1) might be isomorphic to D.
Answer: Since D has 2 elements of order 4, the only possibility is that D might be isomorphic to P, and this turns out to be true.

44. Let n be a positive integer which has the prime decomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, where $p_1 < p_2 < \ldots < p_m$. Prove that $\mathbf{Z}_n^\times \cong \mathbf{Z}_{p_1^{\alpha_1}}^\times \times \mathbf{Z}_{p_2^{\alpha_2}}^\times \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}}^\times$.
Hint: Exercise 3.4.21 states that if m and n are relatively prime positive integers, then $\mathbf{Z}_{mn}^\times \cong \mathbf{Z}_m^\times \times \mathbf{Z}_n^\times$. This can be proved by using the function $\phi : \mathbf{Z}_{mn}^\times \to \mathbf{Z}_m^\times \times \mathbf{Z}_n^\times$ defined by setting $\phi([x]_{mn}) = ([x]_m, [x]_n)$. One possible approach is to use this result to give a proof by induction.

47. Let G be a group. Recall from Problem 3.4.60 that an isomorphism $\phi : G \to G$ is called an *automorphism* of G, and the set of all automorphisms of G is denoted by $\mathrm{Aut}(G)$. Show that $\mathrm{Aut}(\mathbf{Z}_n)$ is isomorphic to $\mathbf{Z}_n^\times$.
Hint: For $[m]_n \in \mathbf{Z}_n^\times$, define $\phi_m([x]_n) : \mathbf{Z}_n \to \mathbf{Z}_n$ by $\phi_m([x]_n) = [mx]_n$, for $[x]_n \in \mathbf{Z}_n$. Define $\Phi : \mathbf{Z}_n^\times \to \mathrm{Aut}(\mathbf{Z}_n)$ by setting $\Phi([m]_n) = \phi_m$.

3.6 Permutation Groups

28. In the dihedral group $D_n = \{a^i b^j \mid 0 \le i < n,\ 0 \le j < 2\}$ with $o(a) = n$, $o(b) = 2$, and $ba = a^{-1}b$, show that $ba^i = a^{n-i}b$, for all $0 \le i < n$.

Solution: For $i = 1$, the equation $ba^i = a^{n-i}b$ is just the relation that defines the group. If we assume that the result holds for $i = k$, then for $i = k + 1$ we have

$$ba^{k+1} = (ba^k)a = (a^{n-k}b)a = a^{n-k}(ba) = a^{n-k}a^{-1}b = a^{n-(k+1)}b \, .$$

This implies that the result must hold for all i with $0 \le i < n$.

Comment: This is similar to a proof by induction, but for each given n we only need to worry about a finite number of equations.

29. In the dihedral group $D_n = \{a^i b^j \mid 0 \leq i < n,\ 0 \leq j < 2\}$ with $o(a) = n$, $o(b) = 2$, and $ba = a^{-1}b$, show that each element of the form $a^i b$ has order 2.

Solution: Using the result from Problem 28, we have $(a^i b)^2 = (a^i b)(a^i b) = a^i(ba^i)b = a^i(a^{n-i}b)b = (a^i a^{n-i})(b^2) = a^n e = e$.

30. In S_4, find the subgroup H generated by $(1,2,3)$ and $(1,2)$.

Solution: Let $a = (1,2,3)$ and $b = (1,2)$. Then H must contain $a^2 = (1,3,2)$, $ab = (1,3)$ and $a^2 b = (2,3)$, and this set of elements is closed under multiplication. (We have just listed the elements of S_3.) Thus $H = \{(1), a, a^2, b, ab, a^2 b\} = \{(1),\ (1,2,3),\ (1,3,2),\ (1,2),\ (1,3),\ (2,3)\}$.

31. For the subgroup H of S_4 defined in the previous problem, find the corresponding subgroup $\sigma H \sigma^{-1}$, for $\sigma = (1,4)$.

Comment: Exercise 2.3.13 in the text shows that if $(1,2,\ldots,k)$ is a cycle of length k and σ is any permutation, then $\sigma(1,2,\ldots,k)\sigma^{-1} = (\sigma(1),\sigma(2),\ldots,\sigma(k))$.

Solution: We need to compute $\sigma\tau\sigma^{-1}$, for each $\tau \in H$. Since $(1,4)^{-1} = (1,4)$, we have $(1,4)(1)(1,4) = (1)$, and $(1,4)(1,2,3)(1,4) = (2,3,4)$. As a shortcut, we can use Exercise 2.3.13, which shows immediately that $\sigma(1,2,3)\sigma^{-1} = (\sigma(1),\sigma(2),\sigma(3)) = (4,2,3)$. Then we can quickly do the other computations:

$$\begin{aligned} (1,4)(1,3,2)(1,4)^{-1} &= (4,3,2) \\ (1,4)(1,2)(1,4)^{-1} &= (4,2) \\ (1,4)(1,3)(1,4)^{-1} &= (4,3) \\ (1,4)(2,3)(1,4)^{-1} &= (2,3). \end{aligned}$$

Thus $(1,4)H(1,4)^{-1} = \{(1),\ (2,3,4),\ (2,4,3),\ (2,3),\ (2,4),\ (3,4)\}$.

32. Show that each element in A_4 can be written as a product of 3-cycles.

Solution: We first list the 3-cycles: $(1,2,3)$, $(1,2,4)$, $(1,3,2)$, $(1,3,4)$, $(1,4,2)$, $(1,4,3)$, $(2,3,4)$, and $(2,4,3)$. Rather than starting with each of the other elements and then trying to write them as a product of 3-cycles, it is easier to just look at the possible products of 3-cycles. We have $(1,2,3)(1,2,4) = (1,3)(2,4)$, $(1,2,4)(1,2,3) = (1,4)(2,3)$, $(1,2,3)(2,3,4) = (1,2)(3,4)$, and this accounts for all 12 of the elements in A_4.

33. In the dihedral group $D_n = \{a^i b^j \mid 0 \leq i < n,\ 0 \leq j < 2\}$ with $o(a) = n$, $o(b) = 2$, and $ba = a^{-1}b$, find the centralizer of a.

Solution: The centralizer $C(a)$ contains all powers of a, so we have $\langle a \rangle \subseteq C(a)$. This shows that $C(a)$ has at least n elements. On the other hand, $C(a) \neq D_n$, since by definition b does not belong to $C(a)$. Since $\langle a \rangle$ contains exactly half of the elements in D_n, Lagrange's theorem show that there is no subgroup that lies strictly between $\langle a \rangle$ and D_n, so $\langle a \rangle \subseteq C(a) \subseteq D_n$ and $C(a) \neq D_n$ together imply that $C(a) = \langle a \rangle$.

34. Find the centralizer of $(1,2,3)$ in S_3, in S_4, and in A_4.

Comment: It helps to have some shortcuts when doing the necessary computations. To see that x belongs to $C(a)$, we need to check that $xa = ax$, or, equivalently, that $axa^{-1} = x$. Exercise 2.3.13 provides a quick way to do this in a group of permutations. As noted previously in this section, that exercise shows that if $(1,2,\ldots,k)$ is a cycle of length k and σ is any permutation, then $\sigma(1,2,\ldots,k)\sigma^{-1} = (\sigma(1),\sigma(2),\ldots,\sigma(k))$.

Solution: Since any power of an element a commutes with a, the centralizer $C(a)$ always contains the cyclic subgroup $\langle a\rangle$ generated by a. Thus the centralizer of $(1,2,3)$ always contains the subgroup $\{(1),(1,2,3),(1,3,2)\}$.

In S_3, the centralizer of $(1,2,3)$ is equal to $\langle\,(1,2,3)\,\rangle$, since it is easy to check that $(1,2)$ does not belong to the centralizer, and by Lagrange's theorem a *proper* subgroup of a group with 6 elements can have at most 3 elements.

To find the centralizer of $(1,2,3)$ in S_4 we have to work a bit harder. Let $a = (1,2,3)$. From the computations in S_3, we know that $(1,2)$, $(1,3)$, and $(2,3)$ do not commute with a. The remaining transpositions in S_4 are $(1,4)$, $(2,4)$, and $(3,4)$. Using Exercise 2.3.13, we have $a(1,4)a^{-1} = (2,4)$, $a(2,4)a^{-1} = (3,4)$, and $a(3,4)a^{-1} = (1,4)$, so no transposition in S_4 commutes with a. For the products of the transpositions, we have $a(1,2)(3,4)a^{-1} = (2,3)(1,4)$, $a(1,3)(2,4)a^{-1} = (2,1)(3,4)$, and $a(1,4)(2,3)a^{-1} = (2,4)(3,1)$, and so no product of transpositions belongs to $C(a)$.

If we do a similar computation with a 4-cycle, we have $a(x,y,z,4)a^{-1} = (u,v,w,4)$, since a just permutes the numbers x, y, and z. This means that $w \neq z$, so $(u,v,w,4)$ is not equal to $(x,y,z,4)$. Without doing all of the calculations, we can conclude that no 4-cycle belongs to $C(a)$. This accounts for an additional 6 elements. A similar argument shows that no 3-cycle that includes the number 4 as one of its entries can belong to $C(a)$. Since there are 6 elements of this form, we now have a total of 21 elements (out of 24) that are not in $C(a)$, and therefore $C(a) = \langle a\rangle$.

Finally, since A_4 contains the three products of transpositions and the six 3-cycles that include 4, we have nine elements (out of 12 in A_4) that do not commute with $(1,2,3)$. Thus in A_4 we get the same answer: $C(a) = \langle a\rangle$.

35. With the notation of the comments preceding the statement of Theorem 3.6.6, find $\sigma(\Delta_3)$ for each $\sigma \in S_n$.

Solution: By definition, $\Delta_3 = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$.

For $\sigma = (1)$, $\sigma(\Delta_3) = \Delta_3$.

For $\sigma = (1,2,3)$, $\sigma(\Delta_3) = (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) = \Delta_3$.

For $\sigma = (1,3,2)$, $\sigma(\Delta_3) = (x_3 - x_1)(x_3 - x_2)(x_1 - x_2) = \Delta_3$.

For $\sigma = (1,2)$, $\sigma(\Delta_3) = (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = -\Delta_3$.

For $\sigma = (1,3)$, $\sigma(\Delta_3) = (x_3 - x_2)(x_3 - x_1)(x_2 - x_1) = -\Delta_3$.

For $\sigma = (2,3)$, $\sigma(\Delta_3) = (x_1 - x_3)(x_1 - x_2)(x_3 - x_2) = -\Delta_3$.

ANSWERS AND HINTS

36. Compute the centralizer of $(1,2)(3,4)$ in S_4.
Answer: $C((1,2)(3,4)) =$
$\{(1), (1,2)(3,4), (1,2), (3,4), (1,3)(2,4), (1,4)(2,3), (1,4,2,3), (1,3,2,4)\}$.

37. Show that the group of rigid motions of a cube can be generated by two elements.
Hint: Let ρ be a 90 degree rotation that leaves the top and bottom fixed. Let σ be a 120 degree rotation with axis of rotation the line through two opposite vertices. To help in the computations, you can number the faces of the cube and represent ρ and σ as elements of S_6.

39. Describe the possible shapes of the permutations in A_6. Use a combinatorial argument to determine how many of each type there are.
Answer: 40 have shape (a,b,c); 45 have shape $(a,b)(c,d)$; 144 have shape (a,b,c,d,e); 90 have shape $(a,b,c,d)(e,f)$; 15 have shape $(a,b,c)(d,e,f)$; 1 has shape (a).

40. Find the largest possible order of an element in each of the alternating groups A_5, A_6, A_7, A_8.
Answer: The largest order in A_5 and A_6 is 5. In A_7, the largest possible order is 7. In A_8, the largest possible order is 15.

41. Let G be the dihedral group D_6, denoted by $G = \{a^i b^j | 0 \leq i < 6 \text{ and } 0 \leq j < 2\}$, where a has order 6, b has order 2, and $ba = a^{-1}b$. Find $C(ab)$.
Answer: $C(ab) = \{e, ab, a^3, a^4b\}$

44. Is D_{12} isomorphic to $D_4 \times \mathbf{Z}_3$?
Answer: No. *Hint:* Count the number of elements of order 6.

3.7 Homomorphisms

21. Find all group homomorphisms from $\mathbf{Z}_4$ into $\mathbf{Z}_{10}$.

Solution: As noted in Example 3.7.7, any group homomorphism from $\mathbf{Z}_n$ into $\mathbf{Z}_k$ must have the form $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$. Under any group homomorphism $\phi : \mathbf{Z}_4 \to \mathbf{Z}_{10}$, the order of $\phi([1]_4)$ must be a divisor of 4 and of 10, so the only possibilities are $o(\phi([1]_4) = 1$ or $o(\phi([1]_4) = 2$. Thus $\phi([1]_4) = [0]_{10}$, which defines the zero function, or else $\phi([1]_4) = [5]_{10}$, which leads to the formula $\phi([x]_4) = [5x]_{10}$, for all $[x]_4 \in \mathbf{Z}_4$.

22. (a) Find the formulas for all group homomorphisms from $\mathbf{Z}_{18}$ into $\mathbf{Z}_{30}$.

Solution: As noted in Example 3.7.7, any group homomorphism from $\mathbf{Z}_{18}$ into $\mathbf{Z}_{30}$ must have the form $\phi([x]_{18}) = [mx]_{30}$, for all $[x]_{18} \in \mathbf{Z}_{18}$. Since $\gcd(18, 30) = 6$, the possible orders of $[m]_{30} = \phi([1]_{18})$ are $1, 2, 3, 6$. The corresponding choices for $[m]_{30}$ are $[0]_{30}$ (order 1), $[15]_{30}$ (order 2), $[10]_{30}$ and $[20]_{30}$ (order 3), and $[5]_{30}$ and $[25]_{30}$ (order 6).

(b) Choose one of the nonzero formulas in part (a), and name it ϕ. Find $\phi(\mathbf{Z}_{18})$ and $\ker(\phi)$, and show how elements of $\phi(\mathbf{Z}_{18})$ correspond to equivalence classes of $\sim_\phi$.

Solution: For example, consider $\phi([x]_{18}) = [5x]_{30}$. The image of ϕ consists of the multiples of 5 in $\mathbf{Z}_{30}$, which are $0, 5, 10, 15, 20, 25$. We have $\ker(\phi) = \{0, 6, 12\}$, and using Proposition 3.7.9 to find the equivalence classes of $\sim_\phi$, we add 1, 2, 3, 4, and 5, respectively, to the kernel. We have the following correspondence:

$\{[0]_{18}, [6]_{18}, [12]_{18}\} \longleftrightarrow \phi([0]_{18}) = [0]_{30}$, $\quad \{[3]_{18}, [9]_{18}, [15]_{18}\} \longleftrightarrow \phi([3]_{18}) = [15]_{30}$,

$\{[1]_{18}, [7]_{18}, [13]_{18}\} \longleftrightarrow \phi([1]_{18}) = [5]_{30}$, $\quad \{[4]_{18}, [10]_{18}, [16]_{18}\} \longleftrightarrow \phi([4]_{18}) = [20]_{30}$,

$\{[2]_{18}, [8]_{18}, [14]_{18}\} \longleftrightarrow \phi([2]_{18}) = [10]_{30}$, $\quad \{[5]_{18}, [11]_{18}, [17]_{18}\} \longleftrightarrow \phi([5]_{18}) = [25]_{30}$.

23. (a) Show that $\mathbf{Z}_{11}^\times$ is cyclic, with generator $[2]_{11}$.

Solution: An element of $\mathbf{Z}_{11}^\times$ can have order 1, 2, 5, or 10. Since $2^2 \equiv 4 \not\equiv 1$ and $2^5 \equiv 10 \not\equiv 1$, it follows that $[2]_{11}$ cannot have order 2 or 5, so it must have order 10.

(b) Show that $\mathbf{Z}_{19}^\times$ is cyclic, with generator $[2]_{19}$.

Solution: Since $\mathbf{Z}_{19}^\times$ has order 18, the order of [2] is 2, 3, 6, or 18. The element $[2]_{19}$ is a generator for $\mathbf{Z}_{19}^\times$ because it has order 18, since $2^2 = 4 \not\equiv 1$, $2^3 = 8 \not\equiv 1$, and $2^6 \equiv (2^3)^2 \equiv 7 \not\equiv 1$.

(c) Completely determine all group homomorphisms from $\mathbf{Z}_{19}^\times$ into $\mathbf{Z}_{11}^\times$.

Solution: Any group homomorphism $\phi : \mathbf{Z}_{19}^\times \to \mathbf{Z}_{11}^\times$ is determined by its value on the generator $[2]_{19}$, and the order of $\phi([2]_{19})$ must be a common divisor of 18 and 10. Thus the only possible order of $\phi([2]_{19})$ is 1 or 2, so either $\phi([2]_{19}) = [1]_{11}$ or $\phi([2]_{19}) = [10]_{11} = [-1]_{11}$. In the first case, $\phi([x]_{19}) = [1]_{11}$ for all $[x]_{19} \in \mathbf{Z}_{19}^\times$, and in the second case $\phi([2]_{19}^n) = [-1]_{11}^n$, for all $[x]_{19} = [2]_{19}^n \in \mathbf{Z}_{19}^\times$.

24. Define $\phi : \mathbf{Z}_4 \times \mathbf{Z}_6 \to \mathbf{Z}_4 \times \mathbf{Z}_3$ by $\phi([x]_4, [y]_6) = ([x + 2y]_4, [y]_3)$.

(a) Show that ϕ is a well-defined group homomorphism.

Solution: If $y_1 \equiv y_2 \pmod 6$, then $2y_1 - 2y_2$ is divisible by 12, so $2y_1 \equiv 2y_2 \pmod 4$, and then it follows quickly that ϕ is a well-defined function. It is also easy to check that ϕ preserves addition.

(b) Find the kernel and image of ϕ, and apply Theorem 3.7.8.

Solution: If $([x]_4, [y]_6)$ belongs to $\ker(\phi)$, then $y \equiv 0 \pmod 3$, so $y = 0$ or $y = 3$. If $y = 0$, then $x = 0$, and if $y = 3$, then $x = 2$. Thus the elements of the kernel K are $([0]_4, [0]_6)$ and $([2]_4, [3]_6)$.

It follows that there are $24/2 = 12$ equivalence classes determined by ϕ. These are in one-to-one correspondence with the elements of the image, so ϕ must map $\mathbf{Z}_4 \times \mathbf{Z}_6$ onto $\mathbf{Z}_4 \times \mathbf{Z}_3$. Thus $(\mathbf{Z}_4 \times \mathbf{Z}_6)/\phi \cong \mathbf{Z}_4 \times \mathbf{Z}_3$.

25. Let n and m be positive integers, such that m is a divisor of n. Show that $\phi : \mathbf{Z}_n^\times \to \mathbf{Z}_m^\times$ defined by $\phi([x]_n) = [x]_m$, for all $[x]_n \in \mathbf{Z}_n^\times$, is a well-defined group homomorphism.

Solution: First, note that ϕ is a well-defined function, since if $[x_1]_n = [x_2]_n$ in $\mathbf{Z}_n^\times$, then $n \mid (x_1 - x_2)$, and this implies that $m \mid (x_1 - x_2)$, since $m \mid n$. Thus $[x_1]_m = [x_2]_m$, and so $\phi([x_1]_n) = \phi([x_2]_n)$.

Next, ϕ is a homomorphism since for $[a]_n, [b]_n \in \mathbf{Z}_n^\times$, we have $\phi([a]_n[b]_n) = \phi([ab]_n) = [ab]_m = [a]_m[b]_m = \phi([a]_n)\phi([b]_n)$.

26. For the group homomorphism $\phi : \mathbf{Z}_{36}^{\times} \to \mathbf{Z}_{12}^{\times}$ defined by $\phi([x]_{36}) = [x]_{12}$, for all $[x]_{36} \in \mathbf{Z}_{36}^{\times}$, find the kernel and image of ϕ, and apply Theorem 3.7.8.

Solution: The previous problem shows that ϕ is a group homomorphism. It is evident that ϕ maps $\mathbf{Z}_{36}^{\times}$ onto $\mathbf{Z}_{12}^{\times}$, since if $\gcd(x, 12) = 1$, then $\gcd(x, 36) = 1$. The kernel of ϕ consists of the elements in $\mathbf{Z}_{36}^{\times}$ that are congruent to 1 mod 12, namely $[1]_{36}, [13]_{36}, [25]_{36}$. It follows that $\mathbf{Z}_{36}^{\times}/\phi \cong \mathbf{Z}_{12}^{\times}$.

27. Prove that $\mathrm{SL}_n(\mathbf{R})$ is a normal subgroup of $\mathrm{GL}_n(\mathbf{R})$.

Solution: Let $G = \mathrm{GL}_n(\mathbf{R})$ and $N = \mathrm{SL}_n(\mathbf{R})$. The condition we need to check, that $gxg^{-1} \subseteq N$ for all $n \in N$ and all $g \in G$, translates into the condition that if P is any invertible matrix and $\det(A) = 1$, then PAP^{-1} has determinant 1. This follows immediately from the fact that

$$\det(PAP^{-1}) = \det(P)\det(A)\det(P^{-1} = \det(P)\det(A)\frac{1}{\det(P)} = \det(A) \ ,$$

which you may remember from your linear algebra course as the proposition that similar matrices have the same determinant.

Alternate solution: Here is a slightly more sophisticated proof. Note that $\mathrm{SL}_n(\mathbf{R})$ is the kernel of the determinant homomorphism from $\mathrm{GL}_n(R)$ into $\mathbf{R}$ (Example 3.7.1 in the text shows that the determinant defines a group homomorphism.) The result then follows immediately from Proposition 3.7.4 (a), which shows that the kernel of any group homomorphism is a normal subgroup.

ANSWERS AND HINTS

28. Prove or disprove each of the following assertions:
(a) The set of all nonzero scalar matrices is a normal subgroup of $\mathrm{GL}_n(\mathbf{R})$.
Answer: This set is the center of $\mathrm{GL}_n(\mathbf{R})$, and so it is a normal subgroup.
(b) The set of all diagonal matrices with nonzero determinant is a normal subgroup of $\mathrm{GL}_n(\mathbf{R})$.
Answer: This set is a subgroup, but it is not normal.

31. Define $\phi : \mathbf{Z}_{15}^{\times} \to \mathbf{Z}_{15}^{\times}$ by $\phi([x]_{15}) = [x]_{15}^3$, for all $[x]_{15} \in \mathbf{Z}_{15}^{\times}$. Find the kernel and image of ϕ.
Answer: The function ϕ is an isomorphism.

32. Define $\phi : \mathbf{Z}_{15}^{\times} \to \mathbf{Z}_5^{\times}$ by $\phi([x]_{15}) = [x]_5^3$. Show that ϕ is a group homomorphism, and find its kernel and image.
Answer: The function ϕ is onto with $\ker(\phi) = \{[1]_{15}, [11]_{15}\}$.

34. How many homomorphisms are there from $\mathbf{Z}_{12}$ into $\mathbf{Z}_4 \times \mathbf{Z}_3$?
Answer: There are 12, since $[1]_{12}$ can be mapped to any element of $\mathbf{Z}_4 \times \mathbf{Z}_3$.

36. Define $\phi : \mathbf{R} \to \mathbf{C}^{\times}$ by setting $\phi(x) = e^{ix}$, for all $x \in \mathbf{R}$. Show that ϕ is a group homomorphism, and find $\ker(\phi)$ and the image $\phi(\mathbf{R})$.
Answer: The image is the unit circle in the complex plane, and $\ker(\phi) = \{2k\pi \mid k \in \mathbf{Z}\}$.

37. Let G be a group, with a subgroup $H \subseteq G$. Define $N(H) = \{g \in G \mid gHg^{-1} = H\}$.
(b) Let $G = S_4$. Find $N(H)$ for the subgroup H generated by $(1,2,3)$ and $(1,2)$.
Answer: In this example, $N(H) = H$.

38. Find all normal subgroups of A_4.
Answer: $\{(1)\}$, $N = \{(1)$, $(1,2)(3,4)$, $(1,3)(2,4)$, $(1,4)(2,3)\}$, and A_4 are the normal subgroups of A_4.

3.8 Cosets, Normal Subgroups, and Factor Groups

29. Define $\phi : \mathbf{C}^\times \to \mathbf{R}^\times$ by $\phi(z) = |z|$, for all $z \in \mathbf{C}^\times$.

(a) Show that ϕ is a group homomorphism.

Solution: For $z_1, z_2 \in \mathbf{C}^\times$, we have $\phi(z_1 z_2) = |z_1 z_2|$ and $\phi(z_1)\phi(z_2) = |z_1|\,|z_2|$. Thus ϕ is a group homomorphism since $|z_1 z_2| = |z_1|\,|z_2|$, for all $z_1, z_2 \in \mathbf{C}^\times$.

(b) Find $\ker(\phi)$ and $\phi(\mathbf{C}^\times)$.

Solution: The kernel of ϕ is the circle group $\{z \in \mathbf{C} \mid |z| = 1\}$, and $\phi(\mathbf{C}^\times) = \mathbf{R}^+$.

(c) Describe the cosets of $\ker(\phi)$, and explain how they are in one-to-one correspondence with the elements of $\phi(\mathbf{C}^\times)$.

Solution: As in Problem 2.2.19, in the complex plane the cosets of the kernel are the concentric circles with center at the origin. They form a group isomorphic to $\mathbf{R}^+$, and multiplication of cosets is most easily calculated by using the unique positive real number in the coset.

30. List the cosets of $\langle 9\rangle$ in $\mathbf{Z}_{16}^\times$, and find the order of each coset in $\mathbf{Z}_{16}^\times / \langle 9\rangle$.

Solution: $\mathbf{Z}_{16}^\times = \{1,3,5,7,9,11,13,15\}$.

$\langle 9\rangle = \{1,9\}$ $\quad 3\langle 9\rangle = \{3,11\}$ $\quad 5\langle 9\rangle = \{5,13\}$ $\quad 7\langle 9\rangle = \{7,15\}$

Recall Example 3.8.5, which shows that the order of aN is the smallest positive integer n such that $a^n \in N$.

The coset $3\langle 9\rangle$ has order 2 since $3^2 = 9$ and 9 belongs to the subgroup $\langle 9\rangle$. (We could have used either element of the coset to do the calculation.) The coset $5\langle 9\rangle$ also has order 2, since $5^2 = 9$. The coset $7\langle 9\rangle$ has order 2 since $7^2 = 1$.

31. List the cosets of $\langle 7\rangle$ in $\mathbf{Z}_{16}^\times$. Is the factor group $\mathbf{Z}_{16}^\times / \langle 7\rangle$ cyclic?

Solution: $\mathbf{Z}_{16}^\times = \{1,3,5,7,9,11,13,15\}$.

$\langle 7\rangle = \{1,7\}$ $\quad 3\langle 7\rangle = \{3,5\}$ $\quad 9\langle 7\rangle = \{9,15\}$ $\quad 11\langle 7\rangle = \{11,13\}$

Since $3^2 \notin \langle 7\rangle$, the coset $3\langle 7\rangle$ does not have order 2, so it must have order 4, showing that the factor group is cyclic.

32. Let $G = \mathbf{Z}_6 \times \mathbf{Z}_4$, let $H = \{([0]_6, [0]_4), ([0]_6, [2]_4)\}$, and let $K = \{([0]_6, [0]_4), ([3]_6, [0]_4)\}$.

(a) List all cosets of H; list all cosets of K.

Solution: The cosets of $H = \{([0]_6, [0]_4), ([0]_6, [2]_4)\}$ are

$([0]_6,[0]_4)+H=\{([0]_6,[0]_4),([0]_6,[2]_4)\}$ $([1]_6,[0]_4)+H=\{([1]_6,[0]_4),([1]_6,[2]_4)\}$
$([2]_6,[0]_4)+H=\{([2]_6,[0]_4),([2]_6,[2]_4)\}$ $([3]_6,[0]_4)+H=\{([3]_6,[0]_4),([3]_6,[2]_4)\}$
$([4]_6,[0]_4)+H=\{([4]_6,[0]_4),([4]_6,[2]_4)\}$ $([5]_6,[0]_4)+H=\{([5]_6,[0]_4),([5]_6,[2]_4)\}$

$([0]_6,[1]_4)+H=\{([0]_6,[1]_4),([0]_6,[3]_4)\}$ $([1]_6,[1]_4)+H=\{([1]_6,[1]_4),([1]_6,[3]_4)\}$
$([2]_6,[1]_4)+H=\{([2]_6,[1]_4),([2]_6,[3]_4)\}$ $([3]_6,[1]_4)+H=\{([3]_6,[1]_4),([3]_6,[3]_4)\}$
$([4]_6,[1]_4)+H=\{([4]_6,[1]_4),([4]_6,[3]_4)\}$ $([5]_6,[1]_4)+H=\{([5]_6,[1]_4),([5]_6,[3]_4)\}$

The cosets of $K=\{([0]_6,[0]_4),([3]_6,[0]_4)\}$ are

$([0]_6,[0]_4)+K=\{([0]_6,[0]_4),([3]_6,[0]_4)\}$ $([0]_6,[1]_4)+K=\{([0]_6,[1]_4),([3]_6,[1]_4)\}$
$([0]_6,[2]_4)+K=\{([0]_6,[2]_4),([3]_6,[2]_4)\}$ $([0]_6,[3]_4)+K=\{([0]_6,[3]_4),([3]_6,[3]_4)\}$

$([1]_6,[0]_4)+K=\{([1]_6,[0]_4),([4]_6,[0]_4)\}$ $([1]_6,[1]_4)+K=\{([1]_6,[1]_4),([4]_6,[1]_4)\}$
$([1]_6,[2]_4)+K=\{([1]_6,[2]_4),([4]_6,[2]_4)\}$ $([1]_6,[3]_4)+K=\{([1]_6,[3]_4),([4]_6,[3]_4)\}$

$([2]_6,[0]_4)+K=\{([2]_6,[0]_4),([5]_6,[0]_4)\}$ $([2]_6,[1]_4)+K=\{([2]_6,[1]_4),([5]_6,[1]_4)\}$
$([2]_6,[2]_4)+K=\{([2]_6,[2]_4),([5]_6,[2]_4)\}$ $([2]_6,[3]_4)+K=\{([2]_6,[3]_4),([5]_6,[3]_4)\}$

(b) You may assume that any abelian group of order 12 is isomorphic to either $\mathbf{Z}_{12}$ or $\mathbf{Z}_6\times\mathbf{Z}_2$. Which answer is correct for G/H? For G/K?

Solution: Adding an element of G to itself 6 times yields a 0 in the first component and either 0 or 2 in the second component, producing an element in H. Thus the order of an element in G/H is at most 6, and so $G/H\cong\mathbf{Z}_6\times\mathbf{Z}_2$.

On the other hand, $([1]_6,[1]_4)+K$ has order 12 in G/K, and so $G/K\cong\mathbf{Z}_{12}$.

33. Let the dihedral group D_n be given via generators and relations, with generators a of order n and b of order 2, satisfying $ba=a^{-1}b$.

(a) Show that $ba^i=a^{-i}b$ for all i with $1\leq i<n$, and that any element of the form a^ib has order 2.

Solution: These questions are review: see Problems 3.6.28 and 3.6.29.

(b) List all left cosets and all right cosets of $\langle a\rangle$.

Solution: The subgroup $\langle a\rangle$ has n elements, and so its index is 2. Therefore the left and right cosets coincide, and they are $\langle a\rangle=\{a^i\}$ and $\langle a\rangle\,b=\{a^ib\}$.

(c) List all left cosets and all right cosets of $\langle b\rangle$.

Solution: There are n left cosets of $\langle b\rangle=\{e,b\}$, and they have the form $a^i\,\langle b\rangle=\{a^i,a^ib\}$, for $0\leq i<n$.

The right cosets of $\langle b\rangle$ have the form $\langle b\rangle\,a^i=\{a^i,a^{-i}b\}$, for $0\leq i<n$.

(d) List all left cosets and all right cosets of $\langle ab\rangle$.

Solution: Since $\langle ab\rangle=\{e,ab\}$, the left cosets have the form $a^i\,\langle ab\rangle=\{a^i,a^{i+1}b\}$, for $0\leq i<n$.

The right cosets of $\langle ab\rangle$ have the form $\langle ab\rangle\,a^i=\{a^i,a^{1-i}b\}$, for $0\leq i<n$.

34. Let G be the dihedral group D_6 and let N be the subgroup $\langle a^3 \rangle = \{e, a^3\}$ of G.

(a) Show that N is a normal subgroup of G.

Solution: Since $N = \langle a^3 \rangle$, it is a subgroup. It is normal since $a^i(a^3)a^{-i} = a^3$ and $a^ib(a^3)a^ib = a^ia^{-3}ba^ib = a^ia^{-3}a^{-i}b^2 = a^{-3} = a^3$. (We are using the fact that $ba^i = a^{-i}b$, and we have actually shown that a^3 is in the center of D_6.)

(b) Since $|G/N| = 6$, you can assume that G/N is isomorphic to either $\mathbf{Z}_6$ or S_3. (Exercise 3.3.17 characterizes groups of order 6 as isomorphic to either $\mathbf{Z}_6$ or S_3.) Which group gives the correct answer?

Solution: For $aN = \{a, a^4\}$ and $bN = \{b, a^3b\}$, we have $(aN)(bN) = abN = \{ab, a^4b\}$, while $(bN)(aN) = baN = a^5bN = \{a^5b, a^2b\}$. Thus $(aN)(bN) \neq (bN)(aN)$, and G/N is not abelian. This implies that $G/N \cong S_3$.

35. Let G be the dihedral group D_6 and let H be the subgroup $\langle b \rangle = \{e, b\}$ of G. Show that H is not a normal subgroup of G.

Solution: We will compute the left and right cosets of N. First, $aH = \{a, ab\}$. The corresponding right coset is $Ha = \{a, ba\} = \{a, a^5b\}$. (See Problem 33.) This immediately shows that the left and right cosets of H do not coincide, and so Proposition 3.8.8 implies that H is not a normal subgroup of G.

36. Let G be the dihedral group D_6 and let H be the subset $\{e, a^3, b, a^3b\}$ of G.

(a) Show that H is subgroup of G.

Solution: We first note that $ba^3 = a^{-3}b = a^3b$, and so a^3 and b commute. It is then easy to check that H is closed under multiplication, so it is a subgroup since it is a finite subset of G.

(b) Is H a normal subgroup of G?

Solution: We will compute the left and right cosets of H. First, $aH = \{a, a^4, ab, a^4b\}$. The corresponding right coset is $Ha = \{a, a^4, ba, a^3ba\} = \{a, a^4, a^5b, a^2b\}$. Since the left and right cosets do not coincide, Proposition 3.8.8 implies that H is not a normal subgroup of G.

37. Let G be the dihedral group D_{12}, and let N be the subgroup $\langle a^3 \rangle = \{e, a^3, a^6, a^9\}$.

(a) Prove that N is a normal subgroup of G, and list all cosets of N.

Solution: Since $N = \langle a^3 \rangle$, it is a subgroup. It is normal since $a^i(a^{3n})a^{-i} = a^{3n}$ and $a^ib(a^{3n})a^ib = a^ia^{-3n}a^{-i} = (a^{3n})^{-1}$. (We are using the fact that $ba^i = a^{-i}b$.)

The cosets of N are

$N = \{e, a^3, a^6, a^9\}$, $\quad Nb = \{ab, a^3b, a^6b, a^9b\}$,

$Na = \{a, a^4, a^7, a^{10}\}$, $\quad Nab = \{ab, a^4b, a^7b, a^{10}b\}$,

$Na^2 = \{a^2, a^5, a^8, a^{11}\}$, $\quad Na^2b = \{a^2b, a^5b, a^8b, a^{11}b\}$.

(b) Since $|G/N| = 6$, you can assume that G/N is isomorphic to either $\mathbf{Z}_6$ or S_3. Which group gives the correct answer?

Solution: The factor group G/N is not abelian, since $NaNb = Nab$ but $NbNa = Na^2b$, because $ba = a^{11}b \in Na^2b$. Thus $G/N \cong S_3$.

38. Let G be a group. For $a, b \in G$ we say that b is **conjugate** to a, written $b \sim a$, if there exists $g \in G$ such that $b = gag^{-1}$. Following part (a), the equivalence classes of $\sim$ are called the **conjugacy classes** of G.

(a) Show that $\sim$ is an equivalence relation on G.

Solution: We have $a \sim a$ since we can use $g = e$. If $b \sim a$, the $b = gag^{-1}$ for some $g \in G$, and so $a = g^{-1}bg = g^{-1}b(g^{-1})^{-1}$, which shows that $a \sim b$. If $c \sim b$ and $b \sim a$, then $c = gbg^{-1}$ and $b = hah^{-1}$ for some $g, h \in G$, so $c = g(hah^{-1})g^{-1} = (gh)a(gh)^{-1}$, which shows that $c \sim a$. Thus $\sim$ is an equivalence relation.

(b) Show that a subgroup N of G is normal in G if and only if N is a union of conjugacy classes.

Solution: The subgroup N is normal in G if and only if $a \in N$ implies $gag^{-1} \in G$, for all $g \in G$. Thus N is normal if and only if whenever it contains an element a it also contains the conjugacy class of a. Another way to say this is that N is a union of conjugacy classes.

39. Find the conjugacy classes of D_4.

Solution: Remember: the notion of a conjugacy class was just defined in Problem 38. Let $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, with $a^4 = e$, $b^2 = e$, and $ba = a^{-1}b$.

Conjugacy class of e: This is just $\{e\}$ since $xex^{-1} = e$ for all $x \in D_4$.

Conjugacy class of a: if $x = a^i$, then $xax^{-1} = a$, but if $x = a^ib$, then $xax^{-1} = a^ibaa^{-i}b = a^ia^{i-1}b^2 = a^{2i-1}$. Thus the conjugacy class of a is $\{a, a^3\}$.

Conjugacy class of a^2: If $x = a^i$, then $xa^2x^{-1} = a^2$, and if $x = a^ib$, then $xax^{-1} = a^iba^2a^ib = a^ia^2ba^ib = a^ia^2a^{-i}b^2 = a^2$, so the conjugacy class of a^2 is $\{a^2\}$.

Conjugacy class of b: If $x = a^i$, then $xbx^{-1} = a^iba^{-i} = a^ia^ib = a^{2i}b$. If $x = a^ib$, then $xbx^{-1} = (a^ib)b(a^ib)^{-1} = a^ia^ib = a^{2i}b$. Thus the conjugacy class of b is $\{b, a^2b\}$.

Conjugacy class of ab: If $x = a^i$, then $x(ab)x^{-1} = a^iaba^{-i} = a^{i+1}a^ib = a^{2i+1}b$. If $x = a^ib$, then $xabx^{-1} = (a^ib)ab(a^ib)^{-1} = a^ia^{-1}a^ib = a^{2i-1}b$. Thus the conjugacy class of ab is $\{ab, a^3b\}$.

Answer: The conjugacy classes of D_4 are $\{e\}$, $\{a, a^3\}$, $\{a^2\}$, $\{b, a^2b\}$, $\{ab, a^3b\}$.

40. Show that A_4 is the only subgroup of index 2 in S_4.

Solution: Suppose that H is a subgroup of S_4 with $|H| = 12$. It follows from Example 3.8.8 that H must be normal since it has index 2, and it follows from Problem 38 (b) that H must be a union of conjugacy classes.

If $\sigma \in S_4$, then $\sigma(a_1, \cdots, a_n)\sigma^{-1} = (\sigma(a_1), \cdots, \sigma(a_n))$, so

$\sigma(a, b)\sigma^{-1} = (\sigma(a), \sigma(b))$,

$\sigma(a, b)(c, d)\sigma^{-1} = \sigma(a, b)\sigma^{-1}\sigma(cd)\sigma^{-1} = (\sigma(a), \sigma(b))(\sigma(c), \sigma(d))$,

$\sigma(a, b, c)\sigma^{-1} = (\sigma(a), \sigma(b), \sigma(c))$, and

$\sigma(a,b,c,d)\sigma^{-1} = (\sigma(a),\sigma(b),\sigma(c),\sigma(d))$.

We can summarize this by saying that the conjugate of any product of disjoint cycles has exactly the same number of cycles of the same length. Furthermore, it follows from Exercise 2.3.13 (b) in the text that if two permutations have the same shape (the same number of disjoint cycles of the same length) then they are conjugate.

There are $\frac{4\cdot3}{2} = 6$ transpositions in S_4, and $\frac{4\cdot3}{2\cdot2} = 3$ permutations of the form $(a,b)(c,d)$. The number of 3-cycles is $\frac{4\cdot3\cdot2}{3} = 8$, and the number of 4-cycles is $\frac{4\cdot3\cdot2\cdot1}{4} = 6$.

Because H is a union of conjugacy classes, we have to be able to write 12 as a sum of some combination of the numbers 1, 6, 3, 8 and 6. Since $(1) \in H$, the only possibility is $12 = 1+3+8$, so H must contain (1), all 3-cycles, and all permutations of the form $(a,b)(c,d)$. These are precisely the even permutations, and thus $H = A_4$.

41. Let G be a group, and let N and H be subgroups of G such that N is normal in G. It follows from Proposition 3.3.2 that HN is a subgroup, and Exercise 3.8.27 shows that N is a normal in HN. Prove that if $H \cap N = \{e\}$, then $HN/N \cong H$.

Solution: Define $\phi : H \to HN/N$ by $\phi(x) = xN$ for all $x \in H$. (Defining a function from HN/N into H is more complicated.) Then $\phi(xy) = xyN = xNyN = \phi(x)\phi(y)$ for all $x, y \in H$. Any coset of N in HN has the form hnN for some $h \in H$ and some $n \in N$. But then $hnN = hN = \phi(h)$, and so this shows that ϕ is onto. Finally, ϕ is one-to-one since if $h \in H$ belongs to the kernel of ϕ, then $hN = \phi(h) = N$, and so $h \in N$. By assumption, $H \cap N = \{e\}$, and so $h = e$.

42. Use Problem 41 to show that $\mathbf{Z}_{16}^{\times}/\langle 7\rangle \cong \mathbf{Z}_4$.

Solution: Let $H = \langle 3\rangle = \{1,3,9,11\}$ and let $N = \langle 7\rangle = \{1,7\}$. Then $H \cap N = \{1\}$, and $HN = \{1,3,9,11,1\cdot7,3\cdot7,9\cdot7,11\cdot7\} = \{1,3,9,11,7,5,15,13\} = \mathbf{Z}_{16}^{\times}$. The isomorphism then follows from Problem 41 since $\mathbf{Z}_{16}^{\times}/\langle 7\rangle = HN/N \cong H = \langle 3\rangle \cong \mathbf{Z}_4$.

Comment: The result also follows from Problem 31, where we showed that $\mathbf{Z}_{16}^{\times}/\langle 7\rangle$ is cyclic of order 4.

ANSWERS AND HINTS

43. In $\mathbf{Z}_{25}^{\times}/\langle 6\rangle$, find the order of each of the cosets $2\langle 6\rangle$, $3\langle 6\rangle$, and $4\langle 6\rangle$.
Answer: The coset $2\langle 6\rangle$ has order 4, while $3\langle 6\rangle$ has order 4, and $4\langle 6\rangle$ has order 2.

45. Let G_1 and G_2 be groups with normal subgroups $N_1 \subseteq G_1$ and $N_2 \subseteq G_2$.
(b) Show that $G_1 \times G_2/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2)$.
Answer: Define $\phi : G_1 \times G_2 \to (G_1/N_1) \times (G_2/N_2)$ by $\phi(g_1,g_2) = (g_1N_1, g_2N_2)$.
It only takes some easy calculations to show that ϕ is a group homomorphism. It is clear that ϕ is an onto mapping, and that $(g_1,g_2) \in \ker(\phi)$ if and only if $g_1 \in N_1$ and $g_2 \in N_2$. Thus $\ker(\phi) = N_1 \times N_2$, and applying the fundamental homomorphism theorem gives the desired result.

46. Exercise 3.8.25 asks for an example of a finite group G with two normal subgroups H and K such that $G/H \cong G/K$ but $H \ncong K$. As a complement to that exercise,

give an example of a finite group G with normal subgroups $H \cong K$ but $G/H \ncong G/K$.
Answer: Let $G = \mathbf{Z}_{16}^{\times}$, let $H = \langle 7 \rangle$, and let $K = \langle -7 \rangle$. (See Problems 30 and 31.)

52. Show that the quaternion group Q cannot be the internal direct product of two proper subgroups.
Hint: Check that any two nontrivial subgroups have nontrivial intersection.

Chapter 3 Review Problems

§3.1–3.5

1. (a) What are the possibilities for the order of an element of $\mathbf{Z}_{13}^{\times}$? Explain your answer.

   Solution: The group $\mathbf{Z}_{13}^{\times}$ has order 12, and the order of any element must be a divisor of 12, so the possible orders are 1, 2, 3, 4, 6, and 12.

   (b) Show that $\mathbf{Z}_{13}^{\times}$ is a cyclic group.

   Solution: The first element to try is [2], and we have $2^2 = 4$, $2^3 = 8$, $2^4 = 16 \equiv 3$, $2^5 \equiv 2 \cdot 2^4 \equiv 6$, and $2^6 \equiv 2 \cdot 2^5 \equiv 12$, so the order of [2] is greater than 6. By part (a) it must be 12, and thus [2] is a generator for $\mathbf{Z}_{13}^{\times}$. We could also write this as $\mathbf{Z}_{13}^{\times} = \langle [2]_{13} \rangle$.

2. What is the largest order of an element in $\mathbf{Z}_{12} \times \mathbf{Z}_{18}$? Use your answer to show, in particular, that the group is not cyclic.

   Solution: The order of an element in a direct product is the least common multiple of the orders of its components by Proposition 3.3.4 (b). Since $12 = 2^2 \cdot 3$ and $18 = 2 \cdot 3^2$, we have $\text{lcm}[12, 18] = 2^2 \cdot 3^2 = 36$. The group cannot be cyclic since it has order $12 \cdot 18 = 6 \cdot 36$, and no element could serve as a generator.

3. Find all subgroups of $\mathbf{Z}_{11}^{\times}$, and the diagram showing the inclusions between them.

   Solution: First check for cyclic subgroups, in shorthand notation: $2^2 = 4$, $2^3 = 8$, $2^4 = 5$, $2^5 = 10$, $2^6 = 9$, $2^7 = 7$, $2^8 = 3$, $2^9 = 6$, $2^{10} = 1$. This shows that $\mathbf{Z}_{11}^{\times}$ is cyclic, so the subgroups are as follows, in addition to $\mathbf{Z}_{11}^{\times}$ and $\{[1]\}$: $\langle [2]^2 \rangle = \{[1], [2]^2, [2]^4, [2]^6, [2]^8\} = \{[1], [4], [5], [9], [3]\}$ and $\langle [2]^5 \rangle = \{[1], [2]^5\} = \{[1], [10]\}$ The lattice diagram forms a diamond.

4. Which of the groups listed below are isomorphic to each other?

   $G_1 = \mathbf{Z}_8$, $G_2 = \mathbf{Z}_4 \times \mathbf{Z}_2$, $G_3 = \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$, $G_4 = \mathbf{Z}_{24}^{\times}$, $G_5 = \mathbf{Z}_{30}^{\times}$, $G_6 = D_4$.

   Solution: Each group has 8 elements, so we cannot tell the groups apart by order. But G_6 is not abelian, while the rest *are* abelian, so G_6 cannot be isomorphic to any of the rest.

   The group G_1 is cyclic, but G_2 and G_3 are not, so G_1 is not isomorphic to either G_2 or G_3. In G_2 there is an element of order 4, namely $(1, 0)$, but in G_3 all elements have order 2.

So far we can see that there are four different isomorphism "classes", represented by G_1, G_2, G_3, and G_6. We need to look more deeply at G_4 and G_5. Exercise 3.4.21 proves that if $\gcd(m,n) = 1$, then $\mathbf{Z}_{mn}^\times \cong \mathbf{Z}_m^\times \times \mathbf{Z}_n^\times$. Thus

$$\mathbf{Z}_{24}^\times \cong \mathbf{Z}_3^\times \times \mathbf{Z}_8^\times \cong \mathbf{Z}_2 \times (\mathbf{Z}_2 \times \mathbf{Z}_2) \cong G_3 \ .$$

The isomorphism $\mathbf{Z}_8^\times \cong \mathbf{Z}_2 \times \mathbf{Z}_2$ follows from calculation showing that every element of $\mathbf{Z}_8^\times$ has order 2. Next, we have

$$\mathbf{Z}_{30}^\times \cong \mathbf{Z}_2^\times \times \mathbf{Z}_3^\times \times \mathbf{Z}_5^\times \cong \mathbf{Z}_2 \times \mathbf{Z}_4 \cong G_2 \ .$$

5. Let G be the subset of $\mathrm{GL}_3(\mathbf{R})$ consisting of all matrices of the form $\begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ such that $a, b \in \mathbf{R}$. Show that G is a subgroup of $\mathrm{GL}_3(\mathbf{R})$.

Solution: We have $\begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & c & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+c & b+d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, so the closure property holds. The identity matrix belongs to the set, and $\begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -a & -b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, so the set is closed under taking inverses.

6. Show that the group G in Problem 5 is isomorphic to the direct product $\mathbf{R} \times \mathbf{R}$.

Solution: Define $\phi : G \to \mathbf{R} \times \mathbf{R}$ by $\phi\left(\begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) = (a, b)$. This is one-to-one and onto because it has an inverse function $\theta : \mathbf{R} \times \mathbf{R} \to G$ defined by $\theta((a,b)) = \begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Finally, ϕ preserves the respective operations since

$$\begin{aligned} \phi\left(\begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & c & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) &= \phi\left(\begin{bmatrix} 1 & a+c & b+d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) \\ &= (a+c, b+d) = (a,b) + (c,d) \\ &= \phi\left(\begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) + \phi\left(\begin{bmatrix} 1 & c & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) \ . \end{aligned}$$

§3.6–3.8

7. List the cosets of the cyclic subgroup $\langle 9\rangle$ in $\mathbf{Z}_{20}^{\times}$. Is $\mathbf{Z}_{20}^{\times}/\langle 9\rangle$ cyclic?

Solution: $\mathbf{Z}_{20}^{\times} = \{\pm 1, \pm 3, \pm 7, \pm 9\}$.

$\langle 9\rangle = \{1, 9\}$ $\quad (-1)\langle 9\rangle = \{-1, -9\}$ $\quad 3\langle 9\rangle = \{3, 7\}$ $\quad (-3)\langle 9\rangle = \{-3, -7\}$

Since $x^2 \in \langle 9\rangle$, for each element x of $\mathbf{Z}_{20}^{\times}$, the factor group is not cyclic.

8. Let F be a field, let $G = \mathrm{GL}_2(F)$, let H be the subset of upper triangular matrices in G, and let N be the subset of $\mathrm{GL}_2(F)$ consisting of all matrices of the form $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$.

(a) Show that H is a subgroup of G, but that H is not normal in G.

Solution: The 2×2 identity matrix belongs H, and the product of two invertible upper triangular matrices is easily shown to be an invertible upper triangular matrix. The set H is closed under formation of inverses since if $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in H$, then $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}^{-1} = \begin{bmatrix} a^{-1} & -a^{-1}bd^{-1} \\ 0 & d^{-1} \end{bmatrix} \in H$. The calculation

$$\begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1+1 & 1 \\ -1 & 1 \end{bmatrix}$$

shows that H is not a normal subgroup of G.

(b) Show that N is a normal subgroup of H.

Solution: The set N is nonempty since it contains the identity matrix, and it is a subgroup since $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}\begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}\begin{bmatrix} c^{-1} & -c^{-1}d \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} ac^{-1} & b - ac^{-1}d \\ 0 & 1 \end{bmatrix}$. Furthermore, N is normal in H since $\begin{bmatrix} x & y \\ 0 & z \end{bmatrix}\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}\begin{bmatrix} x & y \\ 0 & z \end{bmatrix}^{-1} =$

$$\begin{bmatrix} xa & xb+y \\ 0 & z \end{bmatrix}\begin{bmatrix} x^{-1} & -x^{-1}yz^{-1} \\ 0 & z^{-1} \end{bmatrix} = \begin{bmatrix} a & -ayz^{-1} + xbz^{-1} + yz^{-1} \\ 0 & 1 \end{bmatrix} \in N.$$

Alternate solution: First prove part (c). Then part (b) follows, since the kernel of any group homomorphism is a normal subgroup.

(c) Show that H/N is isomorphic to the multiplicative group $F^{\times}$.

Solution: Define $\phi : H \to F^{\times}$ by $\phi\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\right) = c$. Then we have

$$\begin{aligned} \phi\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\begin{bmatrix} u & v \\ 0 & w \end{bmatrix}\right) &= \phi\left(\begin{bmatrix} au & av+bw \\ 0 & cw \end{bmatrix}\right) = cw \\ &= \phi\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\right)\phi\left(\begin{bmatrix} u & v \\ 0 & w \end{bmatrix}\right), \end{aligned}$$

and so ϕ is a group homomorphism. Since c can be any nonzero element of F, it follows that ϕ maps H onto $F^\times$, and $\phi\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\right) = 1$ if and only if $c = 1$, so $N = \ker(\phi)$. The fundamental homomorphism theorem implies that $H/N \cong F^\times$.

9. Assume that the dihedral group D_4 is given as $\{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e$, $b^2 = e$, and $ba = a^3b$. Let N be the subgroup $\langle a^2 \rangle = \{e, a^2\}$.

   (a) Show by a direct computation that N is a normal subgroup.

   Solution: We have $a^i a^2 a^{-i} = a^2$ and $(a^i b)a^2(a^i b)^{-1} = a^i a^{-2} b a^i b = a^i a^{-2} a^{-i} b^2 = a^{-2} = a^2$, for all i, which implies that N is normal.

   (b) Is the factor group D_4/N a cyclic group?

   Solution: The cosets of N are $N = \{e, a^2\}$, $Na = \{a, a^3\}$, $Nb = \{b, a^2b\}$, and $Nab = \{ab, a^3b\}$.

   Since b and ab have order 2, and $a^2 \in N$, we see that each coset has order 2 in the factor group, so D_4/N is not cyclic. Note that we therefore have $D_4/N \cong \mathbf{Z}_2 \times \mathbf{Z}_2$.

   (c) Find all subgroups of D_4/N.

   Comment: The subgroups of D_4, and the inclusion relationships between them, can be found in Figure 3.6.6 on page 148 of **Abstract Algebra**.

   Solution: By Proposition 3.8.7 (b), the subgroups of D_4/N are in one-to-one correspondence with the subgroups of D_4 that contain N. These subgroups can be shown to be N itself, $\{e, a^2, b, a^2b\} = H_1$, $\{e, a, a^2, a^3\} = H_2$, $\{e, a^2, ab, a^3b\} = H_3$, and D_4.

   Let's only look at the proper nontrivial subgroups of D_4/N. Under the correspondence defined in Proposition 3.8.7, we must find the cosets that correspond to these elements. The subgroup H_1 collapses from four elements in D_4 to two elements in D_4/N: the cosets N and bN. The subgroup H_2 will correspond to the subgroup of D_4/N consisting of the cosets N and aN, while the subgroup H_3 collapses to $\{N, abN\}$.

   Comment: We should have expected to find three proper nontrivial subgroups with two elements each, since that is what we would find in the Klein 4-group $\mathbf{Z}_2 \times \mathbf{Z}_2$ to which D_4/N is isomorphic.

10. Let $G = D_8$, and let $N = \{e, a^2, a^4, a^6\}$.

    (a) List all left cosets and all right cosets of N, and verify that N is a normal subgroup of G.

    Solution: The right cosets of N are

    $N = \{e, a^2, a^4, a^6\}$, $\quad Na = \{a, a^3, a^5, a^7\}$,

    $Nb = \{b, a^2b, a^4b, a^6b\}$, $\quad Nab = \{ab, a^3b, a^5b, a^7b\}$.

    The left cosets of N are more trouble to compute, but we get

    $N = \{e, a^2, a^4, a^6\}$, $\quad aN = \{a, a^3, a^5, a^7\}$,

    $bN = \{b, a^6b, a^4b, a^2b\}$, $\quad abN = \{ab, a^7b, a^5b, a^3b\}$.

The fact that the left and right cosets of N coincide shows that N is normal.

(b) Show that G/N has order 4, but is not cyclic.

Solution: It is clear that there are 4 cosets. We have $NaNa = Na^2 = N$, $NbNb = Ne = N$, and $NabNab = Ne = N$, so each coset has order 2.

11. (a) Show that $\mathbf{R}^\times/\mathbf{R}^+$ is cyclic of order 2.

Solution: The subgroup $\mathbf{R}^+$ has two cosets: $\mathbf{R}^+$ and $(-1)\mathbf{R}^+$.

(b) Let H be a subgroup of $\mathbf{R}^\times$ that contains $\mathbf{R}^+$. Show that either $H = \mathbf{R}^\times$ or $H = \mathbf{R}^+$.

Solution: This follows from part (a) and Proposition 3.8.7 (b).

12. (a) Show that every element of the group $\mathbf{Q}/\mathbf{Z}$ has finite order.

Solution: Since $\mathbf{Q}$ is abelian, the subgroup $\mathbf{Z}$ is normal, and so we can form the cosets $\frac{m}{n} + \mathbf{Z}$ of $\mathbf{Z}$ with no difficulty, where for simplicity we assume that $n > 0$. To add $\frac{m}{n} + \mathbf{Z}$ to itself n times, we add the representative $\frac{m}{n}$ to itself n times, which gives us $m \in \mathbf{Z}$. Thus $\frac{m}{n} + \mathbf{Z}$ added to itself n times gives us the identity coset, which shows that the order of $\frac{m}{n} + \mathbf{Z}$ is a divisor of n.

(b) Show that for each $n \in \mathbf{Z}^+$, the group $\mathbf{Q}/\mathbf{Z}$ contains an element of order n.

Solution: It follows from the argument in part (a) that $\frac{1}{n} + \mathbf{Z}$ has order n.

Chapter 4

Polynomials

4.1 Fields; Roots of Polynomials

25. Let F be a field, and let $f(x), g(x) \in F[x]$ be polynomials of degree less than n. Assume that $f(x)$ agrees with $g(x)$ on n distinct elements of F. (That is, $f(x_i) = g(x_i)$ for distinct elements $x_1, \ldots, x_n \in F$.) Prove that $f(x) = g(x)$ (as polynomials).

    Solution: Look at the polynomial $p(x) = f(x) - g(x)$. It is either zero or has degree less than n. The given condition shows that $p(x)$ has n distinct roots in F, given by $x_1, \ldots, x_n$. This contradicts Corollary 4.1.12 unless $p(x) = 0$ is the zero polynomial, and so we must have $f(x) = g(x)$.

26. Let $c \in F$ and let $f(x) \in F[x]$. Show that $r \in F$ is a root of $f(x)$ if and only if $r - c$ is a root of $f(x + c)$.

    Solution: Let $g(x) = f(x+c)$ be the polynomial we get after making the substitution of $x + c$ in place of x. If r is a root of $f(x)$, then $f(r) = 0$, and so substituting $r - c$ into $g(x)$ gives us $g(r - c) = f(r - c + c) = f(r) = 0$. Conversely, if $r - c$ is a root of $g(x)$, then $g(r - c) = 0$, so $f(r) = f(r - c + c) = g(r - c) = 0$ and r is a root of $f(x)$.

27. For $f(x) = x^3 - 5x^2 - 6x + 2 \in \mathbf{Q}[x]$, use the method of Theorem 4.1.9 to write $f(x) = q(x)(x + 1) + f(-1)$.

    Solution: We have $f(-1) = -1 - 5 + 6 + 2 = 2$. Therefore

$$\begin{aligned} f(x) - f(-1) &= (x^3 - (-1)^3) - 5(x^2 - (-1)^2) - 6(x - (-1)) + (2 - 2) \\ &= (x + 1)((x^2 - x + 1) - 5(x - 1) - 6) \;=\; (x + 1)(x^2 - 6x)\ , \end{aligned}$$

    and so $f(x) = (x^2 - 6x)(x + 1) + 2$.

28. For $f(x) = x^3 - 2x^2 + x + 3 \in \mathbf{Z}_7[x]$, use the method of Theorem 4.1.9 to write $f(x) = q(x)(x - 2) + f(2)$.

    Solution: For simplicity, we will just write a for the elements of $\mathbf{Z}_7$, rather than $[a]_7$. We have $f(2) = 8 - 8 + 2 + 3 = 5$. Therefore

$$\begin{aligned} f(x) - f(2) &= (x^3 - (2)^3) - 2(x^2 - (2)^2) + (x - 2) + (3 - 3) \\ &= (x - 2)((x^2 + 2x + 4) - 2(x + 2) + 1) \;=\; (x - 2)(x^2 + 1)\ , \end{aligned}$$

and so $f(x) = (x^2+1)(x-2)+5$.

29. Show that the set of matrices of the form $\begin{bmatrix} a & b \\ -3b & a \end{bmatrix}$, where $a, b \in \mathbf{Q}$, is a field under the operations of matrix addition and multiplication.

Solution: Since a linear algebra course is a prerequisite for this text, it is fair to assume that the associative and distributive laws hold for matrix addition and multiplication. It is also true that addition is commutative, though multiplication need not satisfy the commutative law. To check that we have a field, it is sufficient to check the closure properties, the existence of identities and inverses, and commutativity of multiplication.

(i) Closure of + and $\cdot$:

$$\begin{bmatrix} a & b \\ -3b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -3d & c \end{bmatrix} = \begin{bmatrix} (a+c) & (b+d) \\ -3(b+d) & (a+c) \end{bmatrix} \in F$$

$$\begin{bmatrix} a & b \\ -3b & a \end{bmatrix} \begin{bmatrix} c & d \\ -3d & c \end{bmatrix} = \begin{bmatrix} (ac-3bd) & (ad+bc) \\ -3(ad+bc) & (ac-3bd) \end{bmatrix} \in F$$

(iii) In the given set, multiplication is commutative:

$$\begin{bmatrix} a & b \\ -3b & a \end{bmatrix} \begin{bmatrix} c & d \\ -3d & c \end{bmatrix} = \begin{bmatrix} ac-3bd & ad+bc \\ -3(ad+bc) & ac-3bd \end{bmatrix} = \begin{bmatrix} c & d \\ -3d & c \end{bmatrix} \begin{bmatrix} a & b \\ -3b & a \end{bmatrix}.$$

(v) Identity Elements: The matrices $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ belong to F and are the identity elements.

(vi) Inverse Elements: The negative of $\begin{bmatrix} a & b \\ -3b & a \end{bmatrix}$ is $\begin{bmatrix} -a & -b \\ -3(-b) & -a \end{bmatrix} \in F$. If the matrix $\begin{bmatrix} a & b \\ -3b & a \end{bmatrix}$ is nonzero, then at least one of a or b is nonzero, so the determinant a^2+3b^2 is nonzero since $\sqrt{3}$ is not a rational number. The standard formula for the inverse of a 2×2 matrix yields $\begin{bmatrix} a & b \\ -3b & a \end{bmatrix}^{-1} = \dfrac{1}{a^2+3b^2} \begin{bmatrix} a & -b \\ -3(-b) & a \end{bmatrix}^{-1} \in F$.

30. Prove that if p is a prime number, then the multiplicative group $\mathbf{Z}_p^\times$ is cyclic.

Solution: We will use Proposition 3.5.9 (b), which states that a finite abelian group is cyclic if and only if its exponent is equal to its order. Suppose that the exponent of $\mathbf{Z}_p^\times$ is m. Then $a^m = 1$ for all nonzero $a \in \mathbf{Z}_p^\times$, and so the polynomial $x^m - 1$ has $p-1$ distinct roots in $\mathbf{Z}_p^\times$. It follows from Corollary 4.1.12 that $m = p-1$, and so $\mathbf{Z}_p^\times$ must be cyclic.

31. Let p be a prime number, and let $a, b \in \mathbf{Z}_p^\times$. Show that if neither a nor b is a square, then ab *is* a square.

Solution: By Problem 30, we can choose a generator α for $\mathbf{Z}_p^\times$. If neither a nor b is a square, then $a = \alpha^s$ and $b = \alpha^t$, where s and t are odd. Therefore $ab = (\alpha^k)^2$, where $s + t = 2k$, and so ab is a square.

32. Use the method of divided differences to find the polynomial of degree 2 whose graph passes through $(0, 5)$, $(1, 7)$, and $(-1, 9)$.

Solution: Let $p(x)$ be the polynomial we are looking for. We get the following table of differences, where the entry in the 3rd column is $\frac{2-(-4)}{1-(-1)}$.

n	$p(n)$		
1	7		
		2	
0	5		3
		-4	
-1	9		

This gives us the polynomial $p(x) = 9 + (-4)(x - (-1)) + 3(x - (-1))(x - 0)$
$= 9 - 4x - 4 + 3x^2 + 3x = 3x^2 - x + 5$. Check: $p(0) = 5$, $p(1) = 7$, $p(-1) = 9$.

33. Use the method of divided differences to find a formula for $\sum_{i=1}^n i^2$.

Solution: We know that $1+2+\cdots+n = n(n+1)/2$. This suggests that the formula for the sum of squares might be a cubic polynomial in n. Let's write $p(n) = \sum_{i=0}^n i^2$. Then $p(0) = 0$, $p(1) = 0^2+1^2 = 1$, $p(2) = 0^2+1^2+2^2 = 5$, and $p(3) = 0^2+1^2+2^2+3^2 = 14$. We get the following table of differences.

n	$p(n)$			
3	14			
		9		
2	5		5/2	
		4		1/3
1	1		3/2	
		1		
0	0			

This gives the polynomial $p(n) = 0+1(n-0)+\frac{3}{2}(n-0)(n-1)+\frac{1}{3}(n-0)(n-1)(n-2) = n(1 + \frac{3}{2}n - \frac{3}{2} + \frac{1}{3}n^2 - n + \frac{2}{3} = \frac{1}{6}n(2n^2 + 3n + 1)$, which simplifies to the well-known formula $p(n) = \frac{1}{6}n(n + 1)(2n + 1)$.

ANSWERS AND HINTS

34. Find the number of elements $a \in \mathbf{Z}_p$ for which $x^2 - a$ has a root in $\mathbf{Z}_p$.
Answer: $(p + 1)/2$

39. Use the method of divided differences to find the cubic polynomial whose graph passes through the points $(0, -5)$, $(1, -3)$, $(-1, -11)$, and $(2, 1)$.
Answer: $1 + 4(x - 2) + 1(x - 2)(x - 1) + 1(x - 2)(x - 1)(x - 0) = -5 + 3x - 2x^2 + x^3$

41. Use the method of divided differences to verify the formula for $\sum_{i=1}^{n} i^3$.
Answer: $n + \frac{7}{2}n(n-1) + 2n(n-1)(n-2) + \frac{1}{4}n(n-1)(n-2)(n-3) = \frac{1}{4}n^2(n+1)^2$

42. Let F be a finite field, and let $f(x) : F \to F$ be any function. Prove that there exists a polynomial $p(x) \in F[x]$ such that $f(a) = p(a)$ for all $a \in F$.
Hint: Use the Lagrange interpolation formula.

4.2 Factors

21. Over the field of rational numbers, use the Euclidean algorithm to show that $2x^3 - 2x^2 - 3x + 1$ and $2x^2 - x - 2$ are relatively prime.

Let $2x^3 - 2x^2 - 3x + 1 = f(x)$ and $2x^2 - x - 2 = g(x)$.

Solution: Using the division algorithm to divide $f(x)$ by $g(x)$, we obtain $f(x) = (x - \frac{1}{2})g(x) - \frac{3}{2}x$ as the first step. At the next step we can use x rather than $\frac{3}{2}x$, and then dividing $g(x)$ by x gives us $g(x) = (2x-1)\cdot(x) - 2$. The constant remainder at this step shows that $\gcd(f(x), g(x)) = \gcd(g(x), x) = 1$.

22. Over the field of rational numbers, find the greatest common divisor of $x^3 - 1$ and $x^4 + x^3 + 2x^2 + x + 1$, and express it as a linear combination of the given polynomials.

Solution: Let $x^4 + x^3 + 2x^2 + x + 1 = f(x)$ and $x^3 - 1 = g(x)$. From the division algorithm we first obtain $f(x) = (x+1)g(x) + 2(x^2 + x + 1)$, and then the next step yields $g(x) = (x-1)(x^2 + x + 1)$, so $\gcd(f(x), g(x)) = x^2 + x + 1$. Solving the first equation for the remainder shows that $(x^2 + x + 1) = \frac{1}{2}f(x) - \frac{1}{2}(x+1)g(x)$.

23. Find the greatest common divisor of $x^3 - 2x + 1$ and $x^2 - x - 2$ in $\mathbf{Z}_5[x]$, and express it as a linear combination of the given polynomials.

Solution: Rather than using the standard congruence classes $0, 1, 2, 3, 4$ in $\mathbf{Z}_5$, we will use $0, \pm 1, \pm 2$, and in the computations we will reduce coefficients at each step. (For simplicity, we are omitting the brackets in the congruence class notation.)

Let $x^3 - 2x + 1 = f(x)$ and $x^2 - x - 2 = g(x)$. Using the division algorithm to divide $f(x)$ by $g(x)$, we get $f(x) = (x+1)g(x) + x - 2$.

$$
\begin{array}{rr|rrr}
 & & & x & +1 \\
\cline{3-5}
x^2 - x - 2 & & x^3 & -2x & +1 \\
 & & x^3 - x^2 & -2x & \\
\cline{3-5}
 & & x^2 & & +1 \\
 & & x^2 & -x & -2 \\
\cline{3-5}
 & & & x & -2
\end{array}
$$

The next step yields $g(x) = (x-1)(x-2)$, so $\gcd(f(x), g(x)) = x - 2$. Solving the first equation for the remainder shows that $x - 2 = f(x) - (x+1)g(x)$.

24. (a) Express $x^4 + x$ as a product of polynomials irreducible over $\mathbf{Z}_5$.

Solution: In general, we have $x^4 + x = x(x^3 + 1) = x(x + 1)(x^2 - x + 1)$. The factor $p(x) = x^2 - x + 1$ is irreducible over $\mathbf{Z}_5$ since it can be checked that it has no roots in $\mathbf{Z}_5$. (We get $p(0) = 1$, $p(1) = 1$, $p(-1) = 3$, $p(2) = 3$, $p(-2) = 2$.)

(b) Show that $x^3 + 2x^2 + 3$ is irreducible over $\mathbf{Z}_5$.

Solution: For $p(x) = x^3 + 2x^2 + 3$, we have $p(0) = 3$, $p(1) = 1$, $p(-1) = -1$, $p(2) = 4$, and $p(-2) = 3$, so $p(x)$ is irreducible over $\mathbf{Z}_5$ since it has no roots in $\mathbf{Z}_5$.

25. Express $2x^3 + x^2 + 2x + 2$ as a product of polynomials irreducible over $\mathbf{Z}_5$.

Solution: We first factor out 2, using $(2)(-2) = -4 \equiv 1 \pmod 5$. This reduces the question to factoring $p(x) = x^3 - 2x^2 + x + 1$. (We could also multiply each term by 3.) Checking for roots shows that $p(0) = 1$, $p(1) = 1$, $p(-1) = -3$, $p(2) = 3$, and $p(-2) \equiv -2$, so $p(x)$ itself is irreducible over $\mathbf{Z}_5$ since it has no roots in $\mathbf{Z}_5$.

26. Factor $x^4 + 2$ over $\mathbf{Z}_3$.

Solution: If we replace 2 with the congruent number -1, we get $x^4 + 2 = x^4 - 1 = (x^2-1)(x^2+1) = (x-1)(x+1)(x^2+1)$. Since x^2+1 has no root in $\mathbf{Z}_3$, it is irreducible over $\mathbf{Z}_3$. Using the standard congruence classes for $\mathbf{Z}_3$, we have the factorization $x^4 + 2 = (x + 1)(x + 2)(x^2 + 1)$.

27. Factor $x^4 + 1$ over $\mathbf{Z}_2$, over $\mathbf{Z}_5$, over $\mathbf{Z}_7$, and over $\mathbf{Z}_{11}$.

Solution: Over $\mathbf{Z}_2$, we have $x^4 + 1 = (x^2 + 1)(x^2 - 1) = (x + 1)^4$, and so 1 is a root with multiplicity 4.

Over $\mathbf{Z}_5$, check that there are no roots. For the factorization, we get $(x^2-2)(x^2+2) = x^4 - 4 \equiv x^4 + 1$.

Over $\mathbf{Z}_7$, there are no roots. We get $(x^2+3x+1)(x^2-3x+1) = x^4-7x^2+1 \equiv x^4+1$.

Over $\mathbf{Z}_{11}$, there are no roots. We get $(x^2+3x-1)(x^2-3x-1) = x^4-11x^2+1 \equiv x^4+1$.

Note that since $x^4 + 1$ has no roots in $\mathbf{Z}_5$, $\mathbf{Z}_7$, or $\mathbf{Z}_{11}$, it's irreducible factors over those fields must be quadratic, and thus the quadratic factors given above must be the irreducible factors of $x^4 + 1$.

Comment: Yes, there is a pattern to these factorizations. In Problem 40 you are asked to find a method to factor $x^4 + 1$ over $\mathbf{Z}_p$.

28. Find a polynomial $q(x)$ such that $(a + bx)q(x) \equiv 1 \pmod{x^2 + 1}$ over $\mathbf{Z}_3$.

Solution: A quick calculation shows that x^2+1 has no roots in $\mathbf{Z}_3$, so it is irreducible in $\mathbf{Z}_3[x]$. This means that we can use the Euclidean algorithm to find $q(x)$, since it follows that $\gcd((a + bx), x^2 + 1) = 1$.

If both a and b are zero, there is no solution. If $b = 0$ and $a \neq 0$, then we can take $q(x)$ to be the constant polynomial a^{-1}. Thus we can assume that $b \neq 0$. Then we need to find a linear combination $q(x)(a+bx) + s(x)(x^2+1)$ of $a+bx$ and x^2+1 that is equal to 1. The answer $q(x)$ will be a multiplicative inverse in the set of congruence classes of $\mathbf{Z}_3[x]$ modulo $x^2 + 1$. The first step is to divide $bx + a$ into $x^2 + 1$.

$$\begin{array}{rr|ll} & & b^{-1}x & -ab^{-2} \\ \hline bx+a & x^2 & & +1 \\ & x^2 & +ab^{-1}x & \\ \hline & & -ab^{-1}x & +1 \\ & & -ab^{-1}x & -a^2b^{-2} \\ \hline & & & 1+a^2b^{-2} \end{array}$$

Thus we get $x^2+1 = (b^{-1}x-ab^{-2})(bx+a)+(1+a^2b^{-2})$. Multiplying both sides of the equation by b^2 and rearranging the terms gives us $(a+bx)(a-bx)+b^2(x^2+1) = a^2+b^2$. In $\mathbf{Z}_3$, we must have $b^2 = 1$, since $b \neq 0$, and then for all possible values of a we have $a^2+b^2 \neq 0$, so $(a^2+b^2)^{-1}$ exists in $\mathbf{Z}_3$. Multiplying both sides by $(a^2+b^2)^{-1}$, we get $(a+bx)(a^2+b^2)^{-1}(a-bx) + (a^2+b^2)^{-1}b^2(x^2+1) = 1$. We finally have the answer: the multiplicative inverse of $a+bx$ is $(a^2+b^2)^{-1}(a-bx)$.

Note: Compare this answer with the one you get when you compute $(a+bi)^{-1}$ in $\mathbf{C}$.

Alternate solution: We know that $x^2+1 \equiv 0 \pmod{x^2+1}$, so the easiest way to calculate the product of two congruence classes $a+bx$ and $c+dx$ modulo x^2+1 (over the field $\mathbf{Z}_3$) is to take the product $(a+bx)(c+dx) = ac+(ad+bc)x+bdx^2$ and substitute -1 for x^2, since they represent congruent polynomials. This give $(a+bx)(c+dx) \equiv (ac-bd)+(ad+bc)x \pmod{x^2+1}$.

Now we can solve the equation $(a+bx)(c+dx) \equiv 1 \pmod{x^2+1}$. (Can we really guarantee that the answer has to be a linear polynomial? Yes, since every polynomial is congruent to its remainder on division by x^2+1, and these never have degree larger than 1.) This leads to two equations in the two unknowns c and d. We get $bc+ad = 0$ and $ac-bd = 1$; multiplying the first by b and the second by a allows us to solve for c. As above we can reduce to the case $b \neq 0$, and then we get $c = a(a^2+b^2)^{-1}$ and $d = -b(a^2+b^2)^{-1}$.

29. Let F be a field, and let $f(x), g(x) \in F[x]$, with $\deg(f(x) = n$ and $\deg(g(x) = m$, where $m < n \in \mathbf{Z}^+$. Write $n = qm+r$, where $r = 0$ or $r < m$. Show that there exist polynomials $r_0(x), r_1(x), \ldots, r_q(x)$ such $f(x) = r_q(x)g(x)^q + \ldots + r_1(x)g(x) + r_0(x)$, where $\deg(r_i(x)) < m$ for $0 \leq i \leq q$.

Solution: (Outline only) Use the division algorithm to write $f(x) = q(x)g(x)^q + r(x)$, where $r(x) = 0$ or $\deg(r(x)) < mq$. It follows that $\deg(q(x)) < m$ since $\deg(q(x)) = r < m$. Continue by induction, repeating this process with $r(x)$ in place of $f(x)$.

30. Let F be a field, and let $f(x) \in F[x]$. Prove that $f(x)$ is irreducible over F if and only if $f(x+c)$ is irreducible over F.

Solution: Suppose that $f(x)$ is irreducible, but $f(x+c) = p(x)q(x)$ can be factored into a product of polynomials of degree less than $\deg(f(x))$. Then substituting $x-c$ for x gives a proper factorization $f(x) = p(x-c)q(x-c)$, a contradiction. Thus $f(x+c)$ is irreducible.

A similar proof shows the converse. Both directions depend on the fact that you get the same answer when you first substitute and then multiply as when you multiply first and then substitute.

ANSWERS AND HINTS

33. Over $\mathbf{Z}_3$, find $\gcd(x^5-x^4+x^3-x^2,\ x^3-x^2+x-1)$ and write it as a linear combination of the given polynomials.
Hint: The gcd is x^3-x^2+x-1.

34. Over $\mathbf{Z}_5$, find $\gcd(x^5+x^4-2x^3-x^2+2x-2,\ x^3-x^2+x-1)$ and write it as a linear combination of the given polynomials.
Hint: The gcd is x^2+1.

35. Over $\mathbf{Z}_7$, find $\gcd(x^5+3x^4-2x^3-3x-3,\ x^3-x^2+x-1)$ and write it as a linear combination of the given polynomials.
Hint: The gcd is x^2+1.

36. Over $\mathbf{Q}$, find $\gcd(x^5-8x^4+25x^3-38x^2+28x-8,\ x^5-x^4-2x^3+2x^2+x-1)$ and write it as a linear combination of the given polynomials.
Hint: The gcd is x^2-2x+1.

39. Factor x^3+6 over $\mathbf{Z}_7$.
Hint: $x^3+6 \equiv x^3-1 \pmod 7$

40. Show that x^4+1 has a proper factorization over $\mathbf{Z}_p$, for all primes p.
Hint: If there exists $b \in \mathbf{Z}_p^\times$ with $b^2=-1$, then $x^4+1=(x^2-b)(x^2+b)$. If there exists $a \in \mathbf{Z}_p^\times$ with $a^2=2$, then $x^4+1=(x^2+ax+1)(x^2-ax+1)$. If there exists $a \in \mathbf{Z}_p^\times$ with $a^2=-2$, then $x^4+1=(x^2+ax-1)(x^2-ax-1)$. Use Problem 4.1.31 to show that one of these cases must occur. (Compare the answers to Problem 27.)

4.3 Existence of Roots

25. Show that the field $F=\left\{\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| a,b \in \mathbf{R}\right\}$ defined in Exercise 4.1.13 is isomorphic to the field of complex numbers.

Solution: Define $\phi\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) = a+bi$. The following calculations show that ϕ respects multiplication.

$$\phi\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ -d & c \end{bmatrix}\right) = \phi\left(\begin{bmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{bmatrix}\right) = (ac-bd)+(ad+bc)i$$

$$\phi\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right)\phi\left(\begin{bmatrix} c & d \\ -d & c \end{bmatrix}\right) = (a+bi)(c+di) = (ac+bdi^2)+(ad+bc)i$$
$$= (ac-bd)+(ad+bc)i$$

It is clear that ϕ is one-to-one and onto and respects addition, so ϕ is an isomorphism.

Comment: Appendix 5 of **Abstract Algebra** contains more details.

26. Show that $\mathbf{Q}(\sqrt{3}i) = \{a + b\sqrt{3}i \mid a, b \in \mathbf{Q}\}$ is a field isomorphic to $\mathbf{Q}[x]/\langle x^2 + 3\rangle$.

Comment: In the course of defining the appropriate function, we will show that $\mathbf{Q}(\sqrt{3}i)$ is a field.

Solution: By Proposition 4.3.3, each congruence class in $\mathbf{Q}[x]/\langle x^2 + 3\rangle$ contains a unique representative of the form $a+bx$, with $a, b \in \mathbf{Q}$. Define $\phi : \mathbf{Q}[x]/\langle x^2 + 3\rangle \to \mathbf{C}$ by $\phi([a + bx]) = a + b\sqrt{3}i$. Since $[a + bx] = [c + dx]$ implies that $a = c$ and $b = d$, it follows that ϕ is a well-defined function.

If $\phi([a + bx]) = \phi([c + dx])$, then $a + b\sqrt{3}i = c + d\sqrt{3}i$, and so $a - c = (d - b)\sqrt{3}i$. Since $\sqrt{3}i \notin \mathbf{Q}$, the only way this can happen is if $a - c = 0$ and $d - b = 0$. Then $a = c$ and $b = d$, so $[a + bx] = [c + dx]$, and thus ϕ is one-to-one. The set $\mathbf{Q}(\sqrt{3}i)$ is the image of ϕ, so ϕ maps $\mathbf{Q}[x]/\langle x^2 + 3\rangle$ onto $\mathbf{Q}(\sqrt{3}i)$

In calculating the product $[a + bx][c + dx]$, we get $[ac + (ad + bc)x + bdx^2]$, and to reduce this to standard form we can make the substitution $x^2 = -3$, since $x^2 + 3 \equiv 0 \pmod{x^2 + 3}$. Thus $[a + bx][c + dx] = [(ac - 3bd) + (ad + bc)x]$. We then have the following calculations.

$$\begin{aligned} \phi([a + bx] + [c + dx]) &= \phi([(a + c) + (b + d)x]) \;=\; (a + c) + (b + d)\sqrt{3}i \\ &= (a + b\sqrt{3}i) + (c + d\sqrt{3}i) \;=\; \phi([a + bx]) + \phi([c + dx]) \end{aligned}$$

$$\begin{aligned} \phi([a + bx][c + dx]) &= \phi([(ac - 3bd) + (ad + bc)x]) \;=\; (ac - 3bd) + (ad + bc)\sqrt{3} \\ &= (a + b\sqrt{3}i)(c + d\sqrt{3}i) \;=\; \phi([a + bx])\phi([c + dx]) \end{aligned}$$

Because $\phi : \mathbf{Q}[x]/\langle x^2 + 3\rangle \to Q(\sqrt{3}i)$ is a one-to-one correspondence that respects addition and multiplication, it transfers the properties of a field to $Q(\sqrt{3}i)$, and so we do not need to go through the verification of all of the field axioms for the set $Q(\sqrt{3}i)$. It follows that ϕ is an isomorphism of fields.

27. Show that the following set of matrices, with entries from $\mathbf{Z}_3$, is a field isomorphic to $\mathbf{Z}_3[x]/\langle x^2 + 1\rangle$.

$$\left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ -1 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 1 & -1 \end{bmatrix} \right\} = F$$

Solution: (This is just an outline of the solution.) Define $\phi : \mathbf{Z}_3[x]/\langle x^2 + 1\rangle \to F$ by $\phi([a + bx]) = a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. The mapping is well-defined since each congruence class contains a unique representative of the form $a+bx$, and simply listing the possible values of ϕ shows it to be a one-to-one correspondence. It is clear that ϕ will preserve addition. That ϕ preserves multiplication depends on the fact that the congruence class $[x]$, which satisfies the equation $[x]^2 = -[1]$, maps to the matrix $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, which satisfies the corresponding equation $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^2 = -\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

28. Construct a field with 25 elements.

Solution: We will construct a field of the form $F[x]/\langle p(x)\rangle$. The fact that $25 = 5^2$ shows that we need to take $F = \mathbf{Z}_5$, and that $p(x)$ must be an irreducible polynomial of degree 2. A bit of trial and error (checking for roots in $\mathbf{Z}_5$) identifies $x^2 + x + 1$ as one of the possible choices for a polynomial of degree 2 irreducible in $\mathbf{Z}_5[x]$.

The field $\mathbf{Z}_5[x]/\langle x^2 + x + 1\rangle$ has 25 elements, as required. We should also give the identity necessary to reduce products $[a + bx][c + dx]$ to standard form:

$x^2 \equiv -x - 1 \pmod{x^2 + x + 1}$.

29. Find all powers of $[x]$ in $\mathbf{Z}_3[x]/\langle x^2 + x - 1\rangle$, and then find $[x]^{-1}$.

Solution: Since $x^2 \equiv 1 - x \pmod{x^2 + x - 1}$, we have the following list:

$[x]^0 = [1]$, $[x]^1 = [x]$, $[x]^2 = [1-x]$, $[x]^3 = [x][1-x] = [x-x^2] = [x-(1-x)] = [-1-x]$, $[x]^4 = [x][-1 - x] = [-x - x^2] = [-x - (1 - x)] = [-1]$, $[x]^5 = [-x]$, $[x]^6 = [-x^2] = [-1 + x]$, $[x]^7 = [x]^4[x]^3 = [1 + x]$, $[x]^8 = ([x]^4)^2 = [1]$.

Since $[x]$ has order 8 in the multiplicative group of the field, its inverse is $[x]^7 = [1+x]$.

Comment: Each nonzero element of $\mathbf{Z}_3/\langle x^2 + x - 1\rangle$ is a power of $[x]$, so we have shown that the multiplicative group of this finite field is cyclic, with generator $[x]$.

30. In $\mathbf{Z}_2[x]/\langle x^3 + x + 1\rangle$, find the multiplicative inverse of $[x + 1]$.

Solution: We first give a solution using the Euclidean algorithm. For $p(x) = x^3+x+1$ and $f(x) = x+1$, the first step of the Euclidean algorithm gives $p(x) = (x^2+x)f(x)+1$. Thus $p(x)-(x^2+x)f(x) = 1$, and so reducing modulo $p(x)$ gives $[-x^2-x][f(x)] = [1]$, and therefore $[x + 1]^{-1} = [-x^2 - x] = [x^2 + x]$.

Alternate Solution: We next give a solution that uses the identity $[x^3] = [x + 1]$ to solve a system of equations. We need to solve $[1] = [x + 1][ax^2 + bx + c]$ or

$$\begin{aligned}
[1] &= [ax^3 + bx^2 + cx + ax^2 + bx + c] \\
&= [ax^3 + (a + b)x^2 + (b + c)x + c] \\
&= [a(x + 1) + (a + b)x^2 + (b + c)x + c] \\
&= [(a + b)x^2 + (a + b + c)x + (a + c)] \ ,
\end{aligned}$$

so we need $a + b \equiv 0 \pmod 2$, $a + b + c \equiv 0 \pmod 2$, and $a + c \equiv 1 \pmod 2$. This gives $c \equiv 0 \pmod 2$, and therefore $a \equiv 1 \pmod 2$, and then $b \equiv 1 \pmod 2$. Again, we see that $[x + 1]^{-1} = [x^2 + x]$.

31. Is $[x]$ a generator of the multiplicative group of the field $\mathbf{Z}_5[x]/\langle x^2 + x + 1\rangle$? Is $[1+x]$ a generator?

Comment: This is the field defined in the solution to Problem 28.

Solution: The field has 25 elements, so its multiplicative group has 24 elements, and $[x]$ is a generator if and only if it has order 24. We have $x^2 \equiv -1-x \pmod{x^2+x+1}$, so $[x]^3 = [x][-1 - x] = [-x - x^2] = [-x - (-x - 1)] = [-x + x + 1] = [1]$. Thus $[x]$ has order 3, so it is not a generator.

Since $1+x \equiv -x^2 \pmod{x^2+x+1}$, we have $[1+x]^2 = [x]$ and $[1+x]^3 = -[x]^6 = -([x]^3)^2 = -[1]$. Thus $[1+x]^6 = [1]$, but no smaller power is the identity, showing that $[1+x]$ has order 6, so it is not a generator.

32. Show that x^4+x+1 is irreducible over $\mathbf{Z}_2$. Factor x^4+x+1 over $\mathbf{Z}_2[x]/\langle x^4+x+1\rangle$.

Comment: This question could be quite confusing. The expression x^4+x+1 is first of all an element of $\mathbf{Z}_2[x]$. It is used to construct a field $F = \mathbf{Z}_2[x]/\langle x^4+x+1\rangle$. Then it is regarded as an element of $F[x]$, and has to be factored in $F[x]$. To try to clarify the situation, we will use α to denote the congruence class of x in F.

Some of the calculations may also look confusing, because we will use the following shortcut. Since we are dealing with cosets of polynomials whose coefficients come from $\mathbf{Z}_2$, for $a, b \in F$ we have $2ab = 0$, and therefore $(a+b)^2 = a^2 + b^2$.

Solution: The answer to Exercise 4.2.12 (given in the text) states that $p(x) = x^4+x+1$ is irreducible over $\mathbf{Z}_2$. For the sake of completeness, we should still write out a proof here. It is easy to see that $p(x)$ has no roots in $\mathbf{Z}_2$, so it has no linear factors in $\mathbf{Z}_2[x]$. Can it be the product of two quadratic factors? The only irreducible quadratic in $\mathbf{Z}_2[x]$ is x^2+x+1, since the other three quadratics all have roots. (Here is the list: x^2, x^2+1, x^2+x.) Since $(x^2+x+1)^2 = x^4+x^2+1$, we have $x^4+x+1 \neq (x^2+x+1)^2$, so x^4+x+1 is irreducible over $\mathbf{Z}_2$, and $\mathbf{Z}_2[x]/\langle x^4+x+1\rangle$ is a field.

In $F = \mathbf{Z}_2[x]/\langle x^4+x+1\rangle$, let $[x] = \alpha$. Then F has $2^4 = 16$ elements, which have the general form $a + b\alpha + c\alpha^2 + d\alpha^3$, where $a, b, c, d \in \mathbf{Z}_2$. We will show that there are 4 roots of x^4+x+1 in F, given by the cosets corresponding to α, α^2, $\alpha+1$, and α^2+1. Remember that $x^4+x+1 \equiv 0$, so $x^4 \equiv x+1$.

To check that the above cosets are roots, We have

$\alpha^4 + \alpha + 1 = [x^4+x+1] \equiv 0$,

$(\alpha^2)^4 + (\alpha^2) + 1 = [x^4]^2 + [x^2] + [1] \equiv [x+1]^2 + [x^2+1] \equiv [x^2+1+x^2+1] \equiv 0$,

$(\alpha+1)^4 + (\alpha+1) + 1 \equiv [x+1]^4 + \alpha \equiv [x^4+1+x] \equiv 0$, and

$(\alpha^2+1)^4 + (\alpha^2+1) + 1 \equiv (\alpha^4)^2 + 1 + \alpha^2 \equiv [x+1]^2 + [1+x^2] \equiv [x^2+1+1+x^2] \equiv 0$.

Thus x^4+x+1 factors as a product of 4 linear terms. Remembering that over $\mathbf{Z}_2$ we have $-1 \equiv 1$, we get $x^4+x+1 = (x+\alpha)(x+\alpha^2)(x+\alpha+1)(x+\alpha^2+1)$.

ANSWERS AND HINTS

33. Factor $f(x) = x^5 - x^4 + x^3 - x^2$ and $g(x) = x^3 - x^2 + x - 1$ over $\mathbf{Z}_3$ and use the factorizations to find their greatest common divisor.
Hint: See Problem 4.2.33. The gcd is $(x-1)(x^2+1)$.

34. Factor $f(x) = x^5 + x^4 - 2x^3 - x^2 + 2x - 2$ and $g(x) = x^3 - x^2 + x - 1$ over $\mathbf{Z}_5$ and use the factorizations to find their greatest common divisor.
Hint: See Problem 4.2.34. The gcd is $(x+2)(x-2)$.

35. Factor $f(x) = x^5 + 3x^4 - 2x^3 - 3x - 3$ and $g(x) = x^3 - x^2 + x - 1$ over $\mathbf{Z}_7$ and use the factorizations to find their greatest common divisor.

Hint: See Problem 4.2.35. The gcd is $x^2 + 1$.

37. Find a generator for the multiplicative group of the field $\mathbf{Z}_2[x]/\langle x^4 + x + 1\rangle$. As in the solution to Problem 32, let $[x] = \alpha$.
Hint: A nontrivial element that does not have order 3 or 5 must have order 15.

38. Find the multiplicative inverses of $[1 + x]$ and $[1 - x]$ in $\mathbf{Z}_3[x]/\langle x^2 + x + 2\rangle$.
Answer: From the multiplication table in Exercise 4.3.18, we have $[1 + x]^{-1} = [x]$ and $[1 - x]^{-1} = -[1 - x]$.

40. Use a calculation in $\mathbf{Q}[x]/\langle x^3 - 2\rangle$ to rationalize the denominator of $\dfrac{1}{1 - \sqrt[3]{2} + \sqrt[3]{4}}$.
Hint: Find the multiplicative inverse of $1 - x + x^2$ in $\mathbf{Q}[x]/\langle x^3 - 2\rangle$.
Answer: $\dfrac{-1 - \sqrt[3]{2}}{3}$

4.4 Polynomials over Z, Q, R, and C

21. Factor $x^5 - 10x^4 + 24x^3 + 9x^2 - 33x - 12$ over $\mathbf{Q}$.

Solution: The possible rational roots of $f(x) = x^5 - 10x^4 + 24x^3 + 9x^2 - 33x - 12$ are $\pm1, \pm2, \pm3, \pm4, \pm6, \pm12$. Since $f(1) = 21$, by the comments in the paragraph preceding the problems we must have $(r-1)|21$ for any root $r \in \mathbf{Z}$. This eliminates all but $\pm2, 4, -6$ as possibile integer roots. Then $f(2) = 32$, $f(-2) = -294$, and $f(4) = 0$. Dividing $f(x)$ by $x-4$ finally gives us the factorization $f(x) = (x-4)(x^4-6x^3+9x+3)$. The second factor is irreducible over $\mathbf{Q}$ since it satisfies Eisenstein's criterion for $p = 3$.

22. Show that $x^3 + (3m - 1)x + (3n + 1)$ is irreducible in $\mathbf{Q}[x]$ for all $m, n \in \mathbf{Z}$.

Solution: The clue to the solution lies in the multiples of 3. Reducing the polynomial modulo 3 simplifies it to $x^3 - x + 1$. You can quickly check that 0 and ±1 are not roots modulo 3. The fact that the polynomial is irreducible in $\mathbf{Z}_3[x]$ shows that it is cannot be factored with integer coefficients, because such a proper factorization in $\mathbf{Z}[x]$ would reduce to a proper factorization modulo 3. Therefore Theorem 4.4.5 implies that there is no proper factorization over the rational numbers.

23. Use Eisenstein's criterion to show that $x^4 + 120x^3 - 90x + 60$ is irreducible over $\mathbf{Q}$.

Solution: Omitting the leading coefficient 1, the greatest common divisor of the other coefficients is $30 = 2 \cdot 3 \cdot 5$. This shows that the only primes that can be used directly (without making a substitution) are $p = 2, 3, 5$. Since 60 is divisible by 2^2 but not by either 3^2 or 5^2, Eisenstein's criterion holds for $p = 3$ and for $p = 5$, although not for $p = 2$. In conclusion, $5 \mid 120$, $5 \mid 90$, $5 \mid 60$, $25 \nmid 60$ shows that the polynomial is irreducible over $\mathbf{Q}$.

24. Factor $x^8 - 1$ over $\mathbf{C}$.

Solution: We have $x^8 - 1 = (x^4 - 1)(x^4 + 1)$. The roots in $\mathbf{C}$ of $x^8 - 1$ are the 8th roots of unity, while the roots of $x^4 - 1$ are the 4th roots of unity: $\{\pm1, \pm i\}$. Thus the

remaining 8th roots of unity $\{\pm\frac{\sqrt{2}}{2} \pm \frac{\sqrt{2}}{2}i\}$ are roots of x^4+1. Finally, x^8-1 factors into the product of the corresponding 8 linear terms.

Comment: See Appendix A.5 of **Abstract Algebra** for information about the nth roots of unity.

25. Factor x^4-2 over $\mathbf{C}$.

Solution: We need to solve $x^4=2$, and for the real solution we get $x=\sqrt[4]{2}$. We now have one particular solution, and we can multiply this by any solution of $x^4=1$ to obtain another solution. Since the 4th roots of unity are $\{\pm 1, \pm i\}$, the full list of solutions is $\{\pm\sqrt[4]{2},\ \pm\sqrt[4]{2}i\}$. This gives us the factorization over $\mathbf{C}$: $x^4-2 = (x-\sqrt[4]{2})(x+\sqrt[4]{2})(x-\sqrt[4]{2}i)(x+\sqrt[4]{2}i)$.

26. Factor x^3-2 over $\mathbf{C}$.

Solution: The cube roots of unity are 1, ω, and ω^2, where $\omega = -\frac{1}{2}+\frac{\sqrt{3}}{2}i$. Thus the roots of $x^3=2$ are $\{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\}$, and $x^3-2=(x-\sqrt[3]{2})(x-\sqrt[3]{2}\omega)(x-\sqrt[3]{2}\omega^2)$.

ANSWERS AND HINTS

27. Find all rational roots of $f(x)=x^3-x^2+x-1$. *Answer:* 1

28. Find all rational roots of $g(x)=x^5-4x^4-2x^3+14x^2-3x+18$. *Answer:* $-2, 3$

29. Factor the polynomials $f(x)$ and $g(x)$ in Problems 27 and 28 and use their factorizations to find $\gcd(f(x),\, g(x))$ in $\mathbf{Q}[x]$. *Answer:* $\gcd(f(x),\, g(x)) = x^2+1$

30. Find all rational roots of $f(x)=x^5-8x^4+25x^3-38x^2+28x-8$. *Answer:* $1, 2$

31. Find all rational roots of $g(x)=x^5-x^4-2x^3+2x^2+x-1$. *Answer:* ± 1

32. Factor the polynomials $f(x)$ and $g(x)$ in Problems 31 and 32 and use the factorizations to find $\gcd(f(x),\, g(x))$ in $\mathbf{Q}[x]$. *Hint:* Compare Problem 4.2.36.
Answer: $\gcd(f(x),\, g(x)) = (x-1)^2$

35. Show that $x^5+5x^4-40x^2-75x-48$ is irreducible over $\mathbf{Q}$. Use Eisenstein's criterion. *Hint:* Substitute $x+1$.

36. Show that $x^5+5x^4-40x^2-75x-48$ is irreducible over $\mathbf{Q}$. Use Eisenstein's criterion. *Hint:* Substitute $x-2$ and use $p=5$.

40. Show that there are infinitely many quaternions that are roots of the polynomial x^2+1.
Hint: Verify that if $b^2+c^2+d^2=1$, then $\begin{bmatrix} bi & c+di \\ -c+di & -bi \end{bmatrix}^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$.

Review Problems

1. Use the Euclidean algorithm to find $\gcd(x^8-1,\ x^6-1)$ in $\mathbf{Q}[x]$ and write it as a linear combination of x^8-1 and x^6-1.

   Solution: Let $x^8-1=f(x)$ and $x^6-1=g(x)$. Using the division algorithm, we have

   $$\begin{aligned} f(x) &= x^2g(x)+(x^2-1) \\ g(x) &= (x^4+x^2+1)(x^2-1)\ . \end{aligned}$$

   This shows that $\gcd(x^8-1,\ x^6-1)=x^2-1$, and that $x^2-1=f(x)-x^2g(x)$.

2. Over the field of rational numbers, find the greatest common divisor of $2x^4-x^3+x^2+3x+1$ and $2x^3-3x^2+2x+2$ and express it as a linear combination of the given polynomials.

   Solution: To simplify the computations, let $2x^4-x^3+x^2+3x+1=f(x)$ and $2x^3-3x^2+2x+2=g(x)$. Using the Euclidean algorithm, we have the following computations.

   $$\begin{aligned} f(x) &= (x+1)g(x)+(2x^2-x-1) \\ g(x) &= (x-1)(2x^2-x-1)+(2x+1) \\ 2x^2-x-1 &= (x-1)(2x+1) \end{aligned}$$

   Thus $2x+1$ is the greatest common divisor (we must then divide by 2 to make it monic). Beginning with the last equation and back-solving, we get

   $$\begin{aligned} 2x+1 &= g(x)-(x-1)(2x^2-x-1) \\ &= g(x)-(x-1)(f(x)-(x+1)g(x)) \\ &= g(x)+(x^2-1)g(x)-(x-1)f(x) \\ &= x^2g(x)-(x-1)f(x) \end{aligned}$$

   This gives the desired linear combination: $x+\frac{1}{2}=\frac{1}{2}x^2g(x)+(-\frac{1}{2})(x-1)f(x)$.

3. Are the following polynomials irreducible over $\mathbf{Q}$?

   (a) $3x^5+18x^2+24x+6$

   Solution: Dividing by 3 we obtain x^5+6x^2+8x+2, and this satisfies Eisenstein's criterion for $p=2$.

   (b) $7x^3+12x^2+3x+45$

   Solution: Reducing the coefficients modulo 2 gives the polynomial x^3+x+1, which is irreducible in $\mathbf{Z}_2[x]$. This implies that the polynomial is irreducible over $\mathbf{Q}$.

   (c) $2x^{10}+25x^3+10x^2-30$

   Solution: Eisenstein's criterion is satisfied for $p=5$.

4. Factor $x^5 - 2x^4 - 2x^3 + 12x^2 - 15x - 2$ over $\mathbf{Q}$.

   Solution: The possible rational roots are $\pm 1, \pm 2$, and since 2 is a root we have the factorization $x^5 - 2x^4 - 2x^3 + 12x^2 - 15x - 2 = (x-2)(x^4 - 2x^2 + 8x + 1)$. The only possible rational roots of the second factor are 1 and -1, and these do not work. (It is important to note that since the degree of the polynomial is greater than 3, the fact that it has not roots in $\mathbf{Q}$ does not mean that it is irreducible over $\mathbf{Q}$.) Since the polynomial has no linear factors, the only possible factorization has the form $x^4 - 2x^2 + 8x + 1 = (x^2 + ax + b)(x^2 + cx + d)$. This leads to the equations $a + c = 0$, $ac + b + d = -2$, $ad + bc = 8$, and $bd = 1$. We have either $b = d = 1$, in which case $a + c = 8$, or $b = d = -1$, in which case $a + c = -8$. Either case contradicts $a + c = 0$, so $x^4 - 2x^2 + 8x + 1$ is irreducible over $\mathbf{Q}$.

   Alternate solution: Once we have the factorization $x^5 - 2x^4 - 2x^3 + 12x^2 - 15x - 2 = (x-2)(x^4 - 2x^2 + 8x + 1)$, we can check the second factor for reducibility modulo p. Reducing modulo 2 gives $x^4 + 1$, which has a root.

   Reducing $x^4 - 2x^2 + 8x + 1$ modulo 3 gives $p(x) = x^4 + x^2 - x + 1$. This polynomial has no roots in $\mathbf{Z}_3$, so the only possible factors are of degree 2. There are nine possible monic polynomials of degree 2 over $\mathbf{Z}_3$. Checking them for roots shows that the monic irreducible polynomials of degree 2 over $\mathbf{Z}_3$ are $x^2 + 1$, $x^2 + x - 1$, and $x^2 - x - 1$. Since the constant term of $p(x)$ is 1, the only possible factorizations are $p(x) = (x^2 + 1)^2$, $p(x) = (x^2 + x - 1)^2$, $p(x) = (x^2 - x - 1)^2$, or $p(x) = (x^2 + x - 1)(x^2 - x - 1)$. In the first the coefficient of x is 0; in the second the coefficient of x is 1; the third has a nonzero cubic term; in the fourth the coefficient of x is 0. We conclude that $p(x)$ is irreducible over $\mathbf{Z}_3$, and hence over $\mathbf{Q}$.

5. (a) Show that $x^2 + 1$ is irreducible over $\mathbf{Z}_3$.

   Solution: To show that $p(x) = x^2 + 1$ is irreducible over $\mathbf{Z}_3$, we only need to check that it has no roots in $\mathbf{Z}_3$, and this follows from the computations $p(0) = 1$, $p(1) = 2$, and $p(-1) = 2$.

   (b) List the elements of the field $F = \mathbf{Z}_3[x]/\langle x^2 + 1 \rangle$.

   Solution: The congruence classes are in one-to-one correspondence with the linear polynomials, so we have the nine elements [0], [1], [2], $[x]$, $[x+1]$, $[x+2]$, $[2x]$, $[2x+1]$, $[2x+2]$.

   (c) In the multiplicative group of nonzero elements of F, show that $[x + 1]$ is a generator, but $[x]$ is not.

   Solution: The multiplicative group of F has 8 elements, and since $[x]^2 = [-1]$, it follows that $[x]$ has order 4 and is not a generator. On the other hand, $[x + 1]^2 = [x^2 + 2x + 1] = [-1 + 2x + 1] = [2x] = [-x]$, and so $[x+1]^4 = [-x]^2 = [-1]$, which shows that $[x+1]$ does not have order 2 or 4. The only remaining possibility (by Lagrange's theorem) is that $[x + 1]$ has order 8, and so it is a generator for the multiplicative group of F.

6. Construct an example of a field with $343 = 7^3$ elements.

Solution: We only need to find a cubic polynomial over $\mathbf{Z}_7$ that has no roots. The simplest case would be to look for a polynomial of the form $x^3 + a$. The cube of any element of $\mathbf{Z}_7$ gives either 1 or -1, so $x^3 = 2$ has no root over $\mathbf{Z}_7$, and thus $p(x) = x^3 - 2$ is an irreducible cubic over $\mathbf{Z}_7$. Using the modulus $p(x)$, the elements of $\mathbf{Z}_7[x]/\langle p(x)\rangle$ correspond to polynomials of degree 2 or less, giving the required 7^3 elements. With this modulus, the identities necessary to determine multiplication are $[x^3] = [2]$ and $[x^4] = [2x]$.

7. Find the multiplicative inverse of $[x^2 + x + 1]$

(a) in $\mathbf{Q}[x]/\langle x^3 - 2\rangle$;

Solution: Using the Euclidean algorithm, we have $x^3 - 2 = (x-1)(x^2+x+1)+(-1)$, and so $[x^2 + x + 1]^{-1} = [x - 1]$.

Comment: This can also be done by solving a system of 3 equations in 3 unknowns.

(b) in $\mathbf{Z}_3[x]/\langle x^3 + 2x^2 + x + 1\rangle$.

Solution: Using the Euclidean algorithm, we have

$$\begin{aligned} x^3 + 2x^2 + x + 1 &= (x+1)(x^2 + x + 1) + (-x) \\ x^2 + x + 1 &= (-x-1)(-x) + 1 \ . \end{aligned}$$

Then substitution gives us

$$\begin{aligned} 1 &= (x^2 + x + 1) + (x+1)(-x) \\ &= (x^2 + x + 1) + (x+1)((x^3 + 2x^2 + x + 1) - (x+1)(x^2 + x + 1)) \\ &= (-x^2 - 2x)(x^2 + x + 1) + (x+1)(x^3 + x^2 + 2x + 1) \ . \end{aligned}$$

Thus $[x^2 + x + 1]^{-1} = [-x^2 - 2x] = [2x^2 + x]$. This can be checked by finding $[x^2 + x + 1][2x^2 + x]$, using the identities $[x^3] = [x^2 - x - 1]$ and $[x^4] = [x - 1]$.

Comment: This problem can also be done by solving a system of equations, or, since the set is finite, by taking successive powers of $[x^2 + x + 1]$. The latter method isn't really practical, since the multiplicative group has order 26, and this element turns out to have order 13, and so $[x^2 + x + 1]^{-1} = [x^2 + x + 1]^{12}$.

8. In $\mathbf{Z}_5[x]/\langle x^3 + x + 1\rangle$, find $[x]^{-1}$ and $[x+1]^{-1}$, and use your answers to find $[x^2+x]^{-1}$.

Solution: Using the division algorithm, we obtain $x^3 + x + 1 = (x^2 + 1)x + 1$, and so $[x^2 + 1][x] = [-1]$. Thus $[x]^{-1} = [-x^2 - 1]$.

Next, we have $x^3 + x + 1 = (x^2 - x + 2)(x + 1) - 1$, and so $[x + 1]^{-1} = [x^2 - x + 2]$.

Finally, we have

$$\begin{aligned} [x^2 + x]^{-1} &= [x]^{-1}[x+1]^{-1} \ = \ [-x^2 - 1][x^2 - x + 2] \\ &= [-x^4 + x^3 - 3x^2 + x - 2] \ . \end{aligned}$$

Using the identities $[x^3] = [-x - 1]$ and $[x^4] = [-x^2 - x]$, this reduces to

$$\begin{aligned} [x^2 + x]^{-1} &= [x^2 + x - x - 1 - 3x^2 + x - 2] \\ &= [-2x^2 + x - 3] \ = \ [3x^2 + x + 2] \ . \end{aligned}$$

Chapter 5

Commutative Rings

5.1 Commutative rings; Integral Domains

23. Let R be a commutative ring. Prove the following statements (listed in Section 5.1):

    (d) $a \cdot 0 = 0$ for all $a \in R$;

    Solution: Since 0 is the additive identity element, we have $0 + 0 = 0$. To connect this property to multiplication, we need to use the distributive law. We have $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$, and then we can subtract $a \cdot 0$ from both sides of the equation to get $0 = a \cdot 0$.

    (e) $-(-a) = a$ for all $a \in R$;

    Solution: This holds in any group.

    (f) $(-a) \cdot (-b) = ab$ for all $a, b \in R$.

    Solution: Because we are proving a relationship between addition (since $-a$ is defined to be the additive inverse of a) and multiplication, we need to use the distributive law. We have $ab + a(-b) = a(b - b) = a \cdot 0 = 0$, and so $a(-b) = -(ab)$. Similarly, $(-a)b = -ab$, and then $(-a)(-b) = -(a(-b)) = -(-ab) = ab$.

24. (a) Is $\mathbf{Z}_2$ a subring of $\mathbf{Z}_6$?

    Solution: No, because $\mathbf{Z}_2$ is not even a *subset* of $\mathbf{Z}_6$.

    (b) Is $3\mathbf{Z}_6$ a subring of $\mathbf{Z}_6$?

    Solution: The set $3\mathbf{Z}_6 = \{[0]_6, [3]_6\}$ is closed under addition, since we know it is a subgroup of the underlying additive group of $\mathbf{Z}_6$. Furthermore, $3\mathbf{Z}_6$ is easily checked to be closed under multiplication. But our definition of a subring requires that the subset must contain the identity element of the ring, and since $[1]_6 \notin 3\mathbf{Z}_6$, we conclude that $3\mathbf{Z}_6$ is *not* a subring of $\mathbf{Z}_6$.

    Comment: Be careful here, because some authors do not require that a subring of a commutative ring with 1 must have the same identity element. In fact, we changed our definition between the second and third editions of our text **Abstract Algebra**.

25. (a) Show that the ring of Gaussian integers is an integral domain.

Solution: It is easy to check that the set $\mathbf{Z}[i] = \{m + ni \mid m, n \in \mathbf{Z}\}$ is closed under addition and multiplication and contains 1. It follows that $\mathbf{Z}[i]$ is a subring of $\mathbf{C}$, and so Theorem 5.1.8 implies that $\mathbf{Z}[i]$ is an integral domain.

(b) Show that $\mathbf{Z}[\sqrt{2}] = \{m + n\sqrt{2} \mid m, n \in \mathbf{Z}\}$ is an integral domain.

Solution: As in part (a), $\mathbf{Z}[\sqrt{2}]$ is a subring of $\mathbf{C}$ and so it follows from Theorem 5.1.8 that $\mathbf{Z}[\sqrt{2}]$ is an integral domain.

Comment: The details of the proofs that $\mathbf{Z}[i]$ and $\mathbf{Z}[\sqrt{2}]$ are subrings of $\mathbf{C}$ can be found in Examples 5.1.5 and 5.1.6 of **Abstract Algebra**.

26. Let R be a commutative ring. Prove that the intersection of any collection of subrings of R is a subring of R.

Solution: To use Proposition 5.1.4, let a and b be elements in the intersection. Then a and b each belong to every subring in the collection, so $a+b$, ab, and $-a$ also belong to every subring in the collection. Therefore $a+b$, ab, and $-a$ belong to the intersection. Finally, the multiplicative identity of R belongs to each subring, so it also belongs to the intersection.

27. Show that in an integral domain the only idempotent elements are 0 and 1.

Solution: Let D be an integral domain, and suppose that $e \in D$ is idempotent. Then $e \cdot e = e^2 = e = e \cdot 1$, and so if $e \neq 0$, then $e = 1$ since the cancellation law holds in D. Since 0 and 1 are idempotent, they are the only idempotent elements in D.

28. Show that if $n = p^k$ (p prime), then in $\mathbf{Z}_n$ the only idempotent elements are 0 and 1.

Solution: If $e^2 = e$ in $\mathbf{Z}_n$, then $p^k \mid e(e-1)$, and since $\gcd(e, e-1) = 1$, this implies the either $p^k \mid e$, and $e = 0$, or else $p^k \mid (e-1)$ and $e = 1$.

29. In $\mathbf{Z}_{24}$,

(a) find all nilpotent elements;

Solution: We have $x^n \equiv 0 \pmod{24}$ if and only if $3 \mid x$ and $2 \mid x$. Thus the list of nilpotent elements is $\{0, 6, 12, 18\} = \langle 2 \cdot 3 \rangle$.

(b) find all idempotent elements.

Solution: If $e \in \mathbf{Z}_{24}$ is idempotent, then $24 \mid e(e-1)$. Since $\gcd(e, e-1) = 1$ this implies that $3 \mid e$ or $3 \mid e-1$, or else $8 \mid e$ or $8 \mid e-1$. The list of elements e with $8 \mid e$ or $8 \mid e-1$ is $\{e \mid e = 0, 1, 8, 9, 16, 17\}$. Adding the condition that $3 \mid e$ or $3 \mid e-1$ reduces the list to $\{0, 1, 9, 16\}$.

30. Let R be the set of all 3×3 matrices of the form $\begin{bmatrix} a & 0 & 0 \\ b & a & 0 \\ c & b & a \end{bmatrix}$ with $a, b, c \in \mathbf{Z}$.

(a) Show that R is a commutative ring.

Solution: From linear algebra we know that addition and multiplication of matrices satisfy all of the axioms of a commutative ring, except the commutative law. Therefore

it is enough to show that the given set satisfies the commutative law, and satisfies the conditions of a subring given in Proposition 5.1.4.

First, it is clear that the set is closed under addition, is closed under forming additive inverses, and contains the identity matrix. The following calculations verify closure and commutativity of multiplication.

$$\begin{bmatrix} a & 0 & 0 \\ b & a & 0 \\ c & b & a \end{bmatrix} \begin{bmatrix} d & 0 & 0 \\ e & d & 0 \\ f & e & d \end{bmatrix} = \begin{bmatrix} ad & 0 & 0 \\ bd+ae & ad & 0 \\ cd+bd+af & bd+ae & ad \end{bmatrix}$$

$$\begin{bmatrix} d & 0 & 0 \\ e & d & 0 \\ f & e & d \end{bmatrix} \begin{bmatrix} a & 0 & 0 \\ b & a & 0 \\ c & b & a \end{bmatrix} = \begin{bmatrix} da & 0 & 0 \\ ea+db & da & 0 \\ fa+eb+dc & ea+db & da \end{bmatrix}$$

(b) Find the units of R.

Solution: Because the entries are from $\mathbf{Z}$, in which only 1 and -1 are invertible, a matrix in R is invertible if and only its determinant is ± 1. Thus an element is invertible if and only if it has either 1 or -1 on the main diagonal.

(c) Find the nilpotent elements of R.

Solution: The nilpotent matrices in R are the strictly lower triangular matrices.

31. Let R and S be commutative rings. Prove or disprove the following statements.

(a) An element $(a, b) \in R \oplus S$ is idempotent if and only if a an idempotent in R and b is idempotent in S.

Solution: Since $(a, b)^2 = (a^2, b^2)$, it is clear that $(a, b)^2 = (a, b)$ if and only if $a^2 = a$ and $b^2 = b$.

(b) An element $(a, b) \in R \oplus S$ is nilpotent if and only if a nilpotent in R and b is nilpotent in S.

Solution: This clearly holds since $(a, b)^n = (a^n, b^n)$.

Comment: If m and k are the smallest positive integers with $a^m = 0$ and $b^k = 0$, respectively, then the smallest positive integer n with $(a, b)^n = (0, 0)$ is $n = \max\{m, k\}$.

(c) An element $(a, b) \in R \oplus S$ is a zero divisor if and only if a is a zero divisor in R and b is a zero divisor in S.

Solution: This part is false since $(1, 0)$ is a zero divisor in $\mathbf{Z} \oplus \mathbf{Z}$ because $(1, 0)(0, 1) = (0, 0)$, but 1 is certainly not a zero divisor in $\mathbf{Z}$.

32. In the ring $\mathbf{Z} \oplus \mathbf{Z}$, let $R = \{(x, y) \mid x \equiv y \pmod 2\}$.

(a) Show that R is a subring of $\mathbf{Z} \oplus \mathbf{Z}$.

Comment: Although the definition of a direct sum was first given in Exercise 5.1.16 of the text, there is also a formal definition in Section 5.2.

Solution: To show that R is a subring we will use Proposition 5.1.4. If (a, b) and (c, d) belong to R, then $a \equiv b \pmod 2$ and $c \equiv d \pmod 2$, so it follows that $a + c \equiv b + d \pmod 2$ and $ac \equiv bd \pmod 2$, and thus R is closed under addition and

multiplication. Furthermore, $-a \equiv -b \pmod 2$ implies $-(a,b) \in R$, and it is clear that the identity $(1,1)$ of $\mathbf{Z} \oplus \mathbf{Z}$ is in R.

(b) Is R an integral domain?

Solution: No, because $(2,0) \cdot (0,2) = (0,0)$.

(c) Find all idempotent elements of R.

Solution: An element of a direct sum of commutative rings is idempotent if and only if each component is idempotent. Thus the idempotent elements of $\mathbf{Z} \oplus \mathbf{Z}$ are $(0,0)$, $(1,1)$, $(1,0)$, $(0,1)$, and of these only $(0,0)$ and $(1,1)$ belong to R.

33. Find a commutative ring with zero divisors a, b such that $a+b$ is *not* a zero divisor and $a+b \neq 0$.

Solution: In $\mathbf{Z}_2 \oplus \mathbf{Z}_2$ we have $(1,0)\cdot(0,1) = (0,0)$, so $(1,0)$ and $(0,1)$ are zero divisors, but their sum $(1,0)+(0,1) = (1,1)$ is *not* a zero divisor.

34. Although the set $\mathbf{Z}_2[x]/\langle x^2+1\rangle$ is not a field, Proposition 4.3.4 shows that addition and multiplication of congruence classes of polynomials is well-defined. Show that in this set the cancellation law for multiplication does not hold.

Solution: Since $x^2+1 \equiv 0$, we have $x^2 \equiv -1 \equiv 1$. Therefore we have $x(1+x) = x + x^2 \equiv x+1$. The cancellation law does not hold since for the nonzero elements 1, x and $1+x$ we have $x(1+x) = 1(1+x)$ but $x \neq 1$.

35. Recall that $\mathbf{Z}_3[x]/\langle x^2+1\rangle$ is a field (this follows from Theorem 4.3.6 since x^2+1 is irreducible over $\mathbf{Z}_3$). Find the order of each element in its group of units.

Solution: The nonzero elements are 1, -1, x, $x+1$, $x-1$, $-x$, $-x+1 = -(x-1)$, and $-x-1 = -(x+1)$. Of course, -1 has order 2. Since $x^2 \equiv -1$, we have $x^3 \equiv -x$ and $x^4 \equiv 1$. It follows that x and $-x$ have order 4, while x^2 has order 2. We have $(x+1)^2 = x^2 - x + 1 \equiv -x$, so $x+1$ has order 8, making it a generator of the group of units. Starting over again and calculating powers of $x+1$, we have the following.

$(x+1)^2 \equiv -x$

$(x+1)^3 \equiv (x+1)(-x) \equiv -x^2 - x \equiv -x+1$

$(x+1)^4 \equiv (-x)^2 \equiv -1$

$(x+1)^5 \equiv -(x+1)$

$(x+1)^6 \equiv -(x+1)^2 \equiv x$

$(x+1)^7 \equiv x(x+1) \equiv x-1$

$(x+1)^8 \equiv (-1)^2 \equiv 1$

Thus the congruence classes of $\pm x \pm 1$ have order 8, while those of $\pm x$ have order 4. Finally -1 has order 2 and 1 has order 1.

Comment: Review Proposition 3.5.3 if you have questions about finding the order of an element of a cyclic group.

36. Let p be an odd prime number that is not congruent to 1 modulo 4. Prove that the ring $\mathbf{Z}_p[x]/\langle x^2+1\rangle$ is a field.

Hint: A root of $x^2 = -1$ leads to an element of order 4 in $\mathbf{Z}_p^\times$.

Solution: We must show that x^2+1 is irreducible over $\mathbf{Z}_p$, or, equivalently, that x^2+1 has no root in $\mathbf{Z}_p$.

Suppose that a is a root of x^2+1 in $\mathbf{Z}_p$. Then $a^2 \equiv -1 \pmod{p}$, and so $a^4 \equiv 1 \pmod{p}$. The element a cannot be a root of x^2-1, so it does not have order 2, and thus it must have order 4. By Lagrange's theorem, this means that 4 is a divisor of the order of $\mathbf{Z}_p^\times$, which is $p-1$. Therefore $p = 4q+1$ for some $q \in \mathbf{Z}$, contradicting the assumption.

37. Let S be a commutative ring.

(a) Let $R = \{n \cdot 1 \mid n \in \mathbf{Z}\}$. Show that R is a subring of S.

Solution: If $m, n \in \mathbf{Z}$, we have $m \cdot 1 + n \cdot 1 = (m+n) \cdot 1$ by the associative law for addition, and $(m \cdot 1) \cdot (n \cdot 1) = (mn) \cdot 1$ by the distributive law. Finally, $1 = 1 \cdot 1$, and so R is subring of S.

(b) Find the subring defined in part (a) for the ring given in Problem 30 and for the field given in Problem 35.

Solution: In the ring $\begin{bmatrix} a & 0 & 0 \\ b & a & 0 \\ c & b & a \end{bmatrix}$ with $a, b, c \in \mathbf{Z}$ defined in Problem 27, the identity element is the identity matrix. The subring defined in part (a) is therefore the set of all scalar matrices.

In the field $\mathbf{Z}_3[x]/\langle x^2+1\rangle$ defined in Problem 30, the elements are the congruence classes represented by linear polynomials. The identity element is the constant polynomial $[1]_3$, and so the subring defined in part (a) is the set of all constant polynomials.

38. (a) Let S be a set that satisfies all of the axioms of commutative ring, with the possible exception of the commutative law for multiplication. Show that the set $R = \{r \in S \mid rs = sr \text{ for all } s \in S\}$ is a commutative ring.

Note: The ring R is called the **center** of S.

Solution: Since all of the axioms except the commutative law hold, we can use the proof of Proposition 5.1.4 to simplify the calculations. If $r_1, r_2 \in R$, then $(r_1+r_2)s = r_1s + r_2s = sr_1 + sr_2 = s(r_1+r_2)$, and $(r_1r_2)s = r_1(r_2s) = r_1(sr_2) = (r_1s)r_2 = (sr_1)r_2 = s(r_1r_2)$. Furthermore, $(-r_1)s = -(r_1s) = -(sr_1) = s(-r_1)$. Finally, by definition $1 \in R$, and since it is clear that elements in R commute with each other, we are justified in concluding that R is a commutative ring.

(b) Find the center of the set $M_2(\mathbf{R})$ of all 2×2 matrices with real entries.

Comment: I need to comment on the following calculations, so that they don't just look like a trick. It would be natural to start out by just writing down an element in the center and seeing what you get by letting it commute with a general element of $M_2(\mathbf{R})$. In fact (you can try it), you would get four equations in four unknowns, with

four general (undetermined) constants, and the situation is quite out of hand. The point is to take these equations and carefully choose some of the constants so that you can get some meaningful equations. The best way to do this seems me to be to pick (carefully) a couple of elements of $M_2(\mathbf{R})$ and see what specific information you get. My choice of elements is based on trial and error.

Solution: Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ belong to the center. In particular, it must commute with the element $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, and so we must have $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. This yields four equations, and the useful ones are $a + b = a$, which shows that b has to be zero, and $c + d = a + c$, which shows that $a = d$. Next, any such element must also commute with $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, so we get $\begin{bmatrix} a & 0 \\ c & a \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & 0 \\ c & a \end{bmatrix}$. Now we get $a = a + c$, and so $c = 0$. We conclude that any element in the center of $M_2(\mathbf{R})$ must be a scalar matrix. On the other hand, it is clear that any scalar matrix is in the center, and so the center is precisely the set of scalar matrices.

ANSWERS AND HINTS

42. Let R and S be commutative rings. Show that $(R \oplus S)^\times \cong R^\times \times S^\times$ (as groups).
Hint: Define $\phi : R^\times \times S^\times \to (R \oplus S)^\times$ by $\phi((u, v)) = (u, v)$ and verify that (u, v) is a unit of $R \oplus S$ if and only if u is a unit in R and v is a unit in S.

44. Let R be a Boolean ring with 16 elements. Find $R^\times$.
Answer: $R^\times = \{1\}$. Note: the number 16 is a red herring.

45. Let R be the ring of continuous functions from $\mathbf{R}$ to $\mathbf{R}$. (Remember that R is a ring under multiplication of functions, *not* composition of functions.)
(b) Characterize the units of R.
Answer: Either $f(x) > 0$ for all $x \in \mathbf{R}$, or $f(x) < 0$ for all $x \in \mathbf{R}$.
(d) Characterize the nilpotent elements of R.
Answer: The only nilpotent element is the zero function.

48. Let R be a commutative ring.
(a) Can $R[x]$ have nilpotent elements of positive degree?
Hint: Look at $\mathbf{Z}_4[x]$.
(b) Can $R[x]$ have idempotent elements of positive degree?
Hint: Look at $\mathbf{Z}_6[x]$.

5.2 Ring Homomorphisms

24. (Back to Calculus) Does the derivative define a ring homomorphism from $\mathbf{R}[x]$ to $\mathbf{R}[x]$?

Solution: The product rule shows that the derivative does not respect multiplication.

25. Is an isomorphism of fields a ring isomorphism?

Comment: Here's the problem: Definition 4.3.7 does not require that an isomorphism of fields maps 1 to 1. (All the other requirements of a ring isomorphism are met.)

Solution: Suppose that $\phi : F_1 \to F_2$ is an isomorphism of fields. Since $1 \neq 0$ and ϕ is one-to-one, we must have $\phi(1) \neq 0$. Then $\phi(1)\phi(1) = \phi(1 \cdot 1) = \phi(1) = 1 \cdot \phi(1)$. Since $\phi_1 \neq 0$ and F_2 is a field, we can cancel to get $\phi(1) = 1$.

Answer: Yes! So there's really no problem.

26. Let R and S be commutative rings, and let $\phi : R \to S$ be a ring homomorphism.

(a) Does ϕ map idempotent elements to idempotent elements?

Solution: Yes; if $e^2 = e$, then $(\phi(e))^2 = \phi(e^2) = \phi(e)$.

(b) Does ϕ map nilpotent elements to nilpotent elements?

Solution: Yes; if $x^n = 0$, then $(\phi(x))^n = \phi(x^n) = \phi(0) = 0$.

(c) Does ϕ map zero divisors to zero divisors?

Solution: No; let $\pi : \mathbf{Z}_2 \oplus \mathbf{Z}_2 \to \mathbf{Z}_2$ be given by $\phi((x, y)) = x$. Then π maps the zero divisor $(1, 0)$ to 1, which is definitely not a zero divisor.

27. Let R and S be commutative rings. Show that the set of 2×2 diagonal matrices with entries from R and S (respectively) forms a commutative ring isomorphic to $R \oplus S$.

Solution: Consider the set T of all matrices of the form $\begin{bmatrix} r & 0 \\ 0 & s \end{bmatrix}$. Define $\phi : R \oplus S \to T$ by $\phi((r, s)) = \begin{bmatrix} r & 0 \\ 0 & s \end{bmatrix}$, for all $(r, s) \in R \oplus S$. It is clear that ϕ is one-to-one and onto, and ϕ maps $(1, 1)$ to the identity matrix. The following calculations show that ϕ preserves addition and multiplication.

$$\phi((r_1, s_1) + (r_2, s_2)) = \phi((r_1 + r_2, s_1 + s_2)) = \begin{bmatrix} r_1 + r_2 & 0 \\ 0 & s_1 + s_2 \end{bmatrix}$$

$$\phi((r_1, s_1)) + \phi((r_2, s_2)) = \begin{bmatrix} r_1 & 0 \\ 0 & s_1 \end{bmatrix} + \begin{bmatrix} r_2 & 0 \\ 0 & s_2 \end{bmatrix} = \begin{bmatrix} r_1 + r_2 & 0 \\ 0 & s_1 + s_2 \end{bmatrix}$$

$$\phi((r_1, s_1) \cdot (r_2, s_2)) = \phi((r_1 r_2, s_1 s_2)) = \begin{bmatrix} r_1 r_2 & 0 \\ 0 & s_1 s_2 \end{bmatrix}$$

$$\phi((r_1, s_1)) \cdot \phi((r_2, s_2)) = \begin{bmatrix} r_1 & 0 \\ 0 & s_1 \end{bmatrix} \cdot \begin{bmatrix} r_2 & 0 \\ 0 & s_2 \end{bmatrix} = \begin{bmatrix} r_1 r_2 & 0 \\ 0 & s_1 s_2 \end{bmatrix}$$

Finally, T is a commutative ring because an isomorphism preserves commutativity.

28. Let R be a commutative ring, with identity 1.

(a) Show that if e is an idempotent element of R, then $1 - e$ is also idempotent.

Solution: We have $(1 - e)^2 = (1 - e)(1 - e) = 1 - e - e + e^2 = 1 - e - e + e = 1 - e$.

(b) Show that if e is idempotent, then $R \cong Re \oplus R(1 - e)$.

Solution: Note that $e(1-e) = e - e^2 = e - e = 0$. Define $\phi : R \to Re \oplus R(1-e)$ by $\phi(r) = (re, r(1-e))$, for all $r \in R$. Then ϕ is one-to-one since if $\phi(r) = \phi(s)$, then $re = se$ and $r(1-e) = s(1-e)$, and adding the two equations gives $r = s$. Furthermore, ϕ is onto, since for any element $(ae, b(1-e))$ we have $(ae, b(1-e)) = \phi(r)$ for $r = ae + b(1-e)$. Finally, it is easy to check that ϕ preserves addition, and for any $r, s \in R$ we have $\phi(rs) = (rse, rs(1-e))$ and $\phi(r)\phi(s) = (re, r(1-e))(se, s(1-e)) = (rse^2, rs(1-e)^2) = (rse, rs(1-e))$. It is clear that $\phi(1) = (e, 1-e)$, which is the multiplicative identity of $Re \oplus R(1-e)$.

Comment: The ring isomorphism in this problem depends on the fact that $er = re$ for all $r \in R$.

29. Use methods of this section to find, in $\mathbf{Z}_{24}$,

Comment: It follows from Example 5.2.13 in **Abstract Algebra** that $\mathbf{Z}_{24} \cong \mathbf{Z}_3 \oplus Z_8$, since $24 = 3 \cdot 2^3$. Then it is possible to use Problem 5.1.31. Note that the isomorphism is $\phi : \mathbf{Z}_{24} \to \mathbf{Z}_3 \oplus \mathbf{Z}_8$ defined by $\phi([x]_{24}) = ([x]_3, [x]_8)$.

(a) all nilpotent elements;

Solution: Using the fact that $\mathbf{Z}_{24} \cong \mathbf{Z}_3 \oplus Z_8$, we will do the calculations in $\mathbf{Z}_3 \oplus Z_8$, Since $\mathbf{Z}_3$ is a field, $[0]_3$ is its only nilpotent element. In $\mathbf{Z}_8$, the nilpotent elements are $[0]_8$, $[2]_8$, $[4]_8$, $[6]_8$. We need to solve four simultaneous congruences.

(1) $x \equiv 0 \pmod 3$ $x \equiv 0 \pmod 8$ (2) $x \equiv 0 \pmod 3$ $x \equiv 2 \pmod 8$

(3) $x \equiv 0 \pmod 3$ $x \equiv 4 \pmod 8$ (4) $x \equiv 0 \pmod 3$ $x \equiv 6 \pmod 8$

The solutions are (1) $x \equiv 0 \pmod{24}$, (2) $x \equiv 18 \pmod{24}$, (3) $x \equiv 12 \pmod{24}$, and (4) $x \equiv 6 \pmod{24}$, as found in Problem 5.1.29.

(b) all idempotent elements.

Solution: Problem 5.1.27 shows that in $\mathbf{Z}_3$ the only idempotents are $[0]_3$ and $[1]_3$. Problem 5.1.28 shows that in $\mathbf{Z}_8$ the only idempotents are $[0]_8$ and $[1]_8$. Corresponding to these ordered pairs in $\mathbf{Z}_3 \oplus \mathbf{Z}_8$ are the elements $[0]_{24}$, $[1]_{24}$, $[8]_{24}$, and $[9]_{24}$ in $\mathbf{Z}_{24}$.

30. Let F be a subfield of the field E. For the element $u \in E$, define $\phi_u : F[x] \to E$ by setting by $\phi_u(f(x)) = f(u)$, for all $f(x) \in F[x]$.

(a) Show that if $\ker(\phi_u) \neq \{0\}$, then $\ker(\phi_u) = \langle p(x) \rangle$, where $p(x)$ is the unique monic polynomial of minimal degree in $\ker(\phi_u)$.

Solution: Assume that $\ker(\phi_u) \neq \{0\}$, and let $p(x)$ be a monic polynomial of minimal degree in $\ker(\phi_u)$. Since $p(x) \in \ker(\phi_u)$, we have $\langle p(x) \rangle \subseteq \ker(\phi_u)$. On the other hand, for any $g(x) \in \ker(\phi_u)$, we can use the division algorithm to write $g(x) = q(x)p(x) + r(x)$, with $r(x) = 0$ or $\deg(r(x)) < \deg(p(x))$. The substitution $x = u$ gives us $0 = q(u) \cdot 0 + r(u)$, and so $r(x) \in \ker(\phi_u)$. This contradicts the fact that $p(x)$ has minimal degree in $\ker(\phi_u)$, unless $r(x) = 0$. We conclude that $g(x) \in \langle p(x) \rangle$, and it follows that $\ker(\phi_u) = \langle p(x) \rangle$. Finally, this argument shows that any other monic polynomial of minimal degree in $\ker(\phi_u)$ would be both a factor of $p(x)$ and a multiple of $p(x)$, so it would be equal to $p(x)$, justifying the statement that $p(x)$ is unique.

(b) Show that the polynomial $p(x)$ in part (a) is irreducible over F.

Solution: Suppose that $p(x)$ has a proper factorization $p(x) = g(x)h(x)$, for $g(x), h(x)$ in $F[x]$. Then $g(u)h(u) = p(u) = 0$ in E, and so either $g(u) = 0$ or $h(u) = 0$. It is impossible for either $g(x)$ or $h(x)$ to belong to $\ker(\phi_u)$, since they have lower degree than $p(x)$. We conclude that $p(x)$ is irreducible over F.

31. Find the kernel of the evaluation map from $\mathbf{R}[x]$ into $\mathbf{C}$ defined by

(a) substitution of i;

Solution: A polynomial with real coefficients that has i as a root must also have $-i$ as a root. Therefore for $f(x) \in \mathbf{R}[x]$ we have $f(i) = 0$ if and only if $x - i$ and $x + i$ are both factors of $f(x)$. That is, if and only if $x^2 + 1$ is a factor of $f(x)$. The kernel of the evaluation mapping is $\langle x^2 + 1 \rangle$.

Alternate solution: It is clear that $x^2 + 1 \in \ker(\phi_i)$, and since no linear polynomial in $\mathbf{R}[x]$ has i as a root, $x^2 + 1$ must be the monic polynomial of minimal degree in $\ker(\phi_i)$. It follow from Problem 30 (a) that $\ker(\phi_i) = \langle x^2 + 1 \rangle$.

(b) substitution of $\sqrt{2}i$.

Solution: As in part (a), we have $f(\sqrt{2}i) = 0$ if and only if $(x-\sqrt{2}i)(x+\sqrt{2}i) = x^2+2$ is a factor of $f(x)$. Thus the kernel of the evaluation mapping is $\langle x^2 + 2 \rangle$.

Alternate solution: As in part (a), it is clear that $x^2 + 2 \in \ker(\phi_{\sqrt{2}i})$, and that $x^2 + 2$ must be the monic polynomial of minimal degree in $\ker(\phi_{\sqrt{2}i})$, so $\ker(\phi_{\sqrt{2}i}) = \langle x^2 + 2 \rangle$.

32. Use the techniques of this section to prove that $\mathbf{Q}[x]/\langle x^2 + 3 \rangle \cong \mathbf{Q}(\sqrt{3}i)$. Note: This is a repeat of Problem 4.3.26.

Solution: Let $\phi_{\sqrt{3}i} : \mathbf{Q}[x] \to \mathbf{C}$ be the evaluation mapping. It is clear that the image of $\phi_{\sqrt{3}i}$ is $\mathbf{Q}(\sqrt{3}i)$, and so to use the fundamental homomorphism theorem to get the desired isomorphism we only need to compute $\ker(\phi_{\sqrt{3}i})$. Since $\sqrt{3}i$ is a root of $x^2 + 3 \in \mathbf{Q}[x]$, and it is clear that no polynomial of smaller degree can belong to $\ker(\phi_{\sqrt{3}i})$, the kernel must be $\langle x^2 + 3 \rangle$. The fundamental homomorphism theorem does all the rest of the work for us.

Comment: To see how valuable the fundamental homomorphism theorem is, look back at the solution to Problem 4.3.26.

33. Prove that the ring of Gaussian integers $\mathbf{Z}[i]$ is isomorphic to $\mathbf{Z}[x]/\langle x^2 + 1 \rangle$.

Solution: Define $\phi : \mathbf{Z}[x] \to \mathbf{C}$ by $\phi(f(x)) = f(i)$, for all $f(x) \in \mathbf{Z}[x]$. This is the mapping defined in Proposition 5.2.7, and so we know that it is a ring homomorphism. It is clear that $\phi(\mathbf{Z}[x]) = \mathbf{Z}[i]$ and that $x^2 + 1 \in \ker(\phi)$.

To show that $\ker(\phi) = \langle x^2 + 1 \rangle$, suppose that $f(x) \in \ker(\phi)$. Considering $f(x)$ as an element of $\mathbf{Q}[x]$, we can divide by $x^2 + 1$ to get $f(x) = q(x)(x^2 + 1) + r(x)$, where $r(x) = 0$ or $\deg(r(x)) < 2$. Since $x^2 + 1$ is monic, it is easy to see that $q(x)$ and $r(x)$ belong to $\mathbf{Z}[x]$, so $r(x) = m + nx$ for some $m, n \in \mathbf{Z}$. Substituting $x = i$ shows that $m + ni = 0$ in $\mathbf{C}$, so $m = n = 0$, and therefore $r(x)$ is the zero polynomial. Thus we have shown that $f(x) \in \langle x^2 + 1 \rangle$.

Since $\ker(\phi) = \langle x^2 + 1 \rangle$ and $\phi(\mathbf{Z}[x]) = \mathbf{Z}[i]$, it follows from the fundamental homomorphism theorem that $\mathbf{Z}[i] \cong \mathbf{Z}[x]/\langle x^2 + 1 \rangle$.

34. Show that the ring $\mathbf{Z}[\sqrt{2}]$ has precisely two automorphisms.

Solution: The first automorphism is the identity mapping. Exercise 5.2.7 in **Abstract Algebra** states that $\phi : \mathbf{Z}[\sqrt{2} \to \mathbf{Z}[\sqrt{2}]$ defined by $\phi(m + n\sqrt{2}) = m - n\sqrt{2}$ is also an automorphism. (You should check this.)

Why are these the only possible automorphisms? By definition, for any automorphism we must have $\phi(1) = 1$, and therefore $\phi(m) = m$ and $\phi(n) = n$ for $m + n\sqrt{2}$. Furthermore, $\phi(\sqrt{2})\phi(\sqrt{2}) = \phi(\sqrt{2}\sqrt{2}) = \phi(2) = 2$, which forces $\phi(\sqrt{2}) = \pm\sqrt{2}$. This shows that we have in fact found all possible automorphisms of $\mathbf{Z}[\sqrt{2}]$.

35. Let F be a field, and define $\phi : F[x] \to F[x]$ by $\phi(f(x)) = f(x^2)$, for all $f(x) \in F[x]$. Show that ϕ is a one-to-one ring homomorphism that is not an automorphism of $F[x]$.

Solution: Substituting x^2 into $f(x)$ and $g(x)$ and then adding (or multiplying) is the same as adding (or multiplying) $f(x)$ and $g(x)$ and then substituting x^2, so ϕ respects the addition and multiplication in $F[x]$. It is clear that $\phi(1) = 1$. The image of ϕ is the set of polynomials in $F[x]$ for which every exponent is even, so it is clear that ϕ is one-to-one but not onto.

36. Find an example of an infinite integral domain that has finite characteristic.

Solution: Let $D = \mathbf{Z}_2[x]$. Then D is certainly infinite and it is an integral domain since $\mathbf{Z}_2$ is a field. We have $\text{char}(D) = 2$ since $1 + 1 = 0$ in Z_2.

37. What is the characteristic of $\mathbf{Z}_m \oplus \mathbf{Z}_n$?

Solution: Recall that the characteristic is the additive order of the identity element $(1, 1)$. From group theory we know that the order of an element is a direct product is the least common multiple of the orders of the components. It follows that $\mathbf{Z}_m \oplus \mathbf{Z}_n$ has characteristic $\text{lcm}[m, n]$.

38. Let R be a commutative ring with $\text{char}(R) = 2$. Define $\phi : R \to R$ by $\phi(x) = x^2$, for all $x \in R$.

(a) Show that ϕ is a ring homomorphism.

Solution: Let $a, b \in R$. Remember that $2x = 0$ for $x \in R$, since $\text{char}(R) = 2$.Then $\phi(a + b) = (a + b)^2 = a^2 + 2ab + b^2 = a^2 + b^2 = \phi(a) + \phi(b)$, and $\phi(ab) = (ab)^2 = a^b b^2 = \phi(a)\phi(b)$, so ϕ respects addition and multiplication. Finally, $\phi(1) = 1^2 = 1$.

(b) Find an example of such a ring in which ϕ is an automorphism.

Solution: Let R be any Boolean ring. We know that it has characteristic 2, and on such a ring ϕ is just the identity mapping.

(c) Find an example of such a ring in which ϕ is not onto.

Solution: The polynomial ring $\mathbf{Z}_2[x]$ has characteristic 2, and in the image of ϕ every polynomial has even degree, so ϕ is not onto.

39. In the multiplicative group $\mathbf{Z}_{180}^{\times}$ of the ring $\mathbf{Z}_{180}$, what is the largest possible order of an element?

Solution: Since $180 = 2^2 \cdot 3^2 \cdot 5$, it follows that $\mathbf{Z}_{180} \cong \mathbf{Z}_4 \oplus \mathbf{Z}_9 \oplus \mathbf{Z}_5$ as rings. Therefore

$$\mathbf{Z}_{180}^{\times} \cong \mathbf{Z}_4^{\times} \times \mathbf{Z}_9^{\times} \times \mathbf{Z}_5^{\times} \cong \mathbf{Z}_2 \times \mathbf{Z}_6 \times \mathbf{Z}_4 \ .$$

In the latter additive group the order of an element is the least common multiple of the orders of its components. It follows that the largest possible order of an element is $\text{lcm}[2, 6, 4] = 12$.

Comment: For background on the description of $\mathbf{Z}_{180}^{\times}$, see Theorem 3.5.5, Example 5.2.13 in **Abstract Algebra**, and Problem 5.1.42.

40. Find all group homomorphisms $\phi : \mathbf{Z}_{120} \to \mathbf{Z}_{42}$ such that

$$\phi([a]_{120}[b]_{120}) = \phi([a]_{120})\phi([b]_{120})$$

for all $[a]_{120}, [b]_{120} \in \mathbf{Z}_{120}$.

Note: These are not ring homomorphisms, since we are not requiring that $\phi([1]_{120}) = [1]_{42}$. Exercise 5.2.15 shows that there is only one possible ring homomorphism.

Solution: Let $\phi : \mathbf{Z}_{120} \to \mathbf{Z}_{42}$ be a function that satisfies the given conditions. The additive order of $\phi(1)$ must be a divisor of $\gcd(120, 42) = 6$, so it must belong to the subgroup $7\mathbf{Z}_{42} = \{0, 7, 14, 21, 28, 35\}$. Furthermore, $\phi(1)$ must be an idempotent, element, since $(\phi([1]_{120}))^2 = \phi([1]_{120})\phi([1]_{120}) = \phi([1]_{120})$. It can be checked that in $7\mathbf{Z}_{42}$, only $0, 7, 21, 28$ are idempotent.

If $\phi(1) = 7$, then the image is $7\mathbf{Z}_{42}$ and the kernel is $6\mathbf{Z}_{120}$. If $\phi(1) = 21$, then the image is $21\mathbf{Z}_{42}$ and the kernel is $2\mathbf{Z}_{120}$. If $\phi(1) = 28$, then the image is $14\mathbf{Z}_{42}$ and the kernel is $3\mathbf{Z}_{120}$.

ANSWERS AND HINTS

43. Let R and S be commutative rings, and let $\phi : R \to S$ be a ring homomorphism.
(a) Give an example in which R is an integral domain but S is not.
Answer: Let ϕ be the projection mapping from $\mathbf{Z}$ onto $\mathbf{Z}_4$.
(b) Give an example in which R is an field but S is not.
Answer: Let ϕ be the inclusion mapping from $\mathbf{R}$ into $\mathbf{R}[x]$.

46. Show that if R and S are isomorphic commutative rings, then the polynomial rings $R[x]$ and $S[x]$ are isomorphic.
Hint: If $\phi : R \to S$ is an isomorphism, define $\Phi : R[x] \to S[x]$ by
$\Phi(a_0 + a_1x + \ldots + a_nx^n) = \phi(a_0) + \phi(a_1)x + \ldots + \phi(a_n)x^n$.

5.3 Ideals and Factor Rings

27. Give an example to show that the set of all zero divisors of a commutative ring need not be an ideal of the ring.

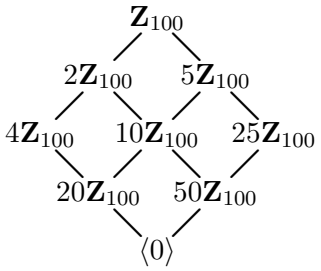
Solution: The elements $(1,0)$ and $(0,1)$ of $\mathbf{Z}\times\mathbf{Z}$ are zero divisors, but if the set of zero divisors were closed under addition it would include $(1,1)$, an obvious contradiction.

28. Show that in $\mathbf{R}[x]$ the set of polynomials whose graph passes through the origin and is tangent to the x-axis at the origin is an ideal of $\mathbf{R}[x]$.

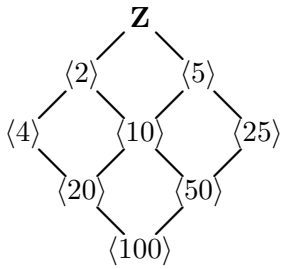
Solution: We can characterize the given set as $I = \{f(x)\mathbf{R}[x] \mid f(0) = 0 \text{ and } f'(x) = 0\}$. Using this characterization of I, it is easy to check that if $f(x), g(x) \in I$, then $f(x) \pm g(x) \in I$. If $g(x) \in \mathbf{R}[x]$ and $f(x) \in I$, then $g(0)f(0) = g(0)\cdot 0 = 0$, and $D_x(g(x)f(x)) = g'(x)f(x) + g(x)f'(x)$, and so evaluating at $x = 0$ gives $g'(0)f(0) + g(0)f'(0) = g'(0)\cdot 0 + g(0)\cdot 0 = 0$. This shows that I is an ideal of $\mathbf{R}[x]$.

29. To illustrate Proposition 5.3.7 (b), give the lattice diagram of ideals of $\mathbf{Z}_{100} = \mathbf{Z}/\langle 100\rangle$, and the lattice diagram of ideals of $\mathbf{Z}$ that contain $\langle 100\rangle$.

Solution: Since multiplication in $\mathbf{Z}_{100}$ corresponds to repeated addition, each subgroup of $\mathbf{Z}_{100}$ is an ideal, and the lattice diagram is the same as that of the subgroups of $\mathbf{Z}_{100}$, given in the following diagram.



The ideals of $\mathbf{Z}$ that contain $\langle 100\rangle$ correspond to the positive divisors of 100.



30. Let R be the ring $\mathbf{Z}_2[x]/\langle x^3+1\rangle$.

Comment: Table 5.1 gives the multiplication table, though it is not necessary to compute it in order to solve the problem.

Table 5.1: Multiplication in $\mathbf{Z}_2[x]/\langle x^3+1\rangle$

$\times$	x^2+x	$x+1$	x^2+1	x^2+x+1	1	x	x^2
x^2+x	x^2+x	$x+1$	x^2+1	0	x^2+x	x^2+1	$x+1$
$x+1$	$x+1$	x^2+1	x^2+x	0	$x+1$	x^2+x	x^2+1
x^2+1	x^2+1	x^2+x	$x+1$	0	x^2+1	$x+1$	x^2+x
x^2+x+1	0	0	0	x^2+x+1	x^2+x+1	x^2+x+1	x^2+x+1
1	x^2+x	$x+1$	x^2+1	x^2+x+1	1	x	x^2
x	x^2+1	x^2+x	$x+1$	x^2+x+1	x	x^2	1
x^2	$x+1$	x^2+1	x^2+x	x^2+x+1	x^2	1	x

(a) Find all ideals of R.

Solution: By Proposition 5.3.7 (b), the ideals of R correspond to the ideals of $\mathbf{Z}_2[x]$ that contain $\langle x^3+1\rangle$. We have the factorization $x^3+1 = x^3-1 = (x-1)(x^2+x+1)$, so the only proper, nonzero ideals are the principal ideals given below.

$A = \langle [x+1]\rangle = \{[0], [x^2+x], [x+1], [x^2+1]\}$

$B = \langle [x^2+x+1]\rangle = \{[0], [x^2+x+1]\}$

Comment: We note that $R = A \oplus B$, accounting for its 8 elements.

(b) Find the units of R.

Solution: We have $[x]^3 = [1]$, so $[x]$ and $[x^2]$ are units. To show that the only units are 1, $[x]$, and $[x^2]$, note that $[x+1][x^2+x+1] = [x^3+1] = [0]$, so $[x+1]$ and $[x^2+x+1]$ cannot be units. This also excludes $[x^2+x] = [x][x+1]$ and $[x^2+1] = [x^2][1+x]$.

(c) Find the idempotent elements of R.

Solution: Using the general fact that $(a+b)^2 = a^2+2ab+b^2 = a^2+b^2$ (since $\mathbf{Z}_2[x]$ has characteristic 2) and the identities $[x^3] = [1]$ and $[x^4] = [x]$, it is easy to see that the idempotent elements of R are [0], [1], $[x^2+x+1]$, and $[x^2+x]$.

31. Let S be the ring $\mathbf{Z}_2[x]/\langle x^3+x\rangle$.

Comment: It isn't necessary to construct Table 5.2 in order to answer (a) and (b).

(a) Find all ideals of S.

Solution: Over $\mathbf{Z}_2$ we have the factorization $x^3+x = x(x^2+1) = x(x+1)^2$, so by Proposition 5.3.7 (b) the proper nonzero ideals of S are the principal ideals generated by $[x]$, $[x+1]$, $[x^2+1] = [x+1]^2$, and $[x^2+x] = [x][x+1]$.

$A = \langle [x]\rangle = \{[0], [x^2], [x], [x^2+x]\} \supseteq C = \langle [x^2+x]\rangle = \{[0], [x^2+x]\}$

$B = \langle [x^2+1]\rangle = \{[0], [x^2+1]\}$ $\quad B+C = \langle [x+1]\rangle = \{[0], [x+1], [x^2+1], [x^2+x]\}$

Comment: We note that $S = A \oplus B$.

(b) Find the units of S.

Table 5.2: Multiplication in $\mathbf{Z}_2[x]/\langle x^3+x\rangle$

$\times$	x^2	x	x^2+x	x^2+1	$x+1$	1	x^2+x+1
x^2	x^2	x	x^2+x	0	x^2+x	x^2	x^2
x	x	x^2	x^2+x	0	x^2+x	x	x
x^2+x	x^2+x	x^2+x	0	0	0	x^2+x	x^2+x
x^2+1	0	0	0	x^2+1	x^2+1	x^2+1	x^2+1
$x+1$	x^2+x	x^2+x	0	x^2+1	x^2+1	$x+1$	$x+1$
1	x^2	x	x^2+x	x^2+1	$x+1$	1	x^2+x+1
x^2+x+1	x^2	x	x^2+x	x^2+1	$x+1$	x^2+x+1	1

Solution: Since no unit can belong to a proper ideal, it follows from part (a) that we only need to check $[x^2+x+1]$. This is a unit since $[x^2+x+1]^2=[1]$.

(c) Find the idempotent elements of S.

Solution: Since $[x^3]=[x]$, we have $[x^2]^2=[x^2]$, and then $[x^2+1]^2=[x^2+1]$. These, together with $[0]$ and $[1]$, are the only idempotents.

32. Show that the rings R and S in Problems 30 and 31 are isomorphic as abelian groups, but not as rings.

Solution: Both R and S are isomorphic to $\mathbf{Z}_2\times Z_2\times\mathbf{Z}_2$, as abelian groups. They cannot be isomorphic as rings since S has a nonzero nilpotent element, $[x^2+x]$, but R does not. We can also prove this by noting that the given multiplication tables show that R has 3 units, while S has only 2.

33. Let I,J be ideals of the commutative ring R, and for $r\in R$, define the function $\phi: R\to R/I\oplus R/J$ by $\phi(r)=(r+I,r+J)$.

(a) Show that ϕ is a ring homomorphism, with $\ker(\phi)=I\cap J$.

Solution: The fact that ϕ is a ring homomorphism follows immediately from the definitions of the operations in a direct sum and in a factor ring. Since the zero element of $R/I\oplus R/J$ is $(0+I,0+J)$, we have $r\in\ker(\phi)$ if and only if $r\in I$ and $r\in J$, so $\ker(\phi)=I\cap J$.

(b) Show that if $I+J=R$, then ϕ is onto, and thus $R/(I\cap J)\cong R/I\oplus R/J$.

Solution: If $I+J=R$, then we can write $1=x+y$, for some $x\in I$ and $y\in J$. Given any element $(a+I,b+J)\in R/I\oplus R/J$, consider $r=bx+ay$, noting that $a=ax+ay$ and $b=bx+by$. We have $a-r=a-bx-ay=ax-bx\in I$, and $b-r=b-bx-ay=by-ay\in J$. Thus $\phi(r)=(a+I,b+J)$, and ϕ is onto. The isomorphism follows from the fundamental homomorphism theorem.

Comment: This result is sometimes called the Chinese remainder theorem for commutative rings. It is interesting to compare this proof with the one given for Theorem 1.3.6.

34. Let I, J be ideals of the commutative ring R. Show that if $I+J = R$, then $I^2+J^2 = R$.

Solution: If $I + J = R$, then there exist $a \in I$ and $b \in J$ with $a + b = 1$. Cubing both sides gives us $a^3+3a^2b+3ab^2+b^3 = 1$. Then we only need to note that $a^3+3a^2b \in I^2$ and $3ab^2 + b^3 \in J^2$.

35. Show that $\langle x^2 + 1\rangle$ is a maximal ideal of $\mathbf{R}[x]$.

Solution: Since x^2+1 is irreducible over $\mathbf{R}$, it follows from results in Chapter 4 that $\mathbf{R}[x]/\langle x^2 + 1\rangle$ is a field. Therefore $\langle x^2 + 1\rangle$ is a maximal ideal.

36. Is $\langle x^2 + 1\rangle$ a maximal ideal of $\mathbf{Z}_2[x]$?

Solution: Since $x^2 + 1$ is not irreducible over $\mathbf{Z}_2$, the ideal it generates is not a maximal ideal. In fact, $x + 1$ generates a larger ideal since it is a factor of $x^2 + 1$.

37. Let R and S be commutative rings, and let $\phi : R \to S$ be a ring homomorphism.

(a) Show that if I is an ideal of S, then $\phi^{-1}(I) = \{a \in R \mid \phi(a) \in I\}$ is an ideal of R.

Solution: If $a, b \in \phi^{-1}(I)$, then $\phi(a) \in I$ and $\phi(b) \in I$, so $\phi(a \pm b) = \phi(a) \pm \phi(b) \in I$, and therefore $a \pm b \in \phi^{-1}(I)$. If $r \in R$, then $\phi(ra) = \phi(r)\phi(a) \in I$, and therefore $ra \in \phi^{-1}(I)$. By Definition 5.3.1, this shows that $\phi^{-1}(I)$ is an ideal of R.

(b) Show that if P is a prime ideal of S, then $\phi^{-1}(P)$ is a prime ideal of R.

Solution: Suppose that P is a prime ideal of R and $ab \in \phi^{-1}(P)$ for $a, b \in R$. Then $\phi(a)\phi(b) = \phi(ab) \in P$, so $\phi(a) \in P$ or $\phi(b) \in P$ since P is prime. Thus $a \in \phi^{-1}(P)$ or $b \in \phi^{-1}(P)$, showing that $\phi^{-1}(P)$ is prime in R.

38. Prove that in a Boolean ring every prime ideal is maximal.

Solution: We will prove a stronger result: if R is a Boolean ring and P is a prime ideal of R, then $R/P \cong \mathbf{Z}_2$. Since $\mathbf{Z}_2$ is a field, Proposition 5.3.9 (a) implies that P is a maximal ideal.

If $a \in R$, then $a^2 = a$, and so $a(a - 1) = 0$. Since P is an ideal, it contains 0, and then $a(a - 1) \in P$ implies $a \in P$ or $a - 1 \in P$, since P is prime. Thus each element of R is in either P or $1 + P$, so there are only two cosets of P in R/P, and therefore R/P must be the ring $\mathbf{Z}_2$.

39. In $R = \mathbf{Z}[i]$, let $I = \{m + ni \mid m \equiv n \pmod 2\}$.

(a) Show that I is an ideal of R.

Solution: Let $a + bi$ and $c + di$ belong to I. Then $a \equiv b \pmod 2$ and $c \equiv d \pmod 2$, so $a+c \equiv b+d \pmod 2$ and $a-c \equiv b-d \pmod 2$, and therefore $(a+bi)\pm(c+di) \in I$. For $m+ni \in R$, we have $(m+ni)(a+bi) = (ma-nb)+(na+mb)i$. Then $ma-nb \equiv na + mb \pmod 2$ since $n \equiv m \pmod 2$ and $-nb \equiv nb \pmod 2$. This completes the proof that I is an ideal of R.

(b) Find a familiar commutative ring isomorphic to R/I.

Solution: Note that $m + ni \in I$ if and only if $m - n \equiv 0 \pmod 2$. Furthermore, $m + ni \in 1 + I$ if and only if $1 - (m + ni) \in I$, and this occurs if and only if

$1 - m \equiv -n \pmod 2$ if and only if $m - n \equiv 1 \pmod 2$. Since any element of $m + ni$ R satisfies either $m - n \equiv 0 \pmod 2$ or $m - n \equiv 1 \pmod 2$, the only cosets in R/I are $0 + I$ and $1 + I$. Therefore $R/I \cong \mathbf{Z}_2$.

ANSWERS AND HINTS

45. Let P and Q be maximal ideals of the commutative ring R. Show that $R/(P \cap Q) \cong R/P \oplus R/Q$.
Hint: If you can show that $P + Q = R$, then you can use Problem 33 (b).

48. Show that in $\mathbf{Z}[\sqrt{2}]$ the principal ideal generated by $\sqrt{2}$ is a maximal ideal.
Hint: Define a ring homomorphism from $\mathbf{Z}[\sqrt{2}]$ onto $\mathbf{Z}_2$.

5.4 Quotient Fields

15. Let F be a field. Explain why $Q(F)$ is isomorphic to F. Why can't we just say that $Q(F) = F$?

Solution: Formally, $Q(F)$ is a set of equivalence classes of ordered pairs of elements of F, so it is not simply equal to the original set F.

In the general construction, we identified $d \in D$ with the equivalence class $[d, 1]$, and used this to show that D is isomorphic to a subring of $Q(D)$. When D is a field, the equivalence class $[a, b]$ is equal to the equivalence class $[ab^{-1}, 1]$ since $a \cdot 1 = b \cdot ab^{-1}$. This shows that when D is a field we have $Q(D) \cong D$.

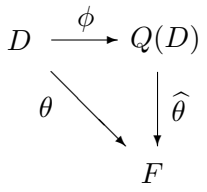
16. Find the quotient field of $\mathbf{Z}_2[x]$.

Solution: We need to formally invert all nonzero polynomials in $\mathbf{Z}_2[x]$. This produces what look like rational functions, though we do not think of them as functions taking values in $\mathbf{Z}_2$ since as functions things would collapse. (Remember that as functions we have $x^2 = x$.) The set of fractions of the form $\dfrac{f(x)}{g(x)}$ such that $f(x), g(x) \in \mathbf{Z}_2[x]$, where $g(x)$ is not the zero polynomial, is denoted by $\mathbf{Z}_2(x)$, and is called the rational function field over $\mathbf{Z}_2$.

17. Prove that if D_1 and D_2 are isomorphic integral domains, then $Q(D_1) \cong Q(D_2)$.

Solution: Let D_1 and D_2 be isomorphic integral domains, with isomorphism $\alpha : D_1 \to D_2$ and $\beta = \alpha^{-1}$. Let $\phi_1 : D_1 \to Q(D_1)$ and $\phi_2 : D_2 \to Q(D_2)$ be the standard mappings defined in Theorem 5.4.6.

Recall that we have the following diagram from Theorem 5.4.6, in which any one-to-one ring homomorphism $\theta : D \to F$, where F is a field, gives rise to a unique ring homomorphism $\widehat{\theta} : Q(D) \to F$ such that $\widehat{\theta}\phi = \theta$.



In the above diagram, we first let $D = D_1$, $\phi = \phi_1$, $F = Q(D_2)$, and $\theta = \phi_2\alpha$. We therefore get $\widehat{\phi_2\alpha} : Q(D_1) \to Q(D_2)$ with $\widehat{\phi_2\alpha}\phi_1 = \phi_2\alpha$. Similarly, letting $D = D_2$, $\phi = \phi_2$, $F = Q(D_1)$, and $\theta = \phi_1\beta$ we get $\widehat{\phi_1\beta} : Q(D_2) \to Q(D_1)$ with $\widehat{\phi_1\beta}\phi_2 = \phi_1\beta$. In following this part of the argument, it may help to draw the corresponding diagrams.

We claim that $\widehat{\phi_2\alpha}$ is the isomorphism we are looking for, with inverse $\widehat{\phi_1\beta}$. To show this, in the original diagram take $D = D_1$, $\phi = \phi_1$, $F = Q(D_1)$, and $\theta = \phi_1$. Then the identity mapping from $Q(D_1)$ to $Q(D_1$ fits the role of $\widehat{\phi_1}$, since $1_{Q(D_1)}\phi_1 = \phi_1$, and it is the unique ring homomorphism for which this is true.

On the other hand, consider $\widehat{\phi_1\beta}\widehat{\phi_2\alpha} : Q(D_1) \to Q(D_2)$. We have $(\widehat{\phi_1\beta}\widehat{\phi_2\alpha})\phi_1 = \widehat{\phi_1\beta}(\phi_2\alpha) = (\phi_1\beta)\alpha = \phi_1(\beta\alpha) = \phi_1$, and so the uniqueness guaranteed by Theorem 5.4.6 implies that $\widehat{\phi_1\beta}\widehat{\phi_2\alpha}$ is the identity mapping. A similar argument shows that $\widehat{\phi_2\alpha}\widehat{\phi_1\beta} : Q(D_2) \to Q(D_1)$ is the identity mapping. This completes the proof that $Q(D_1) \cong Q(D_2)$.

Comment: It is also possible to directly define an isomorphism $\theta : Q(D_1) \to Q(D_2)$ by setting $\theta([a, b]) = [\alpha(a), \alpha(b)]$. The argument given above is a standard one for any "universal" construction that guarantees the existence of a unique mapping. If you continue your study of mathematics, you are likely to encounter arguments like this in more general situations.

ANSWERS AND HINTS

18. Find the quotient field of $\mathbf{Z}[\sqrt{3}i]$.
Answer: $\mathbf{Q}(\sqrt{3}i)$

19. Find the quotient field of $D = \left\{ \begin{bmatrix} m & n \\ -3n & m \end{bmatrix} \middle| m, n \in \mathbf{Z} \right\}$.
Hint: Let $F = \left\{ \begin{bmatrix} a & b \\ -3b & a \end{bmatrix} \middle| a, b \in \mathbf{Q} \right\}$. To apply Corollary 5.4.7, show that every element of F can be written in the form $\begin{bmatrix} m & n \\ -3n & m \end{bmatrix} \begin{bmatrix} d & 0 \\ 0 & d \end{bmatrix}^{-1}$ for some $m, n, d \in \mathbf{Z}$.
Answer: $Q(D) \cong F$.

20. Find the quotient field of $D = \left\{ \begin{bmatrix} m & n \\ -n & m \end{bmatrix} \middle| m, n \in \mathbf{Z} \right\}$.
Answer: $Q(D) = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| a, b \in \mathbf{Q} \right\}$

Review Problems

1. Let R be the ring with 8 elements consisting of all 3×3 matrices with entries in $\mathbf{Z}_2$ which have the following form:

$$\begin{bmatrix} a & 0 & 0 \\ 0 & a & 0 \\ b & c & a \end{bmatrix}$$

You may assume that the standard laws for addition and multiplication of matrices are valid.

(a) Show that R is a commutative ring (you only need to check closure, the existence of a 1, and commutativity of multiplication).

Solution: It is clear that the set is closed under addition, and the following computation checks closure under multiplication.

$$\begin{bmatrix} a & 0 & 0 \\ 0 & a & 0 \\ b & c & a \end{bmatrix} \begin{bmatrix} x & 0 & 0 \\ 0 & x & 0 \\ y & z & x \end{bmatrix} = \begin{bmatrix} ax & 0 & 0 \\ 0 & ax & 0 \\ bx+ay & cx+az & ax \end{bmatrix}$$

The identity matrix serves as an identity element. Because of the symmetry $a \leftrightarrow x$, $b \leftrightarrow y$, $c \leftrightarrow z$, the above computation also checks commutativity.

(b) Find all units of R, and all nilpotent elements of R.

Solution: Four of the matrices in R have 1's on the diagonal, and these are invertible since their determinant is nonzero. Squaring each of the other four matrices gives the zero matrix, and so they are nilpotent.

(c) Find all idempotent elements of R.

Solution: By part (b), an element in R is either a unit or nilpotent. The only unit that is idempotent is the identity matrix (in a group, the only idempotent element is the identity) and the only nilpotent element that is also idempotent is the zero matrix.

2. Let R be the ring $\mathbf{Z}_2[x]/\langle x^2+1 \rangle$. Show that although R has 4 elements, it is not ring isomorphic to either $\mathbf{Z}_4$ or $\mathbf{Z}_2 \oplus \mathbf{Z}_2$.

Solution: In R we have $a + a = 0$, for all $a \in R$ (since $\mathrm{char}(R) = 2$), so R is not isomorphic to $\mathbf{Z}_4$. On the other hand, in R we have $[x+1] \neq [0]$ but $[x+1]^2 = [x^2+1] = [0]$. Thus R cannot be isomorphic to $\mathbf{Z}_2 \oplus \mathbf{Z}_2$, since in that ring $(a, b)^2 = (0, 0)$ implies $a^2 = 0$ and $b^2 = 0$, and this implies $a = 0$ and $b = 0$ since $\mathbf{Z}_2$ is a field.

3. Let R and S be commutative rings. Prove that $R \oplus S \cong S \oplus R$.

Solution: Define $\phi : R \oplus S \to S \oplus R$ by $\phi((r, s)) = (s, r)$, for all $(r, s) \in R \oplus S$. Then $\phi((r_1, s_1) + (r_2, s_2)) = \phi((r_1 + r_2, s_1 + s_2)) = (s_1 + s_2, r_1 + r_2) = (s_1, r_1) + (s_2, r_2) = \phi((r_1, s_1)) + \phi((r_2, s_2))$ and $\phi((r_1, s_1) \cdot (r_2, s_2)) = \phi((r_1 r_2, s_1 s_2)) = (s_1 s_2, r_1 r_2) = (s_1, r_1) \cdot (s_2, r_2) = \phi((r_1, s_1)) \cdot \phi((r_2, s_2))$. Finally, $\phi(1_R, 1_S) = (1_S, 1_R)$, where 1_R is the identity of R and 1_S is the identity of S. Clearly ϕ is a one-to-one correspondence.

4. For the element $a = (0, 2)$ of the ring $R = \mathbf{Z}_{12} \oplus \mathbf{Z}_8$, find $\text{Ann}(a) = \{r \in R \mid ra = 0\}$. Check that $\text{Ann}(a)$ is an ideal of R.

   Solution: We need to solve $(x, y)(0, 2) = (0, 0)$ for $(x, y) \in \mathbf{Z}_{12} \oplus \mathbf{Z}_8$. We only need $2y \equiv 0 \pmod 8$, so the first component x can be any element of $\mathbf{Z}_{12}$, while $y = 0, 4$. Thus $\text{Ann}((0, 2)) = \mathbf{Z}_{12} \oplus 4\mathbf{Z}_8$. This set is certainly closed under addition, and it is also closed under multiplication by any element of R since $4\mathbf{Z}_8$ is an ideal of $\mathbf{Z}_8$.

   Comment: Exercise 5.3.11 shows that $\text{Ann}(a)$ is always an ideal.

5. Let R be the ring $\mathbf{Z}_2[x]/\langle x^4 + 1\rangle$, and let I be the set of all congruence classes in R of the form $[f(x)(x^2 + 1)]$.

   (a) Show that I is an ideal of R.

   (b) Show that $R/I \cong \mathbf{Z}_2[x]/\langle x^2 + 1\rangle$.

   Solution: (to (a) and (b)) Define $\phi : \mathbf{Z}_2[x]/\langle x^4 + 1\rangle \to \mathbf{Z}_2[x]/\langle x^2 + 1\rangle$ by $\phi(f(x) + \langle x^4 + 1\rangle) = (f(x) + \langle x^2 + 1\rangle)$. This mapping is well-defined since $x^2 + 1$ is a factor of $x^4 + 1$ over $\mathbf{Z}_2$. It is not difficult to show that ϕ is an onto ring homomorphism, with kernel equal to I.

   (c) Is I a prime ideal of R?

   Solution: No: $(x + 1)(x + 1) \equiv 0 \pmod{x^2 + 1}$.

   Hint: If you use the fundamental homomorphism theorem, you can do the first two parts together.

6. Find all maximal ideals, and all prime ideals, of $\mathbf{Z}_{36} = \mathbf{Z}/36\mathbf{Z}$.

   Solution: If P is a prime ideal of $\mathbf{Z}_{36}$, then $\mathbf{Z}_{36}/P$ is a finite integral domain, so it is a field, and hence P is maximal. Thus we only need to find the maximal ideals of $\mathbf{Z}_{36}$. The lattice of ideals of $\mathbf{Z}_{36}$ is exactly the same as the lattice of subgroups, so the maximal ideals of $\mathbf{Z}36$ correspond to the prime divisors of 36. The maximal ideals of $\mathbf{Z}_{36}$ are thus $2\mathbf{Z}_{36}$ and $3\mathbf{Z}_{36}$.

   Alternate solution: We can use Proposition 5.3.7, which shows that there is a one-to-one correspondence between the ideals of $\mathbf{Z}/36\mathbf{Z}$ and the ideals of $\mathbf{Z}$ that contain $36\mathbf{Z}$. In $\mathbf{Z}$ every ideal is principal, so the relevant ideals correspond to the divisors of 36. Again, the maximal ideals that contain $36\mathbf{Z}$ are $2\mathbf{Z}$ and $3\mathbf{Z}$, and these correspond to $2\mathbf{Z}_{36}$ and $3\mathbf{Z}_{36}$.

7. Let I be the subset of $\mathbf{Z}[x]$ consisting of all polynomials with even coefficients. Prove that I is a prime ideal; prove that I is not maximal.

   Solution: Define $\phi : \mathbf{Z}[x] \to \mathbf{Z}_2[x]$ by reducing coefficients modulo 2. This is an onto ring homomorphism with kernel I. Then R/I is isomorphic to $\mathbf{Z}_2[x]$, which is an integral domain, so I is a prime ideal. On the other hand, $\mathbf{Z}_2[x]$ is not a field, so I is not maximal.

8. Let $\mathbf{Z}[i]$ be the ring of Gaussian integers, i.e. the subring of $\mathbf{C}$ given by

$$\mathbf{Z}[i] = \{m + ni \in \mathbf{C} \mid m, n \in \mathbf{Z}\} .$$

(a) Define $\phi : \mathbf{Z}[i] \to \mathbf{Z}_2$ by $\phi(m+ni) = [m+n]_2$. Prove that ϕ is a ring homomorphism. Find $\ker(\phi)$ and show that it is a principal ideal of $\mathbf{Z}[i]$.

Solution: It is clear that $\phi(1) = 1$, and we have the following computations which show that ϕ is a ring homomorphism.

$$\begin{aligned} \phi((a+bi)+(c+di)) &= \phi((a+c)+(b+d)i) = [a+c+b+d]_2 \\ \phi((a+bi))+\phi((c+di)) &= [a+b]_2+[c+d]_2 = [a+b+c+d]_2 \end{aligned}$$

$$\begin{aligned} \phi((a+bi)(c+di)) &= \phi((ac-bd)+(ad+bc)i) = [ac-bd+ad+bc]_2 \\ \phi((a+bi))\phi((c+di)) &= [a+b]_2 \cdot [c+d]_2 = [ac+ad+bc+bd]_2 \, . \end{aligned}$$

We claim that $\ker(\phi)$ is generated by $1+i$. It is clear that $1+i$ is in the kernel, and we note that $(1-i)(1+i) = 2$. Let $m+ni \in \ker(\phi) = \{m+ni \mid m+n \equiv 0 \pmod 2\}$. Then m and n are either both even or both odd, and so it follows that $m-n$ is always even. Therefore

$$\begin{aligned} m+ni &= (m-n)+n+ni = (m-n)+n(1+i) \\ &= \left(\frac{m-n}{2}\right)(1-i)(1+i)+n(1+i) \\ &= \left[\frac{1}{2}(m-n)(1-i)+n\right](1+i) \, , \end{aligned}$$

and so $m+ni$ belongs to the principal ideal generated by $1+i$.

Comment: Note that $\ker(\phi)$ is the ideal I of Problem 5.3.39.

(b) For any prime number p, define $\theta : \mathbf{Z}[i] \to \mathbf{Z}_p[x]/\langle x^2+1\rangle$ by $\theta(m+ni) = [m+nx]$. Prove that θ is an onto ring homomorphism.

Solution: We have the following computations, which show that θ is a ring homomorphism. We need to use the fact that $[x^2] = [-1]$ in $\mathbf{Z}_p[x]/\langle x^2+1\rangle$.

$$\begin{aligned} \theta((a+bi)+(c+di)) &= \theta((a+c)+(b+d)i) = [(a+c)+(b+d)x] \\ \theta((a+bi))+\theta((c+di)) &= [a+bx]+[c+dx] = [(a+c)+(b+d)x] \end{aligned}$$

$$\begin{aligned} \theta((a+bi)(c+di)) &= \theta((ac-bd)+(ad+bc)i) = [(ac-bd)+(ad+bc)x] \\ \theta((a+bi))\phi((c+di)) &= [a+bx][c+dx] = [ac+(ad+bc)x+bdx^2] \, . \end{aligned}$$

Since the elements of $\mathbf{Z}_p[x]/\langle x^2+1\rangle$ all have the form $[a+bx]$, for some congruence classes a and b in $\mathbf{Z}_p$, it is clear the θ is an onto function.

Chapter 6

Fields

6.1 Algebraic Elements

13. Let u be a root of the polynomial $x^3 + 3x + 3$. In $\mathbf{Q}(u)$, express $(7 - 2u + u^2)^{-1}$ in the form $a + bu + cu^2$.

    Solution: Dividing $x^3 + 3x + 3$ by $x^2 - 2x + 7$ gives the quotient $x + 2$ and remainder -11. Thus $u^3 + 3u + 3 = (u+2)(u^2 - 2u + 7) - 11$, and so $(7 - 2u + u^2)^{-1} = (2+u)/11 = (2/11) + (1/11)u$.

14. Find the minimal polynomial of the real number $1 + \sqrt[3]{2}$ over $\mathbf{Q}$.

    Solution: Let $x = 1 + \sqrt[3]{2}$. Then $x - 1 = \sqrt[3]{2}$, and so $(x-1)^3 = 2$, which yields $x^3 - 3x^2 + 3x - 1 = 2$, and therefore $x^3 - 3x^2 + 3x - 3 = 0$. Eisenstein's criterion (with $p = 3$) shows that $x^3 - 3x^2 + 3x - 3$ is irreducible over $\mathbf{Q}$, so this is the required minimal polynomial.

15. Find the minimal polynomial of the complex number $1 + \sqrt{3}i$ over $\mathbf{Q}$.

    Solution: Let $x = 1 + \sqrt{3}i$. Then $x - 1 = \sqrt{3}i$, and so $(x-1)^2 = -3$, and therefore $x^2 - 2x + 4 = 0$. Since $1 + \sqrt{3}i \notin \mathbf{Q}$, it follows that $x^2 - 2x + 4$ is the minimal polynomial of $1 + \sqrt{3}i$ over $\mathbf{Q}$.

16. (a) Show that $\mathbf{Q}(\sqrt{2} + i) = \mathbf{Q}(\sqrt{2}, i)$.

    Solution: Let $u = \sqrt{2} + i$. Then $(\sqrt{2}+i)(\sqrt{2}-i) = 2 - i^2 = 3$, so $\sqrt{2} - i = 3(\sqrt{2}+i)^{-1} \in \mathbf{Q}(u)$, and it follows easily that $\sqrt{2} \in \mathbf{Q}(u)$ and $i \in \mathbf{Q}(u)$, so $\mathbf{Q}(\sqrt{2}, i) \subseteq \mathbf{Q}(u)$. The reverse inclusion is obvious.

    (b) Find the minimal polynomial of the complex number $\sqrt{2} + i$ over $\mathbf{Q}$.

    Solution: We have $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}) \subseteq \mathbf{Q}(\sqrt{2}, i)$. Thus $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$ since $\sqrt{2}$ is a root of a polynomial of degree 2 but is not in $\mathbf{Q}$. We have $[\mathbf{Q}(\sqrt{2}, i) : \mathbf{Q}(\sqrt{2})] = 2$ since i is a root of a polynomial of degree 2 over $\mathbf{Q}(\sqrt{2})$ but is not in $\mathbf{Q}(\sqrt{2})$. Thus $[\mathbf{Q}(\sqrt{2} + i) : \mathbf{Q}] = 4$, and so the minimal polynomial for $\sqrt{2} + i$ must have degree 4.

    Since $u = \sqrt{2} + i$, we have $u - i = \sqrt{2}$, $u^2 - 2iu + i^2 = 2$, and $u^2 - 3 = 2iu$. Squaring again and combining terms gives $u^4 - 2u^2 + 9 = 0$. Thus the minimal polynomial for $\sqrt{2} + i$ is $x^4 - 2x^2 + 9$.

17. Show that the polynomial $f(x) = x^2 + x - 1$ is irreducible over the field $K = \mathbf{Z}_3$, but has two roots in the extension field $F = \mathbf{Z}_3[x]/\langle x^2 + 1\rangle$.

Solution: Since $f(0) = -1$, $f(1) = 1$, and $f(-1) = -1$, there are no roots of $f(x)$ in K. Since $x^2 + 1$ also has no roots in K, we know that F is an extension field of K.

Letting $[x] = \alpha$, the elements of F have the form $a + b\alpha$, for $a, b \in \mathbf{Z}_3$, and α behaves like i in $\mathbf{C}$. A clue to finding the roots comes from solving $x^2 + x - 1$ in $\mathbf{C}$. The quadratic formula gives the solutions $\frac{1}{2}(-1 \pm \sqrt{5})$ in $\mathbf{C}$. To translate to $\mathbf{Z}_3$, note that the multiplicative inverse of 2 is 2, and $\sqrt{5} \cong \sqrt{-1}$. In F, we have $\alpha^2 = [x]^2 = -1$, so reasoning by analogy, the candidates for roots are $2(-1 \pm \alpha) = 1 \pm 2\alpha = 1 \pm \alpha$. Now we must check the conjecture.

$(1 + \alpha)^2 + (1 + \alpha) - 1 = 1 + 2[x] + [x]^2 + 1 + [x] - 1 = [x]^2 + 1 \equiv 0.$

$(1 - \alpha)^2 + (1 - \alpha) - 1 = 1 - 2[x] + [x]^2 + 1 - [x] - 1 = [x]^2 + 1 \equiv 0.$

18. Let F be an extension field of K. Let G be the set of all automorphisms $\phi : F \to F$ such that $\phi(x) = x$ for all $x \in K$. Show that G is a group (under composition of functions).

Solution: Recall that an automorphism of F is a just an isomorphism from F to F. We know that the composite of two isomorphisms is an isomorphism, and if both isomorphisms leave the elements of K fixed, then so does the composite, so G satisfies the closure property. Composition of functions is always associative, and the identity mapping certainly belongs to G. The last thing to show is that G is closed under formation of inverses. If $\phi \in G$, then ϕ^{-1} is certainly an automorphism of F, and for all $x \in K$ we have $\phi^{-1}(x) = \phi^{-1}(\phi(x)) = x$.

6.2 Finite and Algebraic Extensions

12. Show that $x^3 + 6x^2 - 12x + 2$ is irreducible over $\mathbf{Q}$, and remains irreducible over $\mathbf{Q}(\sqrt[5]{2})$.

Solution: Let $f(x) = x^3 + 6x^2 - 12x + 2$. Then Eisenstein's criterion, with $p = 2$, shows that $f(x)$ is irreducible over $\mathbf{Q}$.

Since $x^5 - 2$ is also irreducible by Eisenstein's criterion, it follows that $[\mathbf{Q}(\sqrt[5]{2}) : \mathbf{Q}] = 5$. If $f(x)$ could be factored over $\mathbf{Q}(\sqrt[5]{2})$, then it would have a linear factor, and so it would have a root $r \in \mathbf{Q}(\sqrt[5]{2})$. Over $\mathbf{Q}$, the root r would have degree 3, since its minimal polynomial over $\mathbf{Q}$ would be $f(x)$. That leads to a contradiction, since 3 is not a divisor of $[\mathbf{Q}(\sqrt[5]{2}) : \mathbf{Q}]$.

13. Find a basis for $\mathbf{Q}(\sqrt{5}, \sqrt[3]{5})$ over $\mathbf{Q}$.

Solution: The set $\{1, \sqrt[3]{5}, \sqrt[3]{25}\}$ is a basis for $\mathbf{Q}(\sqrt[3]{5})$ over $\mathbf{Q}$, and since this extension has degree 3, the minimal polynomial $x^2 - 5$ of $\sqrt{5}$ remains irreducible over the extension $\mathbf{Q}(\sqrt[3]{5})$. Therefore $\{1, \sqrt{5}\}$ is a basis for $\mathbf{Q}(\sqrt{5}, \sqrt[3]{5})$ over $\mathbf{Q}(\sqrt[3]{5})$, and so the

proof of Theorem 6.2.4 shows that the required basis is the set of products of the two bases: $\{1, \sqrt{5}, \sqrt[3]{5}, \sqrt{5}\sqrt[3]{5}, \sqrt[3]{25}, \sqrt{5}\sqrt[3]{25}\}$.

14. Show that $[\mathbf{Q}(\sqrt{2}+\sqrt[3]{5}) : \mathbf{Q}] = 6$.

Solution: The set $\{1, \sqrt[3]{5}, \sqrt[3]{25}\}$ is a basis for $\mathbf{Q}(\sqrt[3]{5})$ over $\mathbf{Q}$, and since this extension has degree 3, the minimal polynomial $x^2 - 2$ of $\sqrt{2}$ remains irreducible over the extension $\mathbf{Q}(\sqrt[3]{5})$. Thus $\{1, \sqrt[3]{5}, \sqrt[3]{25}, \sqrt{2}, \sqrt{2}\sqrt[3]{5}, \sqrt{2}\sqrt[3]{25}\}$ is a basis for $\mathbf{Q}(\sqrt[3]{5}, \sqrt{2})$ over $\mathbf{Q}$, and this extension contains $u = \sqrt{2} + \sqrt[3]{5}$. It follows that u has degree 2, 3, or 6 over $\mathbf{Q}$.

We will show that u cannot have degree ≤ 3. If $\sqrt{2} + \sqrt[3]{5}$ is a root of a polynomial $ax^3 + bx^2 + cx + d$ in $\mathbf{Q}[x]$, then

$0 = a(\sqrt{2} + \sqrt[3]{5})^3 + b(\sqrt{2} + \sqrt[3]{5})^2 + c(\sqrt{2} + \sqrt[3]{5}) + d =$

$a(2\sqrt{2} + 6\sqrt[3]{5} + 3\sqrt{2}\sqrt[3]{25} + 5) + b(2 + 2\sqrt{2}\sqrt[3]{5} + \sqrt[3]{25}) + c(\sqrt{2} + \sqrt[3]{5}) + d =$

$(5a + 2b + d) \cdot 1 + (6a + c)\sqrt[3]{5} + b\sqrt[3]{25} + (2a + c)\sqrt{2} + 2b\sqrt{2}\sqrt[3]{5} + 3a\sqrt{2}\sqrt[3]{25}.$

Since $\{1, \sqrt[3]{5}, \sqrt[3]{25}, \sqrt{2}, \sqrt{2}\sqrt[3]{5}, \sqrt{2}\sqrt[3]{25}\}$ are linearly independent over $\mathbf{Q}$, it follows immediately that $a = b = 0$, and then $c = d = 0$ as well, so $\sqrt{2} + \sqrt[3]{5}$ cannot satisfy a nonzero polynomial of degree 1, 2, or 3 over $\mathbf{Q}$. We conclude that $[\mathbf{Q}(\sqrt{2} + \sqrt[3]{5}) : \mathbf{Q}] = 6$.

15. Find $[\mathbf{Q}(\sqrt[7]{16} + 3\sqrt[7]{8}) : \mathbf{Q}]$.

Solution: Let $u = \sqrt[7]{16} + 3\sqrt[7]{8}$. Since $u = (\sqrt[7]{2} + 3)(\sqrt[7]{2})^3$, it follows that $u \in \mathbf{Q}(\sqrt[7]{2})$. Since $x^7 - 2$ is irreducible over $\mathbf{Q}$ by Eisenstein's criterion, we have $[\mathbf{Q}(\sqrt[7]{2}) : \mathbf{Q}] = 7$, and then u must have degree 7 over $\mathbf{Q}$ since $[\mathbf{Q}(u) : \mathbf{Q}]$ is a divisor of $[\mathbf{Q}(\sqrt[7]{2}) : \mathbf{Q}]$.

16. Find the degree of $\sqrt[3]{2} + i$ over $\mathbf{Q}$. Does $\sqrt[4]{2}$ belong to $\mathbf{Q}(\sqrt[3]{2} + i)$?

Solution: Let $u = \sqrt[3]{2} + i$, so that $u - i = \sqrt[3]{2}$. Then $(u - i)^3 = 2$, so we have $u^3 - 3iu^2 + 3i^2u - i^3 = 2$, or $u^3 - 3iu^2 - 3u + i = 2$. Solving for i we get $i = (u^3 - 3u - 2)/(3u^2 - 1)$, and this shows that $i \in \mathbf{Q}(\sqrt[3]{2} + i)$. It follows immediately that $\sqrt[3]{2} \in \mathbf{Q}(\sqrt[3]{2} + i)$, and so $\mathbf{Q}(\sqrt[3]{2} + i) = \mathbf{Q}(\sqrt[3]{2}, i)$.

Since $x^3 - 2$ is irreducible over $\mathbf{Q}$, the number $\sqrt[3]{2}$ has degree 3 over $\mathbf{Q}$. Since $x^2 + 1$ is irreducible over $\mathbf{Q}$, we see that i has degree 2 over $\mathbf{Q}$. Therefore $[\mathbf{Q}(\sqrt[3]{2} + i) : \mathbf{Q}] \leq 6$. On the other hand, $[\mathbf{Q}(\sqrt[3]{2} + i) : \mathbf{Q}] = [\mathbf{Q}(\sqrt[3]{2} + i) : \mathbf{Q}(\sqrt[3]{2})][\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}]$ and $[\mathbf{Q}(\sqrt[3]{2} + i) : \mathbf{Q}] = [\mathbf{Q}(\sqrt[3]{2} + i) : \mathbf{Q}(i)][\mathbf{Q}(i) : \mathbf{Q}]$ so $[\mathbf{Q}(\sqrt[3]{2} + i) : \mathbf{Q}]$ must be divisible by 2 and 3. Therefore $[\mathbf{Q}(\sqrt[3]{2} + i) : \mathbf{Q}] = 6$.

Finally, $\sqrt[4]{2}$ has degree 4 over $\mathbf{Q}$ since $x^4 - 2$ is irreducible over $\mathbf{Q}$, so it cannot belong to an extension of degree 6 since 4 is not a divisor of 6.

17. Let F be a field whose multiplicative group $F^\times$ is cyclic. Prove that F must be a finite field.

Comment: This is the converse of an important result which states that the multiplicative group of a finite field is cyclic. (The general result is given in in Theorem 6.5.10 of **Abstract Algebra**.) See Problem 4.1.30 for the special case $\mathbf{Z}_p^\times$.

Solution: Suppose that the group $F^\times$ is infinite cyclic, with generator u. Since u does not have finite order, it is different from 1 and -1, and the only solution of the equation $x^2 = 1$ is $x = 1$. Thus $-1 = 1$, and $\text{char}(F) = 2$. It follows that 1 generates a base field K isomorphic to $\mathbf{Z}_2$.

Since $1 + u \neq 0$, we have $1 + u \in F^\times$. Then because $F^\times$ is cyclic we must have $1 + u = u^n$ or $1 + u = u^{-n}$ for some $n \in \mathbf{Z}^+$. In the first case, u is a root of $x^n - x - 1 \in K[x]$, and in the second case u is a root of $x^n + x^{n-1} - 1 \in K[x]$. It follows that $F = K(u)$ is a finite extension of K, and therefore F itself is finite, a contradiction.

18. Let F be a finite field of characteristic p. Show that F has p^n elements, for some positive integer n.

Solution: Since $\text{char}(F) = p$, the subfield $K = \{n \cdot 1 \mid n \in \mathbf{Z}\}$ is isomorphic to $\mathbf{Z}_p$. Since F is finite, it must certainly have finite dimension as a vector space over K, say $[F : K] = n$. If $v_1, \ldots, v_n$ is a basis for F over K, then each element of F has the form $a_1v_1 + \cdots + a_nv_n$, for $a_1, \ldots, a_n \in K$. Thus to define an element of F there are n coefficients a_i, and for each coefficient there are p choices, since $|K| = p$. Thus the total number of elements in F is p^n.

ANSWERS AND HINTS

19. Over $\mathbf{Z}_2$, factor $x^4 - x$, $x^8 - x$, and $x^{16} - x$.
In the text **Abstract Algebra**, the answer to Exercise 4.2.12 gives the following list of irreducible polynomials over $\mathbf{Z}_2$:
degree 2: $p_2(x) = x^2 + x + 1$
degree 3: $p_{31}(x) = x^3 + x^2 + 1$ and $p_{32}(x) = x^3 + x + 1$
degree 4: $p_{41}(x) = x^4+x^3+x^2+x+1$, $p_{42}(x) = x^4+x^3+1$, and $p_{43}(x) = x^4+x+1$.
Answer: Check the following factorizations; see Theorem 6.6.1 for an explanation.
$x^4 - x = x(x - 1)(x^2 + x + 1) = x(x - 1)(p_2(x))$
$x^8 - x = x(x - 1)(x^3 + x^2 + 1)(x^3 + x + 1) = x(x - 1)(p_{31}(x))(p_{32}(x))$
$x^{16} - x = x(x - 1)(p_2(x))(p_{41}(x))(p_{42}(x))(p_{43}(x))$

21. In the finite field $F = \mathbf{Z}_2[x]/\langle x^4 + x + 1\rangle$, find a subfield K with 4 elements.
Hint: Let $\alpha = [x^2 + x + 1]$. Then $\alpha^2 = [x^4 + x^2 + 1] = [x^2 + x]$, and $\alpha^3 = [x^2 + x + 1][x^2 + x] = [x^4 + x] = [1]$, so $\{1, \alpha, \alpha^2\}$ is closed under multiplication.
Answer: $K = \{0, 1, \alpha, \alpha^2\}$

22. Suppose that E and F are extension fields of $\mathbf{Z}_2$, with $\mathbf{Z}_2 \subset E \subset F$. Given that $[E : \mathbf{Z}_2] = 2$ and $[F : E] = 3$, find $|E|$ and $|F|$.
Answer: $|E| = 4$ and $|F| = 64$

BIBLIOGRAPHY

Allenby, R. B. J. T., *Rings, Fields, and Groups: An Introduction to Abstract Algebra* (4^{th} ed.). Elsevier, 1991.

Artin, M., *Algebra*, Englewood Cliffs, N. J.: Prentice-Hall, Inc., 1991

Birkhoff, G., and S. Mac Lane, *A Survey of Modern Algebra* (4^{th} ed.). New York: Macmillan Publishing Co., Inc., 1977.

Fraleigh, J., *A First Course in Abstract Algebra* (7^{th} ed.). Reading, Mass.: Addison-Wesley Publishing Co., 2003.

Gallian, J., *Contemporary Abstract Algebra* (5^{th} ed.). Boston: Houghton Mifflin Co., 2002

Herstein, I. N., *Abstract Algebra.* (3^{rd} ed.). New York: John Wiley & Sons, Inc., 1996.

———, *Topics in Algebra* (2^{nd} ed.). New York: John Wiley & Sons, Inc., 1975.

Hillman, A. P., and G. L. Alexanderson, *Abstract Algebra: A First Undergraduate Course.* Prospect Heights: Waveland Press, 1999.

Maxfield, J. E., and M. W. Maxfield, *Abstract Algebra and Solution by Radicals.* New York: Dover Publications, Inc., 1992.

Saracino, D., *Abstract Algebra: A First Course.* Prospect Heights: Waveland Press, 1992.

Van der Waerden, B. L., *A History of Algebra: from al-Khwarizmi to Emmy Noether.* New York: Springer-Verlag, 1985.