

ABSTRACT ALGEBRA:

**A STUDY GUIDE
FOR BEGINNERS**

John A. Beachy

Northern Illinois University

2000

This is a supplement to

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

ISBN 0-88133-866-4, Copyright 1996

Waveland Press, Inc.
P.O. Box 400
Prospect Heights, Illinois 60070
847 / 634-0081
www.waveland.com

©John A. Beachy 2000

Permission is granted to copy this document in electronic form, or to print it for personal use, under these conditions:

- it must be reproduced in whole;
- it must not be modified in any way;
- it must not be used as part of another publication.

Formatted February 8, 2002, at which time the original was available at:

http://www.math.niu.edu/~beachy/abstract_algebra/

Contents

| | |
|---|-----------|
| PREFACE | v |
| 1 INTEGERS | 1 |
| 1.1 Divisors | 1 |
| 1.2 Primes | 2 |
| 1.3 Congruences | 3 |
| 1.4 Integers Modulo n | 5 |
| Review problems | 6 |
| 2 FUNCTIONS | 7 |
| 2.1 Functions | 7 |
| 2.2 Equivalence Relations | 8 |
| 2.3 Permutations | 10 |
| Review problems | 12 |
| 3 GROUPS | 13 |
| 3.1 Definition of a Group | 13 |
| 3.2 Subgroups | 15 |
| 3.3 Constructing Examples | 17 |
| 3.4 Isomorphisms | 18 |
| 3.5 Cyclic Groups | 20 |
| 3.6 Permutation Groups | 21 |
| 3.7 Homomorphisms | 22 |
| 3.8 Cosets, Normal Subgroups, and Factor Groups | 24 |
| Review problems | 26 |
| 4 POLYNOMIALS | 27 |
| Review problems | 27 |
| 5 COMMUTATIVE RINGS | 29 |
| Review problems | 29 |

| | |
|----------------------------|------------|
| 6 FIELDS | 33 |
| Review problems | 33 |
| SOLUTIONS | 33 |
| 1 Integers | 35 |
| 2 Functions | 49 |
| 3 Groups | 57 |
| 4 Polynomials | 87 |
| 5 Commutative Rings | 93 |
| 6 Fields | 101 |
| BIBLIOGRAPHY | 104 |
| INDEX | 105 |

PREFACE

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
October 2000

John A. Beachy

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 into the realm 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 be able 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.

—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 .

—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 $r = 0$.

—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.

SOLVED PROBLEMS: §1.1

22. Find $\gcd(435, 377)$, and express it as a linear combination of 435 and 377.
23. Find $\gcd(3553, 527)$, and express it as a linear combination of 3553 and 527.
24. Which of the integers $0, 1, \dots, 10$ can be expressed in the form $12m + 20n$, where m, n are integers?
25. If n is a positive integer, find the possible values of $\gcd(n, n + 10)$.
26. Prove that if a and b are nonzero integers for which $a|b$ and $b|a$, then $b = \pm a$.
27. Prove that if m and n are odd integers, then $m^2 - n^2$ is divisible by 8.
28. Prove that if n is an integer with $n > 1$, then $\gcd(n - 1, n^2 + n + 1) = 1$ or $\gcd(n - 1, n^2 + n + 1) = 3$.
29. 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 $4|n$.
30. Give a proof by induction to show that each number in the sequence 12, 102, 1002, 10002, \dots , is divisible by 6.

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

23. (a) Use the Euclidean algorithm to find $\gcd(1776, 1492)$.
(b) Use the prime factorizations of 1492 and 1776 to find $\gcd(1776, 1492)$.
24. (a) Use the Euclidean algorithm to find $\gcd(1274, 1089)$.
(b) Use the prime factorizations of 1274 and 1089 to find $\gcd(1274, 1089)$.
25. Give the lattice diagram of all divisors of 250. Do the same for 484.
26. Find all integer solutions of the equation $xy + 2y - 3x = 25$.
27. For positive integers a, b , prove that $\gcd(a, b) = 1$ if and only if $\gcd(a^2, b^2) = 1$.
28. Prove that $n - 1$ and $2n - 1$ are relatively prime, for all integers $n > 1$. Is the same true for $2n - 1$ and $3n - 1$?
29. Let m and n be positive integers. Prove that $\gcd(2^m - 1, 2^n - 1) = 1$ if and only if $\gcd(m, n) = 1$.
30. Prove that $\gcd(2n^2 + 4n - 3, 2n^2 + 6n - 4) = 1$, for all integers $n > 1$.

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!

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 .

The 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

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

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

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

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

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

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”, and you can’t afford to skip over their proofs, because you might miss important algorithms or computational techniques.

SOLVED PROBLEMS: §1.3

26. Solve the congruence $42x \equiv 12 \pmod{90}$.
27. (a) Find all solutions to the congruence $55x \equiv 35 \pmod{75}$.
(b) Find all solutions to the congruence $55x \equiv 36 \pmod{75}$.
28. (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 .
29. Solve the system of congruences $x \equiv 2 \pmod{9}$ $x \equiv 4 \pmod{10}$.
30. Solve the system of congruences $5x \equiv 14 \pmod{17}$ $3x \equiv 2 \pmod{13}$.
31. Solve the system of congruences $x \equiv 5 \pmod{25}$ $x \equiv 23 \pmod{32}$.
32. Give integers a, b, m, n to provide an example of a system

$$x \equiv a \pmod{m} \quad x \equiv b \pmod{n}$$

that has no solution.

33. (a) Compute the last digit in the decimal expansion of 4^{100} .
 (b) Is 4^{100} divisible by 3?
34. Find all integers n for which $13 \mid 4(n^2 + 1)$.
35. Prove that $10^{n+1} + 4 \cdot 10^n + 4$ is divisible by 9, for all positive integers n .
36. Prove that the fourth power of an integer can only have 0, 1, 5, or 6 as its units digit.

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.

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

30. Find the multiplicative inverse of each nonzero element of \mathbf{Z}_7 .
31. Find the multiplicative inverse of each nonzero element of \mathbf{Z}_{13} .

32. Find $[91]_{501}^{-1}$, if possible (in \mathbf{Z}_{501}^\times).
33. Find $[3379]_{4061}^{-1}$, if possible (in \mathbf{Z}_{4061}^\times).
34. In \mathbf{Z}_{20} : find all units (list the multiplicative inverse of each); find all idempotent elements; find all nilpotent elements.
35. In \mathbf{Z}_{24} : find all units (list the multiplicative inverse of each); find all idempotent elements; find all nilpotent elements.
36. Show that \mathbf{Z}_{17}^\times is cyclic.
37. 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 .
38. Solve the equation $[x]_{11}^2 + [x]_{11} - [6]_{11} = [0]_{11}$.
39. Let n be a positive integer, and let $a \in \mathbf{Z}$ with $\gcd(a, n) = 1$. Prove that if k is the smallest positive integer for which $a^k \equiv 1 \pmod{n}$, then $k \mid \varphi(n)$.
40. 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 .

Review Problems

1. Find $\gcd(7605, 5733)$, and express it as a linear combination of 7605 and 5733.
2. For $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, prove that $\omega^n = 1$ if and only if $3 \mid n$, for any integer n .
3. Solve the congruence $24x \equiv 168 \pmod{200}$.
4. Solve the system of congruences $2x \equiv 9 \pmod{15}$ $x \equiv 8 \pmod{11}$.
5. List the elements of \mathbf{Z}_{15}^\times . For each element, find its multiplicative inverse, and find its multiplicative order.
6. Show that if $n > 1$ is an odd integer, then $\varphi(2n) = \varphi(n)$.

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.

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 .

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 $f : \mathbf{R} \rightarrow \mathbf{R}^+$ and $g : \mathbf{R}^+ \rightarrow \mathbf{R}$ 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.) In terms of actually using this definition, the text almost immediately goes back to what might be a more familiar definition: a function $f : S \rightarrow T$ 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

20. 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.
21. 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.
more than one
22. 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 2.1.7.
23. Let A be an $n \times n$ matrix with entries in \mathbf{R} . Define a linear transformation $L : \mathbf{R}^n \rightarrow \mathbf{R}^n$ 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.
24. Let A be an $m \times n$ matrix with entries in \mathbf{R} , and assume that $m > n$. Define a linear transformation $L : \mathbf{R}^n \rightarrow \mathbf{R}^m$ 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 .
25. Let A be an $n \times n$ matrix with entries in \mathbf{R} . Define a linear transformation $L : \mathbf{R}^n \rightarrow \mathbf{R}^n$ 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 zero.
Note: A vector \mathbf{x} is called an eigenvector of A if it is nonzero and there exists a scalar λ such that $A\mathbf{x} = \lambda\mathbf{x}$.
26. Let a be a fixed element of \mathbf{Z}_{17}^\times . Define the function $\theta : \mathbf{Z}_{17}^\times \rightarrow \mathbf{Z}_{17}^\times$ 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} .

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 $f : S \rightarrow T$, 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

14. 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.
15. On the set \mathbf{C} of complex numbers, define $z_1 \sim z_2$ if $\|z_1\| = \|z_2\|$. Show that \sim is an equivalence relation.
16. 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 .
17. For the function $f : \mathbf{R} \rightarrow \mathbf{R}$ defined by $f(x) = x^2$, for all $x \in \mathbf{R}$, describe the equivalence relation on \mathbf{R} that is determined by f .
18. For the linear transformation $L : \mathbf{R}^3 \rightarrow \mathbf{R}^3$ 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 .

19. Define the formula $f : \mathbf{Z}_{12} \rightarrow \mathbf{Z}_{12}$ 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 of f and the set \mathbf{Z}_{12}/f of equivalence classes determined by f .
20. On the set of all $n \times n$ matrices over \mathbf{R} , define $A \sim B$ if there exists an invertible matrix P such that $PAP^{-1} = B$. Check that \sim defines an equivalence relation.

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

If G is a nonempty subset of $\text{Sym}(S)$, 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

13. 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 ? Is σ an even permutation? Compute σ^{-1} .
14. 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: $\sigma, \tau, \sigma\tau, \sigma\tau\sigma^{-1}, \sigma^{-1}, \tau^{-1}, \tau\sigma, \tau\sigma\tau^{-1}$.
15. 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} .
16. 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 $\sigma\tau\sigma^{-1}$.
17. Prove that if $\tau \in S_n$ is a permutation with order m , then $\sigma\tau\sigma^{-1}$ has order m , for any permutation $\sigma \in S_n$.

18. Show that S_{10} has elements of order 10, 12, and 14, but not 11 or 13.
19. Let S be a set, and let X be a subset of S . Let $G = \{\sigma \in \text{Sym}(S) \mid \sigma(X) \subset X\}$. Prove that G is a group of permutations.
20. Let G be a group of permutations, with $G \subseteq \text{Sym}(S)$, for the set S . Let τ be a fixed permutation in $\text{Sym}(S)$. Prove that

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

is a group of permutations.

Review Problems

1. For the function $f : \mathbf{R} \rightarrow \mathbf{R}$ defined by $f(x) = x^2$, for all $x \in \mathbf{R}$, describe the equivalence relation on \mathbf{R} that is determined by f .
2. Define $f : \mathbf{R} \rightarrow \mathbf{R}$ by $f(x) = x^3 + 3xz - 5$, for all $x \in \mathbf{R}$. Show that f is a one-to-one function.
Hint: Use the derivative of f to show that f is a strictly increasing function.
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 $\phi : \mathbf{Z}_{17}^{\times} \rightarrow \mathbf{Z}_{17}^{\times}$ 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 $\phi_{\alpha} : S_n \rightarrow S_n$ 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} .

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 $a * b$, so long as everyone knows the convention that we are using.

3.1 Definition of a Group

This section contains these definitions: *binary operation*, *group*, *abelian group*, and *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 a binary operation that is associative, has an identity element, and has inverses for each of its elements. The precise statement is given in Definition 3.1.3; 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 says that you can multiply both sides of an equation by the same value, 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 3.1.6 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 to 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 $GL_n(\mathbf{R})$ 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 \mathcal{S}_n still has an important role to play.

SOLVED PROBLEMS: §3.1

22. Use the dot product to define a multiplication on \mathbf{R}^3 . Does this make \mathbf{R}^3 into a group?
23. 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?
24. On the set $G = \mathbf{Q}^\times$ of nonzero rational numbers, define a new multiplication by $a * b = \frac{ab}{2}$, for all $a, b \in G$. Show that G is a group under this multiplication.
25. Write out the multiplication table for \mathbf{Z}_9^\times .

26. Write out the multiplication table for \mathbf{Z}_{15}^\times .
27. 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 $ba = ab$.
28. 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 .
29. In Definition 3.1.3 of the text, 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.
30. The previous exercise 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.
31. Let F be the set of all *fractional linear transformations* of the complex plane. That is, F is the set of all functions $f(z) : \mathbf{C} \rightarrow \mathbf{C}$ of the form $f(z) = \frac{az + b}{cz + d}$, where the coefficients a, b, c, d are integers with $ad - bc = 1$. Show that F forms a group under composition of functions.
32. 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 $x * y = xy - x - y + 2$.
- Show that the operation $*$ is closed on G .
 - Show that the associative law holds for $*$.
 - Show that 2 is the identity element for the operation $*$.
 - Show that for element $a \in G$ there exists an inverse $a^{-1} \in G$.

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 $\text{Sym}(S)$, for some set S . Any group of $n \times n$ matrices (with entries in \mathbf{R}) is a subgroup of $\text{GL}_n(\mathbf{R})$.

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 is very important. 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.

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 you only need to look at positive powers, since in that case the inverse a^{-1} of any element can be expressed in the form a^n , for some $n > 0$.

SOLVED PROBLEMS: §3.2

23. Find all cyclic subgroups of \mathbf{Z}_{24}^\times .
24. In \mathbf{Z}_{20}^\times , find two subgroups of order 4, one that is cyclic and one that is not cyclic.
25. (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.
26. In $G = \mathbf{Z}_{21}^\times$, show that

$$H = \{[x]_{21} \mid x \equiv 1 \pmod{3}\} \quad \text{and} \quad K = \{[x]_{21} \mid x \equiv 1 \pmod{7}\}$$

are subgroups of G .

27. 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 .
28. 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.
29. In the multiplicative group \mathbf{C}^\times of complex numbers, find the order of the elements $-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ and $-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$.
30. In the group $G = GL_2(\mathbf{R})$ of invertible 2×2 matrices with real entries, show that

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

is a subgroup of G .

31. Let K be the following subset of $GL_2(\mathbf{R})$.

$$K = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid d = a, \quad c = -2b, \quad ad - bc \neq 0 \right\}$$

Show that K is a subgroup of $GL_2(\mathbf{R})$.

32. Compute the centralizer in $GL_2(\mathbf{R})$ of the matrix $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$.

Note: Exercise 3.2.14 in the text defines the centralizer of an element a of the group G to be $C(a) = \{x \in G \mid xa = ax\}$.

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 $GL_n(\mathbf{Z}_p)$.

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 i th 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).

SOLVED PROBLEMS: §3.3

16. Show that $\mathbf{Z}_5 \times \mathbf{Z}_3$ is a cyclic group, and list all of the generators for the group.
17. Find the order of the element $([9]_{12}, [15]_{18})$ in the group $\mathbf{Z}_{12} \times \mathbf{Z}_{18}$.
18. 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 $H_2 \subseteq G_2$.
19. 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 .
20. Show that if p is a prime number, then the order of the general linear group $GL_n(\mathbf{Z}_p)$ is $(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.

21. Find the order of the element $A = \begin{bmatrix} i & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -i \end{bmatrix}$ in the group $GL_3(\mathbf{C})$.

22. Let G be the subgroup of $GL_2(\mathbf{R})$ defined by

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

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 .

23. Compute the centralizer in $GL_2(\mathbf{Z}_3)$ of the matrix $\begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$.

24. Compute the centralizer in $GL_2(\mathbf{Z}_3)$ of the matrix $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$.

25. Let H be the following subset of the group $G = GL_2(\mathbf{Z}_5)$.

$$H = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbf{Z}_5) \mid m, b \in \mathbf{Z}_5, m = \pm 1 \right\}$$

(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 $0 \leq j < 2$.

3.4 Isomorphisms

A one-to-one correspondence $\phi : G_1 \rightarrow G_2$ 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 multiplication of 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 $\phi : G_1 \rightarrow G_2$. 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

21. Show that \mathbf{Z}_{17}^\times is isomorphic to \mathbf{Z}_{16} .
22. Let $\phi : \mathbf{R}^\times \rightarrow \mathbf{R}^\times$ be defined by $\phi(x) = x^3$, for all $x \in \mathbf{R}$. Show that ϕ is a group isomorphism.
23. Let G_1, G_2, H_1, H_2 be groups, and suppose that $\theta_1 : G_1 \rightarrow H_1$ and $\theta_2 : G_2 \rightarrow H_2$ are group isomorphisms. Define $\phi : G_1 \times G_2 \rightarrow H_1 \times H_2$ 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.
24. Prove that the group $\mathbf{Z}_7^\times \times \mathbf{Z}_{11}^\times$ is isomorphic to the group $\mathbf{Z}_6 \times \mathbf{Z}_{10}$.
25. Define $\phi : \mathbf{Z}_{30} \times \mathbf{Z}_2 \rightarrow \mathbf{Z}_{10} \times \mathbf{Z}_6$ by $\phi([n]_{30}, [m]_2) = ([n]_{10}, [4n + 3m]_6)$, for all $([n]_{30}, [m]_2) \in \mathbf{Z}_{30} \times \mathbf{Z}_2$. First prove that ϕ is a well-defined function, and then prove that ϕ is a group isomorphism.
26. 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 .

27. Let G, G_1, G_2 be groups. Prove that if G is isomorphic to $G_1 \times G_2$, 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 $k \in K$.
28. Show that for any prime number p , the subgroup of diagonal matrices in $GL_2(\mathbf{Z}_p)$ is isomorphic to $\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$.
29. (a) In the group $G = GL_2(\mathbf{R})$ of invertible 2×2 matrices with real entries, show that

$$H = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in GL_2(\mathbf{R}) \mid a_{11} = 1, a_{21} = 0, a_{22} = 1 \right\}$$

is a subgroup of G .

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

30. Let G be the subgroup of $GL_2(\mathbf{R})$ defined by

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

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

31. Let H be the following subgroup of group $G = GL_2(\mathbf{Z}_3)$.

$$H = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbf{Z}_3) \mid m, b \in \mathbf{Z}_3, m \neq 0 \right\}$$

Show that H is isomorphic to the symmetric group S_3 .

32. Let G be a group, and let S be any set for which there exists a one-to-one and onto function $\phi : G \rightarrow S$. Define an operation on S by setting $x_1 \cdot x_2 = \phi(\phi^{-1}(x_1)\phi^{-1}(x_2))$, for all $x_1, x_2 \in S$. Prove that S is a group under this operation, and that ϕ is actually a group isomorphism.

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

20. Show that the three groups \mathbf{Z}_6 , \mathbf{Z}_9^\times , and \mathbf{Z}_{18}^\times are isomorphic to each other.
21. Is $\mathbf{Z}_4 \times \mathbf{Z}_{10}$ isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_{20}$?
22. Is $\mathbf{Z}_4 \times \mathbf{Z}_{15}$ isomorphic to $\mathbf{Z}_6 \times \mathbf{Z}_{10}$?
23. Give the lattice diagram of subgroups of \mathbf{Z}_{100} .
24. Find all generators of the cyclic group \mathbf{Z}_{28} .
25. In \mathbf{Z}_{30} , find the order of the subgroup $\langle [18]_{30} \rangle$; find the order of $\langle [24]_{30} \rangle$.
26. 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.
27. Show that any cyclic group of even order has exactly one element of order 2.
28. Use the the result in Problem 27 to show that the multiplicative groups \mathbf{Z}_{15}^\times and \mathbf{Z}_{21}^\times are not cyclic groups.
29. Find all cyclic subgroups of the quaternion group. Use this information to show that the quaternion group cannot be isomorphic to the subgroup of \mathcal{S}_4 generated by $(1, 2, 3, 4)$ and $(1, 3)$.
30. Prove that if p and q are different odd primes, then \mathbf{Z}_{pq}^\times is not a cyclic group.

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 \mathcal{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 algebraists 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 \mathcal{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

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

In doing computations in \mathcal{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

22. In the dihedral group $\mathcal{D}_n = \{a^i b^j \mid 0 \leq i < n, 0 \leq j < 2\}$ with $o(a) = n$, $o(b) = 2$, and $ba = a^{-1}b$, show that $ba^i = a^{n-i}b$, for all $0 \leq i < n$.
23. In the dihedral group $\mathcal{D}_n = \{a^i b^j \mid 0 \leq i < n, 0 \leq j < 2\}$ 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.
24. In \mathcal{S}_4 , find the subgroup H generated by $(1, 2, 3)$ and $(1, 2)$.
25. For the subgroup H of \mathcal{S}_4 defined in the previous problem, find the corresponding subgroup $\sigma H \sigma^{-1}$, for $\sigma = (1, 4)$.
26. Show that each element in \mathcal{A}_4 can be written as a product of 3-cycles.
27. In the dihedral group $\mathcal{D}_n = \{a^i b^j \mid 0 \leq i < n, 0 \leq j < 2\}$ with $o(a) = n$, $o(b) = 2$, and $ba = a^{-1}b$, find the centralizer of a .
28. Find the centralizer of $(1, 2, 3)$ in \mathcal{S}_3 , in \mathcal{S}_4 , and in \mathcal{A}_4 .

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 3.8.8, after we develop the concepts of cosets and factor groups.) In this formulation of the Fundamental Homomorphism Theorem, we start with a group homomorphism $\phi : G_1 \rightarrow G_2$. 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 $\phi : G_1 \rightarrow G_2$ it describes the connections between subgroups of G_1 and subgroups of G_2 . Examples 3.7.4 and 3.7.5 are important, because they give a complete description of all group homomorphisms between two cyclic groups.

SOLVED PROBLEMS: §3.7

17. Find all group homomorphisms from \mathbf{Z}_4 into \mathbf{Z}_{10} .
18. (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 for this formula find the kernel and image, and show how elements of the image correspond to cosets of the kernel.
19. (a) Show that \mathbf{Z}_7^\times is cyclic, with generator $[3]_7$.
(b) Show that \mathbf{Z}_{17}^\times is cyclic, with generator $[3]_{17}$.
(c) Completely determine all group homomorphisms from \mathbf{Z}_{17}^\times into \mathbf{Z}_7^\times .
20. Define $\phi : \mathbf{Z}_4 \times \mathbf{Z}_6 \rightarrow \mathbf{Z}_4 \times \mathbf{Z}_3$ by $\phi(x, y) = (x + 2y, y)$.
(a) Show that ϕ is a well-defined group homomorphism.
(b) Find the kernel and image of ϕ , and apply the fundamental homomorphism theorem.
21. Let n and m be positive integers, such that m is a divisor of n . Show that $\phi : \mathbf{Z}_n^\times \rightarrow \mathbf{Z}_m^\times$ defined by $\phi([x]_n) = [x]_m$, for all $[x]_n \in \mathbf{Z}_n^\times$, is a well-defined group homomorphism.
22. For the group homomorphism $\phi : \mathbf{Z}_{36}^\times \rightarrow \mathbf{Z}_{12}^\times$ 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 the fundamental homomorphism theorem.
23. Let G , G_1 , and G_2 be groups. Let $\phi_1 : G \rightarrow G_1$ and $\phi_2 : G \rightarrow G_2$ be group homomorphisms. Prove that $\phi : G \rightarrow G_1 \times G_2$ defined by $\phi(x) = (\phi_1(x), \phi_2(x))$, for all $x \in G$, is a well-defined group homomorphism.
24. Let p and q be different odd primes. Prove that \mathbf{Z}_{pq}^\times is isomorphic to the direct product $\mathbf{Z}_p^\times \times \mathbf{Z}_q^\times$.

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 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

27. List the cosets of $\langle 7 \rangle$ in \mathbf{Z}_{16}^\times . Is the factor group $\mathbf{Z}_{16}^\times / \langle 7 \rangle$ cyclic?
28. Let $G = \mathbf{Z}_6 \times \mathbf{Z}_4$, let $H = \{(0, 0), (0, 2)\}$, and let $K = \{(0, 0), (3, 0)\}$.
 - (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 ?
29. 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 $1 \leq i < n$.
 - (b) Show that any element of the form $a^i b$ has order 2.
 - (c) List all left cosets and all right cosets of $\langle b \rangle$
30. Let $G = D_6$ 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) Is G/N abelian?
31. Let G be the dihedral group D_{12} , and let $N = \{e, a^3, a^6, a^9\}$.
- (a) Prove that N is a normal subgroup of G , and list all cosets of N .
 - (b) You may assume that G/N is isomorphic to either \mathbf{Z}_6 or S_3 . Which is correct?
32. (a) 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 $b = gag^{-1}$. Show that \sim is an equivalence relation on G . The equivalence classes of \sim are called the *conjugacy classes* of G .
- (b) Show that a subgroup N of G is normal in G if and only if N is a union of conjugacy classes.
33. Find the conjugacy classes of D_4 .
34. Let G be a group, and let N and H be subgroups of G such that N is normal in G .
- (a) Prove that HN is a subgroup of G .
 - (b) Prove that N is a normal subgroup of HN .
 - (c) Prove that if $H \cap N = \{e\}$, then HN/N is isomorphic to H .

Review Problems

- (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.
- Find all subgroups of \mathbf{Z}_{11}^\times , and give the lattice diagram which shows the inclusions between them.
- Let G be the subgroup of $GL_3(\mathbf{R})$ consisting of all matrices of the form

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ such that } a, b \in \mathbf{R}.$$

Show that G is a subgroup of $GL_3(\mathbf{R})$.

- Show that the group G in the previous problem is isomorphic to the direct product $\mathbf{R} \times \mathbf{R}$.
- List the cosets of the cyclic subgroup $\langle 9 \rangle$ in \mathbf{Z}_{20}^\times . Is $\mathbf{Z}_{20}^\times / \langle 9 \rangle$ cyclic?
- Let G be the subgroup of $GL_2(\mathbf{R})$ consisting of all matrices of the form $\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$, and let N be the subset of all matrices of the form $\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$.
 (a) Show that N is a subgroup of G , and that N is normal in G .
 (b) Show that G/N is isomorphic to the multiplicative group \mathbf{R}^\times .
- 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 of D_4 .
 (b) Is the factor group D_4/N a cyclic group?
- 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.

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.

Because you have a lot more experience now than when you started Chapter 1, I didn't break the problems up by section. Of course, you don't have to wait until you have finished the chapter to practice solving some of these problems.

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, use the Euclidean algorithm to show that $2x^3 - 2x^2 - 3x + 1$ and $2x^2 - x - 2$ are relatively prime.
3. Over the field of rational numbers, find the greatest common divisor of $x^4 + x^3 + 2x^2 + x + 1$ and $x^3 - 1$, and express it as a linear combination of the given polynomials.
4. 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.

5. Are the following polynomials irreducible over \mathbf{Q} ?
 - (a) $3x^5 + 18x^2 + 24x + 6$
 - (b) $7x^3 + 12x^2 + 3x + 45$
 - (c) $2x^{10} + 25x^3 + 10x^2 - 30$
6. Factor $x^5 - 10x^4 + 24x^3 + 9x^2 - 33x - 12$ over \mathbf{Q} .
7. Factor $x^5 - 2x^4 - 2x^3 + 12x^2 - 15x - 2$ over \mathbf{Q} .
8. (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.
9. (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 .
10. Express $2x^3 + x^2 + 2x + 2$ as a product of polynomials irreducible over \mathbf{Z}_5 .
11. Construct an example of a field with $343 = 7^3$ elements.
12. In $\mathbf{Z}_2[x]/\langle x^3 + x + 1 \rangle$, find the multiplicative inverse of $[x + 1]$.
13. Find the multiplicative inverse of $[x^2 + x + 1]$
 - (a) in $\mathbf{Q}[x]/\langle x^3 - 2 \rangle$;
 - (b) in $\mathbf{Z}_3[x]/\langle x^3 + 2x^2 + x + 1 \rangle$.
14. In $\mathbf{Z}_5[x]/\langle x^3 + x + 1 \rangle$, find $[x]^{-1}$ and $[x + 1]^{-1}$, and use your answers to find $[x^2 + x]^{-1}$.
15. Factor $x^4 + x + 1$ over $\mathbf{Z}_2[x]/\langle x^4 + x + 1 \rangle$.

Chapter 5

COMMUTATIVE RINGS

This chapter takes its motivation from Chapter 1 and Chapter 4, extending results on factorization to more general settings than just the integers or polynomials over a field. 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. 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.

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 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 isomorphic to either of the rings \mathbf{Z}_4 or $\mathbf{Z}_2 \oplus \mathbf{Z}_2$.
 3. Find all ring homomorphisms from \mathbf{Z}_{120} into \mathbf{Z}_{42} .
 4. Are \mathbf{Z}_9 and $\mathbf{Z}_3 \oplus \mathbf{Z}_3$ isomorphic as rings?

5. In the group \mathbf{Z}_{180}^\times of units of the ring \mathbf{Z}_{180} , what is the largest possible order of an element?
6. For the element $a = (0, 2)$ of the ring $R = \mathbf{Z}_{12} \oplus \mathbf{Z}_8$, find $\text{Ann}(a) = \{r \in R \mid ra = 0\}$. Show that $\text{Ann}(a)$ is an ideal of R .
7. 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.
8. Find all maximal ideals, and all prime ideals, of $\mathbf{Z}_{36} = \mathbf{Z}/36\mathbf{Z}$.
9. Give an example to show that the set of all zero divisors of a ring need not be an ideal of the ring.
10. 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.
11. Let R be any 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 $R \cong Re \oplus R(1 - e)$.
12. 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 .
13. 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 R .
 - (c) Find the idempotent elements of R .
14. Show that the rings R and S in the two previous problems are isomorphic as abelian groups, but not as rings.
15. Let $\mathbf{Z}[i]$ be the subring of the field of complex numbers given by

$$\mathbf{Z}[i] = \{m + ni \in \mathbf{C} \mid m, n \in \mathbf{Z}\} .$$

- (a) Define $\phi : \mathbf{Z}[i] \rightarrow \mathbf{Z}_2$ 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 $\theta : \mathbf{Z}[i] \rightarrow \mathbf{Z}_p[x]/\langle x^2 + 1 \rangle$ by $\theta(m + ni) = [m + nx]$. Prove that θ is an onto ring homomorphism.
16. Let I and J be ideals in the commutative ring R , and define the function $\phi : R \rightarrow R/I \oplus R/J$ by $\phi(r) = (r + I, r + J)$, for all $r \in R$.
- (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 $R/(I \cap J) \cong R/I \oplus R/J$.
17. Considering $\mathbf{Z}[x]$ to be a subring of $\mathbf{Q}[x]$, show that these two integral domains have the same quotient field.
18. 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:* Show that a root of $x^2 = -1$ leads to an element of order 4 in the multiplicative group \mathbf{Z}_p^\times .

Chapter 6

FIELDS

These review problems cover only the first three sections of the chapter. If you are studying abstract algebra because you plan to be a high school teacher, it is precisely these sections (along with the earlier material on polynomials) that are the most relevant to what you will be teaching.

Review Problems

1. 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 $a + bu + cu^2$.
2. (a) Show that $\mathbf{Q}(\sqrt{2} + i) = \mathbf{Q}(\sqrt{2}, i)$.
(b) Find the minimal polynomial of $\sqrt{2} + i$ over \mathbf{Q} .
3. Find the minimal polynomial of $1 + \sqrt[3]{2}$ over \mathbf{Q} .
4. Show that $x^3 + 6x^2 - 12x + 2$ is irreducible over \mathbf{Q} , and remains irreducible over $\mathbf{Q}(\sqrt[5]{2})$.
5. Find a basis for $\mathbf{Q}(\sqrt{5}, \sqrt[3]{5})$ over \mathbf{Q} .
6. Show that $[\mathbf{Q}(\sqrt{2} + \sqrt[3]{5}) : \mathbf{Q}] = 6$.
7. Find $[\mathbf{Q}(\sqrt[7]{16} + 3\sqrt[7]{8}) : \mathbf{Q}]$.
8. Find the degree of $\sqrt[3]{2} + i$ over \mathbf{Q} . Does $\sqrt[4]{2}$ belong to $\mathbf{Q}(\sqrt[3]{2} + i)$?

Chapter 1

Integers

1.1 SOLUTIONS

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

Comment: You definitely need to know how to do these computations.

Solution: We will use the Euclidean algorithm. Divide the larger number by the smaller, which should give you a quotient of 1 and a remainder of 58. Then divide the remainder 58 into 377, and continue the Euclidean algorithm as in Example 1.1.4 in the text. That should give you the following equations.

$$\begin{array}{rcl} 435 & = & 1 \cdot 377 + 58 & \gcd(435, 377) & = & \gcd(377, 58) \\ 377 & = & 6 \cdot 58 + 29 & & = & \gcd(58, 29) \\ 58 & = & 2 \cdot 29 & & = & 29 \end{array}$$

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 the linear combination we need, $29 = (7)(377) - (6)(435)$.

23. 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 22) and the matrix form. In Chapter 4, the Euclidean algorithm is used for polynomials, and the matrix method just gets too complicated, so we have to adapt the back-solving method.

Solution: Just as in Problem 22, the first step is to divide the smaller number into the larger. We get $3553 = 6 \cdot 527 + 391$, so 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. The rest of the steps in reducing the matrix to the form we want should be clear. 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 $17 = (-4)(3553) + (27)(527)$.

24. Which of the integers $0, 1, \dots, 10$ 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

$$0 = 12 \cdot 0 + 20 \cdot 0; \quad 4 = 12 \cdot 2 + 20 \cdot (-1); \quad 8 = 12 \cdot (-1) + 20 \cdot 1.$$

25. 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 ?

$$\text{Yes: } \gcd(3, 13) = 1; \quad \gcd(2, 12) = 2; \quad \gcd(5, 15) = 5; \quad \gcd(10, 20) = 10.$$

26. 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.

Solution: Since $a|b$, there is an integer m with $b = ma$. Since $b|a$, 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 $b = -a$.

27. Prove that if m and n are odd integers, then $m^2 - n^2$ is divisible by 8.

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

$$m^2 - n^2 = (2k + 1 + 2q + 1)(2k + 1 - 2q - 1) = (2)(k + q + 1)(2)(k - q) .$$

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

$$m^2 - n^2 = (2)(k + q + 1)(2)(2)(p) = (8)(k + q + 1)(p) .$$

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

$$m^2 - n^2 = (2)(2)(t)(2)(k - q) = (8)(t)(k - q) .$$

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.

28. Prove that if n is an integer with $n > 1$, then $\gcd(n - 1, n^2 + n + 1) = 1$ 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 $\gcd(6, 57) = 3$. These calculations don't prove anything, but maybe they do make the problem look plausible.

Solution: Problem 25 gives a hint. 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. Dividing $n^2 + n + 1$ by $n - 1$ (using long division of polynomials) we get a quotient of $n + 2$ and a remainder of 3, so $n^2 + n + 1 = (n + 2)(n - 1) + 3$. Now we can see that any common divisor of $n - 1$ and $n^2 + n + 1$ must be a divisor of 3, so the answer has to be 1 or 3.

29. 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 it 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.

$$\begin{aligned} \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}^2 &= \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \\ \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}^3 &= \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{bmatrix} \\ \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}^4 &= \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{aligned}$$

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 $0 \leq r < 4$. 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 $4|n$.

30. 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 4 in the text.

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 $n = 1, 2, \dots$, 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.

1.2 SOLUTIONS

23. (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 1492 and 1776 to find $\gcd(1776, 1492)$.

Solution: Since $1776 = 2^4 \cdot 3 \cdot 37$ and $1492 = 2^2 \cdot 373$, Proposition 1.2.9 shows that $\gcd(1776, 1492) = 2^2$.

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

Solution: We have $1274 = 1089 \cdot 1 + 185$; $1089 = 185 \cdot 5 + 164$;

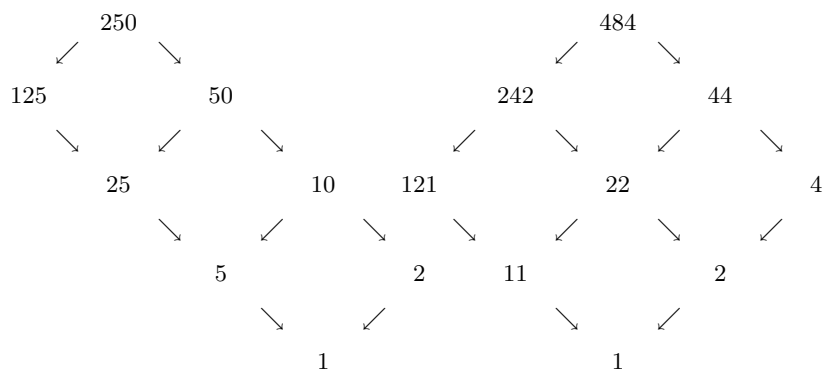
$185 = 164 \cdot 1 + 21$; $164 = 21 \cdot 7 + 17$; $21 = 17 \cdot 1 + 4$; $17 = 4 \cdot 4 + 1$. Thus $\gcd(1274, 1089) = 1$.

- (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.

25. Give the lattice 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 by 5 produces 50, 10, and 2, in succession. These numbers go along one axis of the rectangular diagram.



26. 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 $(-21, 2)$.

27. 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 $\gcd(a, b^2) = 1$.

28. 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: We can write $(1)(2n - 1) + (-2)(n - 1) = 1$, which proves that $\gcd(2n - 1, n - 1) = 1$. 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.

29. 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, we recall that the following identity holds for all values of x : $x^k - 1 = (x - 1)(x^{k-1} + x^{k-2} + \cdots + x + 1)$.

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 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 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.

30. 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 $n - 1$. We have shown 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 28 to conclude that $2n^2 + 4n - 3$ and $2n^2 + 6n - 4$ are relatively prime since $2n - 1$ and $n - 1$ are relatively prime.

(Of course, you could also continue with the Euclidean algorithm, getting $\gcd(2n - 1, n - 1) = \gcd(n - 2, 1) = 1$.)

1.3 SOLUTIONS

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

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 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 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 $-14, -29, -34$, 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 $x \equiv 11, 26, 41, 56, 71, 86 \pmod{90}$.

27. (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

$$55x \equiv 35 \pmod{75}; \quad 11x \equiv 7 \pmod{15}; \quad 44x \equiv 28 \pmod{15};$$

$$-x \equiv 13 \pmod{15}; \quad x \equiv 2 \pmod{15}. \quad \text{The solution is}$$

$$x \equiv 2, 17, 32, 47, 62 \pmod{75}.$$

- (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.

28. (a) Find one particular integer solution to the equation $110x + 75y = 45$.

Solution: Any linear combination of 110 and 75 is a multiple of the gcd.

$$\begin{bmatrix} 1 & 0 & 110 \\ 0 & 1 & 75 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 35 \\ 0 & 1 & 75 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 35 \\ -2 & 3 & 5 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 15 & -22 & 0 \\ -2 & 3 & 5 \end{bmatrix}$$

Thus $-2(110) + 3(75) = 5$, and multiplying by 9 yields a solution $x = -18$, $y = 27$.

Comment: The matrix computation shows that $110(15) + 75(-22) = 0$, so adding any multiple of the vector $(15, -22)$ to the particular solution $(-18, 27)$ will also determine a solution.

Second solution: The equation reduces to the congruence $35x \equiv 45 \pmod{75}$. This reduces 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.

(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 $110(15) - 75(22) = 0$.

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

Solution: Convert the second congruence to the equation $x = 4 + 10q$ for some $q \in \mathbf{Z}$. Then $4 + 10q \equiv 2 \pmod{9}$, which reduces to $q \equiv 7 \pmod{9}$. Thus the solution is $x \equiv 74 \pmod{90}$.

30. 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 $9 \cdot 3 \equiv 1 \pmod{13}$,

$$\text{so } 5x \equiv 14 \pmod{17}; \quad 35x \equiv 98 \pmod{17}; \quad x \equiv 13 \pmod{17}$$

$$\text{and } 3x \equiv 2 \pmod{13}; \quad 27x \equiv 18 \pmod{13}; \quad x \equiv 5 \pmod{13}.$$

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, $x \equiv 13 + 17 \cdot 11 \equiv 200 \pmod{221}$.

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

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 $x \equiv 55 \pmod{25 \cdot 32}$.

32. Give integers a, b, m, n to provide an example of a system

$$x \equiv a \pmod{m} \quad x \equiv b \pmod{n}$$

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 $b = 0$.

33. (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 $6^2 \equiv 6 \pmod{10}$. Thus $4^{100} = (4^2)^{50} \equiv 6^{50} \equiv 6 \pmod{10}$.

(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 $(3, 2^{200}) = 1$.

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

Solution: This is equivalent 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 $x \equiv \pm 5 \pmod{13}$.

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

Solution: This could be proved by induction, but a more elegant proof can be given by simply observing that $10^{n+1} + 4 \cdot 10^n + 4 \equiv 0 \pmod{9}$ since $10 \equiv 1 \pmod{9}$.

36. 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.

1.4 SOLUTIONS

30. 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.

31. 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 . Using 14, we see that $[2]_{13}$ and $[7]_{13}$ are inverses. Using 12, and we see that $[3]_{13}$ and $[-4]_{13}$ are inverses, as are the pairs $[4]_{13}$ and $[-3]_{13}$, and $[6]_{13}$ and $[-2]_{13}$. Using 40, we see that $[5]_{13}$ and $[8]_{13}$ are inverses. Finally, 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 takes care of all of the nonzero elements of \mathbf{Z}_{13} .

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

Solution: We need to use the Euclidean algorithm.

$$\begin{bmatrix} 1 & 0 & 501 \\ 0 & 1 & 91 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -5 & 46 \\ 0 & 1 & 91 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -5 & 46 \\ -1 & 6 & 45 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 2 & -11 & 1 \\ -1 & 6 & 45 \end{bmatrix}$$

$$\text{Thus } [91]_{501}^{-1} = [-11]_{501} = [490]_{501}.$$

33. 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 $(4061, 3379) = 31$.

34. 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 to check 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 $[3]_{20}^{-1} = [7]_{20}$, $[9]_{20}^{-1} = [9]_{20}$, $[11]_{20}^{-1} = [11]_{20}$, $[13]_{20}^{-1} = [17]_{20}$, and $[19]_{20}^{-1} = [19]_{20}$.

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 1.4.13 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 Problem 1.4.40. They are $[0]_{20}$ and $[10]_{20}$.

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

Solution: The units of \mathbf{Z}_{24} are the equivalence classes represented by 1, 5, 7, 11, 13, 17, 19, and 23. For each of these numbers we have $x^2 \equiv 1 \pmod{24}$, and so each element is its own inverse.

The idempotent elements are $[0]_{24}$, $[1]_{24}$, $[9]_{24}$, $[16]_{24}$, and the nilpotent elements are $[0]_{24}$, $[6]_{24}$, $[12]_{24}$, $[18]_{24}$.

36. 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 that 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 $[2]^4 = [16] = [-1]$. Problem 39 shows that the multiplicative order of an element has to be a divisor of 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 is 16 itself, so $[3]$ does in fact have multiplicative order 16, and we are done.

37. 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 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.

38. 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 solution is $[x] = [-3]$ or $[x] = [2]$.

39. Let n be a positive integer, and let $a \in \mathbf{Z}$ with $\gcd(a, n) = 1$. Prove that if k is the smallest positive integer for which $a^k \equiv 1 \pmod{n}$, then $k \mid \varphi(n)$.

Solution: Assume that k is the smallest positive integer for which $a^k \equiv 1 \pmod{n}$. We can use the division algorithm to write $\varphi(n) = qk + r$, where $0 \leq r < k$, and $q \in \mathbf{Z}$. Since $a^k \equiv 1 \pmod{n}$, we know that $\gcd(a, n) = 1$, and so we can apply Theorem 1.4.11, which shows that $a^{\varphi(n)} \equiv 1 \pmod{n}$. Thus $a^r = a^{\varphi(n) - kq} = a^{\varphi(n)}(a^k)^{-q} \equiv 1 \pmod{n}$, so we must have $r = 0$ since $r < k$ and k is the smallest positive integer with $a^k \equiv 1 \pmod{n}$.

40. 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 $[a]_n^k = [0]_n$.

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.

SOLUTIONS TO THE REVIEW PROBLEMS

1. 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 $117 = (-3) \cdot 7605 + 4 \cdot 5733$.

2. For $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, prove that $\omega^n = 1$ if and only if $3 \mid n$, for any integer n .

Solution: Calculations in the introduction to Chapter 1 show 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 $3|n$.

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

Solution: First we find that $\gcd(24, 200) = 8$, and $8 | 168$, 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.

$$\begin{aligned} 24x &\equiv 168 \pmod{200} \\ 3x &\equiv 21 \pmod{25} \\ -24x &\equiv -168 \pmod{25} \\ x &\equiv 7 \pmod{25} \end{aligned}$$

The solution is $x \equiv 7, 32, 57, 82, 107, 132, 157, 182 \pmod{200}$.

4. 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 $x \equiv -3 \pmod{11 \cdot 15}$.

5. 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 $\varphi(15) = 8$. By Problem 39, 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.

6. 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.

Second solution: Since n is odd, the integers n and $2n$ are relatively prime, and so it follows from Exercise 1.4.27 of the text that $\varphi(2n) = \varphi(2)\varphi(n) = \varphi(n)$.

Chapter 2

Functions

2.1 SOLUTIONS

20. 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”.

21. 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.

more than one

22. 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 2.1.7.

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 $f : \mathbf{R} \rightarrow \mathbf{R}$ 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 (x, y) lies on the graph of f^{-1} . Conversely, if (x, y) lies on the graph of f^{-1} , then $x = f^{-1}(y)$, and therefore $y = f(f^{-1}(y)) = f(x)$, which shows that (y, x) 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.

23. Let A be an $n \times n$ matrix with entries in \mathbf{R} . Define a linear transformation $L : \mathbf{R}^n \rightarrow \mathbf{R}^n$ 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 this 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.

24. Let A be an $m \times n$ matrix with entries in \mathbf{R} , and assume that $m > n$. Define a linear transformation $L : \mathbf{R}^n \rightarrow \mathbf{R}^m$ 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 .

Solution: If $\det(A^T A) \neq 0$, then $A^T A$ is an invertible matrix. If we define $K : \mathbf{R}^m \rightarrow \mathbf{R}^n$ by $K(\mathbf{x}) = (A^T A)^{-1} A^T \mathbf{x}$, for all $\mathbf{x} \in \mathbf{R}^m$, then KL is the identity function on \mathbf{R}^n . It then follows from Exercise 17 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 $\det(A^T A)$ 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 $\det(A^T A) \neq 0$ 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 $\det(A^T A) \neq 0$.

25. Let A be an $n \times n$ matrix with entries in \mathbf{R} . Define a linear transformation $L : \mathbf{R}^n \rightarrow \mathbf{R}^n$ 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 zero.

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

Solution: As noted in the solution to problem 23, $A\mathbf{x}_1 = A\mathbf{x}_2$ 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 .

26. Let a be a fixed element of \mathbf{Z}_{17}^\times . Define the function $\theta : \mathbf{Z}_{17}^\times \rightarrow \mathbf{Z}_{17}^\times$ 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 $\psi : \mathbf{Z}_{17}^\times \rightarrow \mathbf{Z}_{17}^\times$ 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.

2.2 SOLUTIONS

14. 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 $a_1b_2 = a_2b_1$, and so $a_2b_1 = a_1b_2$, 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 $a_1b_2 = a_2b_1$ and $a_2b_3 = a_3b_2$. If we multiply the first equation by b_3 and the second equation by b_1 , we get $a_1b_2b_3 = a_2b_1b_3 = a_3b_1b_2$. Since $b_2 \neq 0$ we can cancel to obtain $a_1b_3 = a_3b_1$, showing that $(a_1, b_1) \sim (a_3, b_3)$.

15. On the set \mathbf{C} of complex numbers, define $z_1 \sim z_2$ if $\|z_1\| = \|z_2\|$. Show that \sim is an equivalence relation.

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.

16. 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 an equality, and can easily be verified. Since \mathbf{u} has length 1, $\mathbf{v} \cdot \mathbf{u}$ 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} . It follows that the equivalence classes of \sim are the planes in \mathbf{R}^3 that are perpendicular to \mathbf{u} .

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

Solution: The equivalence relation determined by f is defined by setting $a \sim b$ if $f(a) = f(b)$, so $a \sim b$ if and only if $a^2 = b^2$, or, $a \sim b$ if and only if $|a| = |b|$.

18. For the linear transformation $L : \mathbf{R}^3 \rightarrow \mathbf{R}^3$ 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 $(a_1, a_2, a_3) \sim (b_1, b_2, b_3)$ if $L(a_1, a_2, a_3) = L(b_1, b_2, b_3)$, it follows from the definition of L that $(a_1, a_2, a_3) \sim (b_1, b_2, b_3)$ 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 $(1, 1, 1)$.

19. Define the formula $f : \mathbf{Z}_{12} \rightarrow \mathbf{Z}_{12}$ 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 of f and the set \mathbf{Z}_{12}/f of equivalence classes determined by f .

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 images of f we have $[0]_{12}^2 = [0]_{12}$, $[\pm 1]_{12}^2 = [1]_{12}$, $[\pm 2]_{12}^2 = [4]_{12}$, $[\pm 3]_{12}^2 = [9]_{12}$, $[\pm 4]_{12}^2 = [4]_{12}$, $[\pm 5]_{12}^2 = [1]_{12}$, and $[6]_{12}^2 = [0]_{12}$. Thus $f(\mathbf{Z}_{12}) = \{[0]_{12}, [1]_{12}, [4]_{12}, [9]_{12}\}$. The corresponding equivalence classes determined by f are $\{[0]_{12}, [6]_{12}\}$, $\{[\pm 1]_{12}, [\pm 5]_{12}\}$, $\{[\pm 2]_{12}, [\pm 4]_{12}\}$, $\{[\pm 3]_{12}\}$.

20. On the set of all $n \times n$ matrices over \mathbf{R} , define $A \sim B$ if there exists an invertible matrix P such that $PAP^{-1} = B$. Check that \sim defines an equivalence relation.

Solution: We have $A \sim A$ since $IAI^{-1} = A$, where I is the $n \times n$ identity matrix. If $A \sim B$, then $PAP^{-1} = B$ for some invertible matrix P , and so we get $A = P^{-1}B(P^{-1})^{-1}$. If $A \sim B$ and $B \sim C$, then $PAP^{-1} = B$ and $QBQ^{-1} = C$ for some P, Q . Substituting gives $Q(PAP^{-1})Q^{-1} = (QP)A(QP)^{-1} = C$, and so $A \sim C$.

2.3 SOLUTIONS

13. 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 ? Is σ an even permutation? Compute σ^{-1} .

Solution: We have $\sigma = (1, 7, 8)(2, 5)(3, 6, 4, 9)$, and so its order is 12 since $\text{lcm}[3, 2, 4] = 12$. It is an even permutation, since it can be expressed as the product of 6 transpositions. We have $\sigma^{-1} = (1, 8, 7)(2, 5)(3, 9, 4, 6)$.

14. 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: $\sigma, \tau, \sigma\tau, \sigma\tau\sigma^{-1}, \sigma^{-1}, \tau^{-1}, \tau\sigma, \tau\sigma\tau^{-1}$.

Solution: $\sigma = (1, 2, 5, 3)(4, 8, 7)$; $\tau = (2, 5)(3, 4, 7, 8, 9)$; $\sigma\tau = (1, 2, 3, 8, 9)$; $\sigma\tau\sigma^{-1} = (1, 8, 4, 7, 9)(3, 5)$; $\sigma^{-1} = (1, 3, 5, 2)(4, 7, 8)$; $\tau^{-1} = (2, 5)(3, 9, 8, 7, 4)$; $\tau\sigma = (1, 5, 4, 9, 3)$; $\tau\sigma\tau^{-1} = (1, 5, 2, 4)(7, 9, 8)$.

15. 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 $\sigma^{-1} = (1, 8, 3, 6, 9)(2, 7, 5)$.

16. 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. We have $\sigma\tau\sigma^{-1} = (3, 8, 7)(1, 7, 9)(3, 11, 5, 6, 8, 10)(3, 7, 8) = (1, 3, 9)(8, 11, 5, 6, 7, 10)$, 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.

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

Solution: Assume that $\tau \in \mathcal{S}_n$ 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 $\tau^k = \sigma^{-1}\sigma = (1)$.

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

Solution: The permutation $(1, 2)(3, 4, 5, 6, 7)$ has order 10, while 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} .

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

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

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

is a group of permutations.

SOLUTIONS TO THE REVIEW PROBLEMS

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

2. Define $f : \mathbf{R} \rightarrow \mathbf{R}$ by $f(x) = x^3 + 3xz - 5$, for all $x \in \mathbf{R}$. Show that f is a one-to-one function.

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

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?

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 $\phi : \mathbf{Z}_{17}^{\times} \rightarrow \mathbf{Z}_{17}^{\times}$ 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 $\phi_\alpha : S_n \rightarrow S_n$ 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.

Another way to show that ϕ_α is one-to-one and onto is to 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 $\phi_\alpha((1, 3, 2)) = (1, 2, 3)$.

Chapter 3

Groups

3.1 SOLUTIONS

22. 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 .

23. 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.

24. On the set $G = \mathbf{Q}^\times$ of nonzero rational numbers, define a new multiplication by $a * b = \frac{ab}{2}$, 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 $\frac{ab}{2}$, 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

$$(a * b) * c = \left(\frac{ab}{2}\right) * c = \frac{\left(\frac{ab}{2}\right)c}{2} = \frac{(ab)c}{4}.$$

The number 2 acts as the multiplicative identity, and if a is nonzero, then $\frac{4}{a}$ is a nonzero rational number that serves as the multiplicative inverse of a .

25. Write out the multiplication table for \mathbf{Z}_9^\times .

Solution: $\mathbf{Z}_9^\times = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\}$. We will write m for $[m]_9$.

| | | | | | | |
|---|---|---|---|---|---|---|
| · | 1 | 2 | 4 | 5 | 7 | 8 |
| 1 | 1 | 2 | 4 | 5 | 7 | 8 |
| 2 | 2 | 4 | 8 | 1 | 5 | 7 |
| 4 | 4 | 8 | 7 | 2 | 1 | 5 |
| 5 | 5 | 1 | 2 | 7 | 8 | 4 |
| 7 | 7 | 5 | 1 | 8 | 4 | 2 |
| 8 | 8 | 7 | 5 | 4 | 2 | 1 |

Comment: Rewriting the table, with the elements in a slightly different order, gives a different picture of the group.

| | | | | | | |
|---|---|---|---|---|---|---|
| · | 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 |

Each element in the group is a power of 2, and the second table shows what happens when we arrange the elements in order, as successive powers of 2.

26. 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 $\{1, 2, 4, 7, -7, -4, -2, -1\}$.

| | | | | | | | | |
|----|----|----|----|----|----|----|----|----|
| · | 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 makes it to use the representatives $\{\pm 1, \pm 2, \pm 4, \pm 7\}$ when listing the congruence classes in the group.

27. 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 $ba = ab$.

28. 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 .

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.

$$\begin{aligned} (aba^{-1})^{k+1} &= (aba^{-1})^k(aba^{-1}) \\ &= (ab^k a^{-1})(aba^{-1}) \\ &= (ab^k)(a^{-1}a)(ba^{-1}) \\ &= (ab^k)(ba^{-1}) \\ &= ab^{k+1}a^{-1} \end{aligned}$$

Thus the statement holds for $n = k + 1$, so by induction it holds for all values of n .

29. In Definition 3.1.3 of the text, 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.

30. The previous exercise 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 $(-1)*x = -1$ have no simultaneous solution in G . Finally, $1/|a|$ is a right inverse for any $a \in G$, but the equation $x*a = 1$ 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.

31. Let F be the set of all *fractional linear transformations* of the complex plane. That is, F is the set of all functions $f(z) : \mathbf{C} \rightarrow \mathbf{C}$ of the form $f(z) = \frac{az + b}{cz + d}$,

where the coefficients a, b, c, d are integers with $ad - bc = 1$. Show that F forms a group under 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 3.1.3.

Let $f_1(z) = \frac{a_1z + b_1}{c_1z + d_1}$, and $f_2(z) = \frac{a_2z + b_2}{c_2z + d_2}$, with $a_1d_1 - b_1c_1 = 1$ and $a_2d_2 - b_2c_2 = 1$. Then for any complex number z we have

$$\begin{aligned} f_2 \circ f_1(z) &= f_2(f_1(z)) = \frac{a_2f_1(z) + b_2}{c_2f_1(z) + d_2} \\ &= \frac{a_2\left(\frac{a_1z + b_1}{c_1z + d_1}\right) + b_2}{c_2\left(\frac{a_1z + b_1}{c_1z + d_1}\right) + d_2} \\ &= \frac{a_2(a_1z + b_1) + b_2(c_1z + d_1)}{c_2(a_1z + b_1) + d_2(c_1z + d_1)} \\ &= \frac{(a_2a_1 + b_2c_1)z + (a_2b_1 + b_2d_1)}{(c_2a_1 + d_2c_1)z + (c_2b_1 + d_2d_1)}. \end{aligned}$$

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 $f_2(z) = \frac{a_2z + b_2}{c_2z + d_2}$ and $f_1(z) = \frac{a_1z + b_1}{c_1z + d_1}$ 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 always associative (compare Exercise 3.1.2 in the text, for matrices), and the identity function will serve as an identity element for F . We only need to check that it can be written in the correct form, as a fractional linear transformation, and 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

$f(z) = \frac{az+b}{cz+d}$. This gives $f^{-1}(z) = \frac{dz-b}{-cz+a}$, and completes the proof that F forms a group under composition of functions.

32. 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 $*$.

Solution: Since the operation is 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, $a * (a/(a - 1)) = a^2/(a - 1) - a - a/(a - 1) + 2 = (a^2 - a^2 + a - a)/(a - 1) + 2 = 2$.

3.2 SOLUTIONS

23. 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 $[1]_{24}$.

24. 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 $\langle [3] \rangle$ is a cyclic subgroup of order 4.

The element $[9] = [3]^2$ has order 2. It is easy to check that the subset $H = \{\pm[1], \pm[9]\}$ is closed. Since H is a finite, nonempty subset of a known group, Corollary 3.2.4 implies that it is a subgroup. Finally, H is not cyclic since no element of H has order 4.

25. (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.

26. In $G = \mathbf{Z}_{21}^\times$, show that

$$H = \{[x]_{21} \mid x \equiv 1 \pmod{3}\} \quad \text{and} \quad K = \{[x]_{21} \mid x \equiv 1 \pmod{7}\}$$

are subgroups of G .

Solution: The subset H is finite and nonempty (it certainly contains $[1]_{21}$), so by Corollary 3.2.4 it is enough to show that H is closed under multiplication. If $[x]_{21}$ and $[y]_{21}$ 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 $[x]_{21} \cdot [y]_{21} = [xy]_{21}$ belongs to H .

A similar argument shows that K is a subgroup of \mathbf{Z}_{21}^\times .

27. 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: First, the subset N is nonempty since the identity element e can always be written in the form $e = e^n$. Next, 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 $g_1 g_2 = a_1^n a_2^n = (a_1 a_2)^n$. The last equality holds since G is abelian. Finally, 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 .

28. 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 $[2]_p$ 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 $2^k - 1 < 2^n + 1 = p$. This shows that $[2]_p$ has order $2n$.

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

Solution: The order of $[2]_p$ 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.

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

Solution: It is probably easiest to change these complex numbers from rectangular coordinates into polar coordinates. (See Appendix A.5 for a discussion of the properties of complex numbers.) Each of the numbers has magnitude 1, and you can check that

$$-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i = \cos(3\pi/4) + i\sin(3\pi/4) \quad \text{and} \quad -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i = \cos(5\pi/4) + i\sin(5\pi/4).$$

We can use De Moivre's Theorem (Theorem A.5.2) to compute powers of complex numbers. It follows from this theorem that $(\cos(3\pi/4) + i\sin(3\pi/4))^8 = \cos(6\pi) + i\sin(6\pi) = 1$, and so $-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ 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.

30. In the group $G = GL_2(\mathbf{R})$ of invertible 2×2 matrices with real entries, show that

$$H = \left\{ \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \mid \theta \in \mathbf{R} \right\}$$

is a subgroup of G .

Solution: 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.

$$\begin{aligned} & \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \begin{bmatrix} \cos \phi & -\sin \phi \\ \sin \phi & \cos \phi \end{bmatrix} \\ &= \begin{bmatrix} \cos \theta \cos \phi - \sin \theta \sin \phi & -\cos \theta \sin \phi - \sin \theta \cos \phi \\ \sin \theta \cos \phi + \cos \theta \sin \phi & -\sin \theta \sin \phi + \cos \theta \cos \phi \end{bmatrix} \\ &= \begin{bmatrix} \cos \theta \cos \phi - \sin \theta \sin \phi & -(\sin \theta \cos \phi + \cos \theta \sin \phi) \\ \sin \theta \cos \phi + \cos \theta \sin \phi & \cos \theta \cos \phi - \sin \theta \sin \phi \end{bmatrix} \\ &= \begin{bmatrix} \cos(\theta + \phi) & -\sin(\theta + \phi) \\ \sin(\theta + \phi) & \cos(\theta + \phi) \end{bmatrix} \in H. \end{aligned}$$

Identity: To see that the identity matrix is in the set, let $\theta = 0$.

Existence of inverses: $\begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}^{-1} = \begin{bmatrix} \cos(-\theta) & -\sin(-\theta) \\ \sin(-\theta) & \cos(-\theta) \end{bmatrix} \in H.$

31. Let K be the following subset of $GL_2(\mathbf{R})$.

$$K = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid d = a, \quad c = -2b, \quad ad - bc \neq 0 \right\}$$

Show that K is a subgroup of $GL_2(\mathbf{R})$.

Solution: The closure axiom holds since

$$\begin{bmatrix} a_1 & b_1 \\ -2b_1 & a_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ -2b_2 & a_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 - 2b_1b_2 & a_1b_2 + b_1a_2 \\ -2(a_1b_2 - b_1a_2) & a_1a_2 - 2b_1b_2 \end{bmatrix}. \text{ The}$$

identity matrix belongs to K , and $\begin{bmatrix} a & b \\ -2b & a \end{bmatrix}^{-1} = \frac{1}{a^2 + 2b^2} \begin{bmatrix} a & -b \\ -2(-b) & a \end{bmatrix}$.

Comment: We don't need to worry about the condition $ad - bc \neq 0$, since for any element in H the determinant is $a^2 + 2b^2$, which is always positive.

32. Compute the centralizer in $GL_2(\mathbf{R})$ of the matrix $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$.

Note: Exercise 3.2.14 in the text defines the centralizer of an element a of the group G to be $C(a) = \{x \in G \mid xa = ax\}$.

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 $GL_2(\mathbf{R})$. 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 $GL_2(\mathbf{R})$ of the matrix $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ is the subgroup $\left\{ \begin{bmatrix} a & b \\ b & a-b \end{bmatrix} \mid a, b \in \mathbf{R} \text{ and } ab \neq a^2 + b^2 \right\}$.

3.3 SOLUTIONS

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

Solution: By Proposition 3.3.4 (b), then 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 $\mathbf{Z}_5 \times \mathbf{Z}_3$.

17. 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 $\text{lcm}[4, 6] = 12$.

18. 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.

19. 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 3.2.26) 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 $HK = G$.

20. Show that if p is a prime number, then the order of the general linear group $\text{GL}_n(\mathbf{Z}_p)$ is $(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.

Solution: We need to count the number of ways in which an invertible matrix can be constructed. This is done by noting that we need n linearly independent rows. The first row can be any nonzero vector, so there are $p^n - 1$ choices.

There are p^n 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 $p^n - p$.

For the third row, we need to subtract p^2 , which is the number of vectors in the subspace spanned by the first two rows that we have chosen. Thus there are $p^n - p^2$ possibilities for the third row. This argument can be continued, giving the stated result. (A more formal proof could be given by induction.)

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

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 $o(A) = 4$.

22. Let G be the subgroup of $GL_2(\mathbf{R})$ defined by

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

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 $C(A) = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \mid b \in \mathbf{R} \right\}$.

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 $C(B) = \left\{ \begin{bmatrix} m & 0 \\ 0 & 1 \end{bmatrix} \mid 0 \neq m \in \mathbf{R} \right\}$.

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.

23. Compute the centralizer in $GL_2(\mathbf{Z}_3)$ of the matrix $\begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$.

Solution: Let $A = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$, and suppose that $X = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ belongs to the centralizer of A in $GL_2(\mathbf{Z}_3)$. Then $XA = AX$, and so $\begin{bmatrix} 2a & a+2b \\ 2c & c+2d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 2a+c & 2b+d \\ 2c & 2d \end{bmatrix}$. Equating corresponding entries shows that we must have $2a = 2a + c$, $a + 2b = 2b + d$, $2c = 2c$, and $c + 2d = 2d$. The first equation implies that $c = 0$, while the

second equation implies that $a = d$. It follows that the centralizer in $GL_2(\mathbf{Z}_3)$ of the matrix $\begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$ is the subgroup $\left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \mid a, b \in \mathbf{Z}_3 \text{ and } a \neq 0 \right\}$.

Comment: The centralizer contains 6 elements, while it follows from Problem 20 in this section that $GL_2(\mathbf{Z}_3)$ has $(3^2 - 1)(3^2 - 3) = 48$ elements.

24. Compute the centralizer in $GL_2(\mathbf{Z}_3)$ 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 $GL_2(\mathbf{Z}_3)$. Then $XA = AX$, and so $\begin{bmatrix} 2a+b & a+b \\ 2c+d & c+d \end{bmatrix} =$

$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 2a+c & 2b+d \\ a+c & b+d \end{bmatrix}$. 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 equation implies that $c = b$, while the second equation implies that $d = a - b$. It follows that the centralizer in $GL_2(\mathbf{Z}_3)$ of the matrix $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ is the subgroup

$$\left\{ \begin{bmatrix} a & b \\ b & a-b \end{bmatrix} \mid a, b \in \mathbf{Z}_3 \text{ and } a \neq 0 \text{ or } b \neq 0 \right\}.$$

Comment: In this case the centralizer contains 8 of the 48 elements in $GL_2(\mathbf{Z}_3)$.

25. Let H be the following subset of the group $G = GL_2(\mathbf{Z}_5)$.

$$H = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbf{Z}_5) \mid m, b \in \mathbf{Z}_5, m = \pm 1 \right\}$$

- (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 $A^i B^j$, 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 .

3.4 SOLUTIONS

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

Solution: The element $[3]$ is a generator for \mathbf{Z}_{17}^\times , since $3^2 = 9$, $3^3 = 27 \equiv 10$, $3^4 \equiv 3 \cdot 10 \equiv 30 \equiv 13$, $3^5 \equiv 3 \cdot 13 \equiv 39 \equiv 5$, $3^6 \equiv 3 \cdot 5 \equiv 15$, $3^7 \equiv 3 \cdot 15 \equiv 45 \equiv 11$, and $3^8 \equiv 3 \cdot 11 \equiv 33 \equiv -1 \not\equiv 1$. Therefore \mathbf{Z}_{17}^\times is a cyclic group with 16 elements. 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.

Define $\phi : \mathbf{Z}_{16} \rightarrow \mathbf{Z}_{17}^\times$ 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 2.1.5 that ϕ is also an onto function. The proof that ϕ respects the two group operations follows the proof in Example 3.4.1. 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.

22. Let $\phi : \mathbf{R}^\times \rightarrow \mathbf{R}^\times$ 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 $x = \sqrt[3]{y}$.

23. Let G_1, G_2, H_1, H_2 be groups, and suppose that $\theta_1 : G_1 \rightarrow H_1$ and $\theta_2 : G_2 \rightarrow H_2$ are group isomorphisms. Define $\phi : G_1 \times G_2 \rightarrow H_1 \times H_2$ 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

$$\begin{aligned} \phi((a_1, a_2) \cdot (b_1, b_2)) &= \phi((a_1b_1, a_2b_2)) = (\theta_1(a_1b_1), \theta_2(a_2b_2)) \\ &= (\theta_1(a_1)\theta_1(b_1), \theta_2(a_2)\theta_2(b_2)) \\ \phi((a_1, a_2)) \cdot \phi((b_1, b_2)) &= (\theta_1(a_1), \theta_2(a_2)) \cdot (\theta_1(b_1), \theta_2(b_2)) \\ &= (\theta_1(a_1)\theta_1(b_1), \theta_2(a_2)\theta_2(b_2)) \end{aligned}$$

and so $\phi : G_1 \times G_2 \rightarrow H_1 \times H_2$ is a group isomorphism.

24. 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 21, you can show that $\theta_1 : \mathbf{Z}_6 \rightarrow \mathbf{Z}_7^\times$ defined by $\theta_1([n]_6) = [3]_7^n$ and $\theta_2 : \mathbf{Z}_{10} \rightarrow \mathbf{Z}_{11}^\times$ defined by $\theta_2([m]_{10}) = [2]_{11}^m$ are group isomorphisms. It then follows from Problem 23 that $\phi : \mathbf{Z}_6 \times \mathbf{Z}_{10} \rightarrow \mathbf{Z}_7^\times \times \mathbf{Z}_{11}^\times$ 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.

25. Define $\phi : \mathbf{Z}_{30} \times \mathbf{Z}_2 \rightarrow \mathbf{Z}_{10} \times \mathbf{Z}_6$ by $\phi([n]_{30}, [m]_2) = ([n]_{10}, [4n + 3m]_6)$, for all $([n]_{30}, [m]_2) \in \mathbf{Z}_{30} \times \mathbf{Z}_2$. 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. This means that we can use Proposition 3.4.4 to show that ϕ is one-to-one. If $\phi([n]_{30}, [m]_2) = ([0]_{10}, [0]_2)$, 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 $\phi([n]_{30}, [m]_2) = ([0]_{10}, [0]_2)$, then $([n]_{30}, [m]_2) = ([0]_{30}, [0]_2)$, and so the condition in Proposition 3.4.4 is satisfied. We conclude that ϕ is a one-to-one function. Since the two 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 may conclude that ϕ is a group isomorphism.

26. 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 3.4.13 in the text, the function $\phi : G \rightarrow G$ defined by $\phi(x) = axa^{-1}$, for all $x \in G$, is a group isomorphism. By Exercise 3.4.15 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 $\theta : H \rightarrow aHa^{-1}$ defined by $\theta(x) = axa^{-1}$ is an isomorphism.

27. Let G, G_1, G_2 be groups. Prove that if G is isomorphic to $G_1 \times G_2$, 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: Let $\phi : G_1 \times G_2 \rightarrow G$ be an isomorphism. Exercise 3.3.9 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. We know (by Exercise 3.4.15) that 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.

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

Solution: Since each matrix in $\text{GL}_2(\mathbf{Z}_p)$ has nonzero determinant, it is clear that the mapping $\phi : \mathbf{Z}_p^\times \times \mathbf{Z}_p^\times \rightarrow \text{GL}_2(\mathbf{Z}_p)$ 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.

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

$$H = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in \text{GL}_2(\mathbf{R}) \mid a_{11} = 1, a_{21} = 0, a_{22} = 1 \right\}$$

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 $\phi : \mathbf{R} \rightarrow H$ 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.)

30. Let G be the subgroup of $GL_2(\mathbf{R})$ defined by

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

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.

31. Let H be the following subgroup of group $G = GL_2(\mathbf{Z}_3)$.

$$H = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbf{Z}_3) \mid m, b \in \mathbf{Z}_3, m \neq 0 \right\}$$

Show that H is isomorphic to the symmetric group \mathcal{S}_3 .

Solution: This group is small enough that we can just compare its multiplication table to that of \mathcal{S}_3 , as given in Table 3.3.3 (on page 104 of the text). 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 3.3.25, we can show that $BA = A^{-1}B$, and that each element of H has the form can be written uniquely in the form $A^i B^j$, where $0 \leq i < 3$ and $0 \leq j < 2$. This information should make it plausible that the function $\phi : \mathcal{S}_3 \rightarrow H$ defined by $\phi(a^i b^j) = A^i B^j$, 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 look exactly the same.

32. Let G be a group, and let S be any set for which there exists a one-to-one and onto function $\phi : G \rightarrow S$. Define an operation on S by setting $x_1 \cdot x_2 = \phi(\phi^{-1}(x_1)\phi^{-1}(x_2))$, for all $x_1, x_2 \in S$. Prove that S is a group under this operation, and that ϕ is actually a group isomorphism.

Solution: (*Outline only*) The operation is well-defined on S , since ϕ and ϕ^{-1} are functions and the operation on G is well-defined. The associative law holds

in S because it holds in G ; the identity element in S is $\phi(e)$, where e is the identity of G , and it is easy to check that if $x \in S$, then $x^{-1} = \phi((\phi^{-1}(x))^{-1})$.

Comment: This reveals the secret behind problems like Exercises 3.1.11 and 3.4.12 in the text. Given a known group G such as \mathbf{R}^\times , we can use one-to-one functions defined on G to produce new groups with operations that look rather different from the usual examples.

3.5 SOLUTIONS

20. 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 , $2^2 = 4$, $2^3 = 8 \neq 1$, and so $[2]$ 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 , $5^2 \equiv 7$, $5^3 \equiv 17 \neq 1$, and so $[5]$ 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.

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

Solution: It follows from Theorem 3.5.4 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 3.4.23 that $\mathbf{Z}_4 \times \mathbf{Z}_{10} \cong \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_5$, and $\mathbf{Z}_2 \times \mathbf{Z}_{20} \cong \mathbf{Z}_2 \cong \mathbf{Z}_4 \times \mathbf{Z}_5$. Finally, it is possible to show that the obvious mapping from $\mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_5$ onto $\mathbf{Z}_2 \cong \mathbf{Z}_4 \times \mathbf{Z}_5$ is an isomorphism. Therefore $\mathbf{Z}_4 \times \mathbf{Z}_{10} \cong \mathbf{Z}_2 \times \mathbf{Z}_{20}$.

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

Solution: As in Problem 21, $\mathbf{Z}_4 \times \mathbf{Z}_{15} \cong \mathbf{Z}_4 \times \mathbf{Z}_3 \times \mathbf{Z}_5$, 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.

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

Solution: The subgroups correspond to the divisors of 100, and are given in Figure 3.0.1. Note that $n\mathbf{Z}_{100}$ is used to mean all multiples of n in \mathbf{Z}_{100} .

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

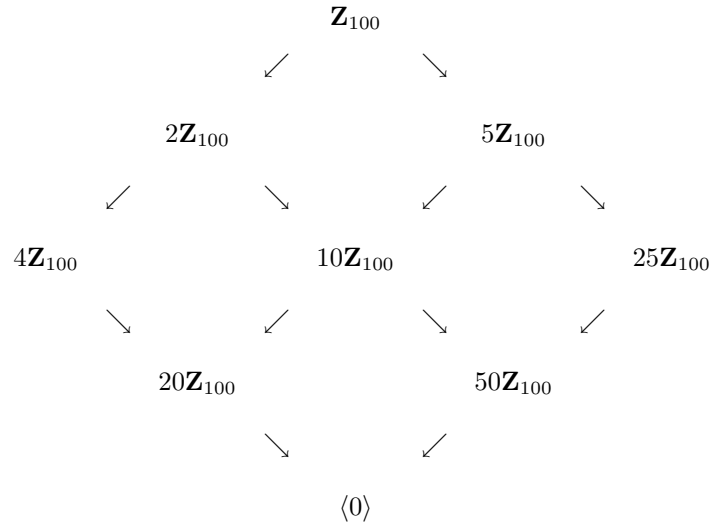
Solution: By Proposition 3.5.3 (b), the generators correspond to the numbers less than 28 and relatively prime to 28. The Euler φ -function allows us to compute how many there are: $\varphi(28) = \frac{1}{2} \cdot \frac{6}{7} \cdot 28 = 12$. The list of generators is $\{\pm 1, \pm 3, \pm 5, \pm 9, \pm 11, \pm 13\}$.

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

Solution: Using Proposition 3.5.3 (a), we first find $\gcd(18, 30) = 6$. Then $\langle [18]_{30} \rangle = \langle [6]_{30} \rangle$, and so the subgroup has $30/6 = 5$ elements.

Similarly, $\langle [24]_{30} \rangle = \langle [6]_{30} \rangle$, and so we actually have $\langle [24]_{30} \rangle = \langle [18]_{30} \rangle$.

Figure 3.1: for Problem 23



26. 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.

27. 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} .

28. Use the the result in Problem 27 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.

29. 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 Example 3.3.7 of the text (see page 108). 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 \mathcal{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.

30. 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 27 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 q 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, and thus $[a]_{pq}$ has order 2.

3.6 SOLUTIONS

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

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 $0 \leq i < n$.

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.

23. In the dihedral group $\mathcal{D}_n = \{a^i b^j \mid 0 \leq i < n, 0 \leq j < 2\}$ 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 the previous problem, we have $(a^i b)^2 = (a^i b)(a^i b) = a^i (b a^i) b = a^i (a^{n-i} b) b = (a^i a^{n-i})(b^2) = a^n e = e$.

24. In \mathcal{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 \mathcal{S}_3 .) Thus $H = \{(1), a, a^2, b, ab, a^2 b\} = \{(1), (1, 2, 3), (1, 3, 2), (1, 2), (1, 3), (2, 3)\}$.

25. For the subgroup H of \mathcal{S}_4 defined in the previous problem, find the corresponding subgroup $\sigma H \sigma^{-1}$, for $\sigma = (1, 4)$.

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 2.3.10, which shows 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 $(1, 4)H(1, 4)^{-1} = \{(1), (2, 3, 4), (2, 4, 3), (2, 3), (2, 4), (3, 4)\}$.

26. Show that each element in \mathcal{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 \mathcal{A}_4 .

27. In the dihedral group $\mathcal{D}_n = \{a^i b^j \mid 0 \leq i < n, 0 \leq j < 2\}$ 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, $C(a) \neq \mathcal{D}_n$, since by definition b does not belong to $C(a)$. Since $\langle a \rangle$ contains exactly half of the elements in \mathcal{D}_n , Lagrange's theorem show that there is no subgroup that lies strictly between $\langle a \rangle$ and \mathcal{D}_n , so $\langle a \rangle \subseteq C(a) \subseteq \mathcal{D}_n$ and $C(a) \neq \mathcal{D}_n$ together imply that $C(a) = \langle a \rangle$.

28. Find the centralizer of $(1, 2, 3)$ in \mathcal{S}_3 , in \mathcal{S}_4 , and in \mathcal{A}_4 .

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 \mathcal{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 \mathcal{S}_4 we have to work a bit harder.

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 that $axa^{-1} = x$. Exercise 2.3.10 provides a quick way to do this in a group of permutations. That exercise shows that if $(1, 2, \dots, k)$ is a cycle of length k and σ is any permutation, then $\sigma(1, 2, \dots, k)\sigma^{-1} = (\sigma(1), \sigma(2), \dots, \sigma(k))$.

Let $a = (1, 2, 3)$. From the computations in \mathcal{S}_3 , we know that $(1, 2)$, $(1, 3)$, and $(2, 3)$ do not commute with a . The remaining transpositions in \mathcal{S}_4 are $(1, 4)$, $(2, 4)$, and $(3, 4)$. Using Exercise 2.3.10, 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 \mathcal{S}_4 commutes with a . For the products of the transposition, 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 will 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 $(u, v, w, 4) \neq (x, y, z, 4)$. 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 that are not in $C(a)$, and therefore $C(a) = \langle a \rangle$. Finally, in \mathcal{A}_4 we must get the same answer: $C(a) = \langle a \rangle$.

3.7 SOLUTIONS

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

Solution: Example 3.7.5 shows that 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 $\phi : \mathbf{Z}_4 \rightarrow \mathbf{Z}_{10}$, the order of $\phi([1]_4)$ must be a divisor of 4 and of 10, so the only possibilities are 1 and 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 $[x]_4 \in \mathbf{Z}_4$.

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

Solution: Example 3.7.5 shows that 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 $[0]_{30}$, of order 1, $[15]_{30}$, of order 2, $[10]_{30}$ and $[20]_{30}$, of order 3, and $[5]_{30}$ and $[25]_{30}$, of order 6.

(b) Choose one of the nonzero formulas in part (a), and for this formula find the kernel and image, and show how elements of the image correspond to cosets of the kernel.

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 then cosets of the kernel are defined by adding 1, 2, 3, 4, and 5, respectively. We have the following correspondence

$$\begin{aligned} \{0, 6, 12\} &\longleftrightarrow \phi(0) = 0, & \{3, 9, 15\} &\longleftrightarrow \phi(3) = 15, \\ \{1, 7, 13\} &\longleftrightarrow \phi(1) = 5, & \{4, 10, 16\} &\longleftrightarrow \phi(4) = 20, \\ \{2, 8, 14\} &\longleftrightarrow \phi(2) = 10, & \{5, 11, 17\} &\longleftrightarrow \phi(5) = 25. \end{aligned}$$

19. (a) Show that \mathbf{Z}_7^\times is cyclic, with generator $[3]_7$.

Solution: Since $3^2 \equiv 2$ and $3^3 \equiv 6$, it follows that $[3]$ must have order 6.

- (b) Show that \mathbf{Z}_{17}^\times is cyclic, with generator $[3]_{17}$.

Solution: The element $[3]$ is a generator for \mathbf{Z}_{17}^\times , since $3^2 = 9$, $3^3 = 27 \equiv 10$, $3^4 \equiv 3 \cdot 10 \equiv 13$, $3^5 \equiv 3 \cdot 13 \equiv 5$, $3^6 \equiv 3 \cdot 5 \equiv 15$, $3^7 \equiv 3 \cdot 15 \equiv 11$, $3^8 \equiv 3 \cdot 11 \equiv 16 \neq 1$.

- (c) Completely determine all group homomorphisms from \mathbf{Z}_{17}^\times into \mathbf{Z}_7^\times .

Solution: Any group homomorphism $\phi: \mathbf{Z}_{17}^\times \rightarrow \mathbf{Z}_7^\times$ is determined by its value on the generator $[3]_{17}$, and the order of $\phi([3]_{17})$ must be a common divisor of 16 and 6. The only possible orders are 1 and 2, so either $\phi([3]_{17}) = [1]_7$ or $\phi([3]_{17}) = [-1]_7$. In the first case, $\phi([x]_{17}) = [1]_7$ for all $[x]_{17} \in \mathbf{Z}_{17}^\times$, and in the second case $\phi([3]_{17}^n) = [-1]_7^n$, for all $[x]_{17} = ([3]_{17})^n \in \mathbf{Z}_{17}^\times$.

20. Define $\phi: \mathbf{Z}_4 \times \mathbf{Z}_6 \rightarrow \mathbf{Z}_4 \times \mathbf{Z}_3$ by $\phi(x, y) = (x + 2y, y)$.

- (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 the fundamental homomorphism theorem.

Solution: If (x, y) 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 $(0, 0)$ and $(2, 3)$.

It follows that there are $24/2 = 12$ cosets of the kernel. These cosets 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 $(\mathbf{Z}_4 \times \mathbf{Z}_6)/\{(0, 0), (2, 3)\} \cong \mathbf{Z}_4 \times \mathbf{Z}_3$.

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

Solution: First, 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 $[a]_n, [b]_n \in \mathbf{Z}_n^\times$, $\phi([a]_n[b]_n) = \phi([ab]_n) = [ab]_m = [a]_m[b]_m = \phi([a]_n)\phi([b]_n)$.

22. For the group homomorphism $\phi : \mathbf{Z}_{36}^\times \rightarrow \mathbf{Z}_{12}^\times$ 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 the fundamental homomorphism theorem.

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 $\mathbf{Z}_{12}^\times \cong \mathbf{Z}_{36}^\times / \langle [13]_{36} \rangle$.

23. Let G, G_1 , and G_2 be groups. Let $\phi_1 : G \rightarrow G_1$ and $\phi_2 : G \rightarrow G_2$ be group homomorphisms. Prove that $\phi : G \rightarrow G_1 \times G_2$ defined by $\phi(x) = (\phi_1(x), \phi_2(x))$, for all $x \in G$, is a well-defined group homomorphism.

Solution: Given a, b in G , we have

$$\begin{aligned} \phi(ab) &= (\phi_1(ab), \phi_2(ab)) \\ &= (\phi_1(a)\phi_1(b), \phi_2(a)\phi_2(b)) \end{aligned}$$

$$\begin{aligned} \phi(a)\phi(b) &= (\phi_1(a), \phi_2(a)) \cdot (\phi_1(b), \phi_2(b)) \\ &= (\phi_1(a)\phi_1(b), \phi_2(a)\phi_2(b)) \end{aligned}$$

and so $\phi : G \rightarrow G_1 \times G_2$ is a group homomorphism.

24. Let p and q be different odd primes. Prove that \mathbf{Z}_{pq}^\times is isomorphic to the direct product $\mathbf{Z}_p^\times \times \mathbf{Z}_q^\times$.

Solution: Using Problem 21, we can define group homomorphisms $\phi_1 : \mathbf{Z}_{pq}^\times \rightarrow \mathbf{Z}_p^\times$ and $\phi_2 : \mathbf{Z}_{pq}^\times \rightarrow \mathbf{Z}_q^\times$ by setting $\phi_1([x]_{pq}) = [x]_p$, for all $[x]_{pq} \in \mathbf{Z}_{pq}^\times$, and $\phi_2([x]_{pq}) = [x]_q$, for all $[x]_{pq} \in \mathbf{Z}_{pq}^\times$.

Using Problem 23, we can define a group homomorphism $\phi : \mathbf{Z}_{pq}^\times \rightarrow \mathbf{Z}_p^\times \times \mathbf{Z}_q^\times$ by setting $\phi([x]_{pq}) = (\phi_1([x]_{pq}), \phi_2([x]_{pq}))$, for all $[x]_{pq} \in \mathbf{Z}_{pq}^\times$. If $[x]_{pq} \in \ker(\phi)$, then $[x]_p = [1]_p$ and $[x]_q = [1]_q$, so $p \mid (x - 1)$ and $q \mid (x - 1)$, and this implies that $pq \mid (x - 1)$, since p and q are relatively prime. It follows that $[x]_{pq} = [1]_{pq}$, and this shows that ϕ is a one-to-one function. Exercise 1.4.27 in the text states that if $m > 0$ and $n > 0$ are relatively prime integers, then $\varphi(mn) = \varphi(m)\varphi(n)$. It follows that \mathbf{Z}_{pq}^\times and $\mathbf{Z}_p^\times \times \mathbf{Z}_q^\times$ have the same order, so ϕ is also an onto function. This completes the proof that ϕ is a group isomorphism.

3.8 SOLUTIONS

27. 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.

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

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

Solution: The cosets of $H = \{(0, 0), (0, 2)\}$ are

$$(0, 0) + H = \{(0, 0), (0, 2)\} \quad (1, 0) + H = \{(1, 0), (1, 2)\}$$

$$(2, 0) + H = \{(2, 0), (2, 2)\} \quad (3, 0) + H = \{(3, 0), (3, 2)\}$$

$$(4, 0) + H = \{(4, 0), (4, 2)\} \quad (5, 0) + H = \{(5, 0), (5, 2)\}$$

$$(0, 1) + H = \{(0, 1), (0, 3)\} \quad (1, 1) + H = \{(1, 1), (1, 3)\}$$

$$(2, 1) + H = \{(2, 1), (2, 3)\} \quad (3, 1) + H = \{(3, 1), (3, 3)\}$$

$$(4, 1) + H = \{(4, 1), (4, 3)\} \quad (5, 1) + H = \{(5, 1), (5, 3)\}$$

The cosets of $K = \{(0, 0), (3, 0)\}$ are

$$(0, 0) + K = \{(0, 0), (3, 0)\} \quad (0, 1) + K = \{(0, 1), (3, 1)\}$$

$$(0, 2) + K = \{(0, 2), (3, 2)\} \quad (0, 3) + K = \{(0, 3), (3, 3)\}$$

$$(1, 0) + K = \{(1, 0), (4, 0)\} \quad (1, 1) + K = \{(1, 1), (4, 1)\}$$

$$(1, 2) + K = \{(1, 2), (4, 2)\} \quad (1, 3) + K = \{(1, 3), (4, 3)\}$$

$$(2, 0) + K = \{(2, 0), (5, 0)\} \quad (2, 1) + K = \{(2, 1), (5, 1)\}$$

$$(2, 2) + K = \{(2, 2), (5, 2)\} \quad (2, 3) + K = \{(2, 3), (5, 3)\}$$

(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, $(1, 1) + K$ has order 12 in G/K , and so $G/K \cong \mathbf{Z}_{12}$.

29. 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 $1 \leq i < n$.

Solution: The identity holds for all positive integers i , and can be proved inductively: assuming $ba^k = a^{-k}b$, we have $ba^{k+1} = ba^k a = a^{-k}ba = a^{-k}a^{-1}b = a^{-(k+1)}b$.

(b) Show that any element of the form $a^i b$ has order 2.

Solution: We have $(a^i b)^2 = a^i b a^i b = a^i a^{-i} b^2 = a^0 = e$.

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

Solution: The left cosets of $\langle b \rangle$ have the form $a^i \langle b \rangle = \{a^i, a^i b\}$, 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 $0 \leq i < n$.

30. Let $G = D_6$ 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: The argument is the same as in the previous problem.

(b) Is G/N abelian?

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.

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

(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 $a^i b (a^{3n}) a^i b = a^i a^{-3n} a^{-i} = (a^{3n})^{-1}$. (We are using the fact that $ba^i = a^{-i}b$.)

The cosets of N are

$$\begin{aligned} N &= \{e, a^3, a^6, a^9\}, & Nb &= \{ab, a^3b, a^6b, a^9b\}, \\ Na &= \{a, a^4, a^7, a^{10}\}, & Nab &= \{ab, a^4b, a^7b, a^{10}b\}, \\ Na^2 &= \{a^2, a^5, a^8, a^{11}\}, & Na^2b &= \{a^2b, a^5b, a^8b, a^{11}b\}. \end{aligned}$$

(b) You may assume that G/N is isomorphic to either \mathbf{Z}_6 or S_3 . Which is correct?

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 $G/N \cong S_3$.

32. (a) 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 $b = gag^{-1}$. Show that \sim is an equivalence relation on G . The equivalence classes of \sim are called the *conjugacy classes* of 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.

33. Find the conjugacy classes of D_4 .

Solution: Remember: the notion of a conjugacy class was just defined in the previous exercise. Let $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, with $a^4 = e$, $b^2 = e$, and $ba = a^{-1}b$. Since $xex^{-1} = e$, the only element conjugate to e is e itself.

If x is any power of a , then x commutes with a , and so $xax^{-1} = a$. If $x = a^i b$, then $xax^{-1} = a^i b a a^{-i} b = a^i a^{i-1} b^2 = a^{2i-1}$, so this shows that a^3 is the only conjugate of a (other than a itself).

The solution of an earlier problem shows that $xa^2x^{-1} = a^2$ in D_4 , so a^2 is not conjugate to any other element.

If $x = a^i$, then $xbx^{-1} = a^i b a^{-i} = a^i a^i b = a^{2i} b$. If $x = a^i b$, then $xbx^{-1} = (a^i b)b(a^i b)^{-1} = a^i a^i b = a^{2i} b$. Thus $a^2 b$ is the only conjugate of b .

If $x = a^i$, then $x(ab)x^{-1} = a^i a b a^{-i} = a^{i+1} a^i b = a^{2i+1} b$. If $x = a^i b$, then $xabx^{-1} = (a^i b)ab(a^i b)^{-1} = a^i a^{-1} a^i b = a^{2i-1} b$. Thus $a^3 b$ is the only conjugate of ab .

34. Let G be a group, and let N and H be subgroups of G such that N is normal in G .

(a) Prove that HN is a subgroup of G .

Solution: See Proposition 3.3.2. It is clear that $e = e \cdot e$ belongs to the set HN , so HN is nonempty. Suppose that x, y belong to HN . Then $x = h_1 n_1$ and $y = h_2 n_2$, for some $h_1, h_2 \in H$ and some $n_1, n_2 \in N$. We have

$$xy^{-1} = h_1 n_1 (h_2 n_2)^{-1} = h_1 n_1 n_2^{-1} h_2^{-1} = (h_1 h_2^{-1})(h_2 (n_1 n_2^{-1}) h_2^{-1}),$$

and this element belongs to HN since the assumption that N is normal guarantees that $h_2 (n_1 n_2^{-1}) h_2^{-1} \in N$.

(b) Prove that N is a normal subgroup of HN .

Solution: Since N is normal in G , it is normal in the subgroup HN , which contains it.

(c) Prove that if $H \cap N = \{e\}$, then HN/N is isomorphic to H .

Solution: Define $\phi : H \rightarrow HN/N$ 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 $h = e$.

SOLUTIONS TO THE REVIEW PROBLEMS

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. Find all subgroups of \mathbf{Z}_{11}^\times , and give the lattice diagram which shows 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.

3. Let G be the subgroup of $GL_3(\mathbf{R})$ consisting of all matrices of the form

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ such that } a, b \in \mathbf{R}.$$

Show that G is a subgroup of $GL_3(\mathbf{R})$.

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.

4. Show that the group G in the previous problem is isomorphic to the direct product $\mathbf{R} \times \mathbf{R}$.

Solution: Define $\phi : G \rightarrow \mathbf{R} \times \mathbf{R}$ 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 $\theta : \mathbf{R} \times \mathbf{R} \rightarrow G$ 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 $\phi\left(\begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & c & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) = \phi\left(\begin{bmatrix} 1 & a+c & b+d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) =$

$$(a+c, b+d) = (a, b) + (c, d) = \phi\left(\begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) + \phi\left(\begin{bmatrix} 1 & c & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right).$$

5. 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.

6. Let G be the subgroup of $GL_2(\mathbf{R})$ consisting of all matrices of the form $\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$, and let N be the subset of all matrices of the form $\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$.

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

Solution: The set N is nonempty since it contains the identity matrix, and

it is a subgroup since $\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -c \\ 0 & 1 \end{bmatrix} =$

$$\begin{bmatrix} 1 & b-c \\ 0 & 1 \end{bmatrix}. \text{ } N \text{ is normal in } G \text{ since } \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}^{-1} =$$

$$\begin{bmatrix} m & mc+b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1/m & -b/m \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & mc \\ 0 & 1 \end{bmatrix} \in N.$$

(b) Show that G/N is isomorphic to the multiplicative group \mathbf{R}^\times .

Solution: Define $\phi : G \rightarrow \mathbf{R}^\times$ by $\phi\left(\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}\right) = m$. Then we have

$$\phi\left(\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} n & c \\ 0 & 1 \end{bmatrix}\right) = \phi\left(\begin{bmatrix} mn & mc+b \\ 0 & 1 \end{bmatrix}\right) = mn =$$

$$\phi\left(\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}\right) \phi\left(\begin{bmatrix} n & c \\ 0 & 1 \end{bmatrix}\right). \text{ Since } m \text{ can be any nonzero real number, } \phi$$

maps G onto \mathbf{R}^\times , and $\phi\left(\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}\right) = 1$ if and only if $m = 1$, so $N = \ker(\phi)$.

The fundamental homomorphism theorem implies that $G/N \cong \mathbf{R}^\times$.

Note that this part of the proof covers part (a), since once you have determined the kernel, it is always a normal subgroup. Thus parts (a) and (b) can be proved at the same time, using the argument given for part (b).

7. 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 of D_4 .

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

$$N = \{e, a^2\}, \quad Na = \{a, a^3\}, \quad Nb = \{b, a^2b\}, \quad \text{and} \quad Nab = \{ab, a^3b\}.$$

Since b and ab have order 2, and $a^2 \in N$, we see that each element in the factor group has order 2, so G/N is not cyclic.

8. 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

$$\begin{aligned} N &= \{e, a^2, a^4, a^6\}, & Na &= \{a, a^3, a^5, a^7\}, \\ Nb &= \{b, a^2b, a^4b, a^6b\}, & Nab &= \{ab, a^3b, a^5b, a^7b\}. \end{aligned}$$

The left cosets of N are more trouble to compute, but we get

$$\begin{aligned} N &= \{e, a^2, a^4, a^6\}, & aN &= \{a, a^3, a^5, a^7\}, \\ bN &= \{b, a^6b, a^4b, a^2b\}, & abN &= \{ab, a^7b, a^5b, a^3b\}. \end{aligned}$$

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.

Chapter 4

Polynomials

SOLUTIONS TO THE 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 $x^6 - 1 = g(x)$. We have $f(x) = x^2g(x) + (x^2 - 1)$, and $g(x) = (x^4 + x^2 + 1)(x^2 - 1)$, so this shows that $\gcd(x^8 - 1, x^6 - 1) = x^2 - 1$, and $x^2 - 1 = f(x) - x^2g(x)$.

2. 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.

Solution: Let $2x^3 - 2x^2 - 3x + 1 = f(x)$ and $2x^2 - x - 2 = g(x)$. We first obtain $f(x) = (x - \frac{1}{2})g(x) - \frac{3}{2}x$. At the next step we can use x rather than $\frac{3}{2}x$, and then $g(x) = (2x - 1)g(x) - 2$. The constant remainder at the second step implies that $\gcd(f(x), g(x)) = 1$.

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

Solution: Let $x^4 + x^3 + 2x^2 + x + 1 = f(x)$ and $x^3 - 1 = g(x)$. 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 $\gcd(f(x), g(x)) = x^2 + x + 1$, and $(x^2 + x + 1) = \frac{1}{2}f(x) - \frac{1}{2}(x + 1)g(x)$.

4. 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 first obtain

$f(x) = (x+1)g(x) + (2x^2 - x - 1)$, and then $g(x) = (x-1)(2x^2 - x - 1) + (2x+1)$. At the next step we obtain $2x^2 - x - 1 = (x-1)(2x+1)$, so $2x+1$ 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 final answer, $x + \frac{1}{2} = \frac{1}{2}x^2g(x) + (-\frac{1}{2})(x-1)f(x)$.

5. 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 $p = 5$.

6. 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 $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$. We have $f(1) = 21$, so for any root we must have $(r-1)|21$, so this eliminates all but $\pm 2, 4, -6$ as possibilities. Then $f(2) = 32$, $f(-2) = -294$, and finally we obtain 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 $p = 3$.

7. 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} .

As an alternate solution, we could reduce $x^4 - 2x^2 + 8x + 1$ modulo 3 to get $p(x) = x^4 + x^2 + 2x + 1$. This polynomial has no roots in \mathbf{Z}_3 , so the only possible factors are of degree 2. The monic irreducible polynomials of degree 2 over \mathbf{Z}_3 are $x^2 + 1$, $x^2 + x + 2$, and $x^2 + 2x + 2$. Since the constant term of $p(x)$ is 1, the only possible factorizations are $p(x) = (x^2 + x + 2)^2$, $p(x) = (x^2 + 2x + 2)^2$, or $p(x) = (x^2 + x + 2)(x^2 + 2x + 2)$. In the first the coefficient of x is 1; the second has a nonzero cubic term; in the third the coefficient of x is 0. Thus $p(x)$ is irreducible over \mathbf{Z}_3 , and hence over \mathbf{Q} .

8. (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 .

9. (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: If $p(x) = x^3 + 2x^2 + 3$, then $p(0) = 3$, $p(1) = 1$, $p(-1) = -1$, $p(2) = 4$, and $p(-2) = 3$, so $p(x)$ is irreducible over \mathbf{Z}_5 .

10. 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 .

11. 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 $[x^3] = [5]$ and $[x^4] = [5x]$.

12. 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 thus $[x + 1]^{-1} = [-x^2 - x] = [x^2 + x]$.

We next give an alternate solution, which 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 $[x + 1]^{-1} = [x^2 + x]$.

13. 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

$$x^3 - 2 = (x^2 + x + 1)(x - 1) + (-1), \text{ and so } [x^2 + x + 1]^{-1} = [x - 1].$$

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

$$x^3 + 2x^2 + x + 1 = (x + 1)(x^2 + x + 1) + (-x) \text{ and}$$

$$x^2 + x + 1 = (-x - 1)(-x) + 1. \text{ Then a substitution gives us}$$

$$\begin{aligned} 1 &= (x^2 + x + 1) + (x + 1)(-x) \\ &= (x^2 + x + 1) + (x + 1)((x^3 + 2x^2 + x + 1) - (x + 1)(x^2 + x + 1)) \\ &= (-x^2 - 2x)(x^2 + x + 1) + (x + 1)(x^3 + x^2 + 2x + 1). \end{aligned}$$

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 $[x^4] = [x - 1]$.

This 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.

14. 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 $x^3 + x + 1 = x(x^2 + 1) + 1$, and so $[x][x^2 + 1] = [-1]$. Thus $[x]^{-1} = [-x^2 - 1]$.

Next, we have $x^3 + x + 1 = (x + 1)(x^2 - x + 2) - 1$, and so $[x + 1]^{-1} = [x^2 - x + 2]$.

Finally, we have

$$\begin{aligned} [x^2 + x]^{-1} &= [x]^{-1}[x + 1]^{-1} = [-x^2 - 1][x^2 - x + 2] \\ &= [-x^4 + x^3 - 2x^2 - x^2 + x - 2]. \end{aligned}$$

Using the identities $[x^3] = [-x - 1]$ and $[x^4] = [-x^2 - x]$, this reduces to

$$\begin{aligned} [x^2 + x]^{-1} &= [x^2 + x - x - 1 - 3x^2 + x - 2] \\ &= [-2x^2 + x - 3] = [3x^2 + x + 2]. \end{aligned}$$

15. Factor $x^4 + x + 1$ over $\mathbf{Z}_2[x]/\langle x^4 + x + 1 \rangle$.

Solution: There are 4 roots of $x^4 + x + 1$ in the given field, given by the cosets corresponding to x , x^2 , $x + 1$, $x^2 + 1$. This can be shown by using the multiplication table, with the elements in the form 10, 100, 11, and 101, or by computing with polynomials, using the fact that $(a + b)^2 = a^2 + b^2$ since $2ab = 0$. We have $x^4 + x + 1 \equiv 0$,

$$(x^2)^4 + (x^2) + 1 = (x^4)^2 + x^2 + 1 \equiv (x + 1)^2 + x^2 + 1 \equiv x^2 + 1 + x^2 + 1 \equiv 0,$$

$$(x + 1)^4 + (x + 1) + 1 \equiv x^4 + 1 + x \equiv x + 1 + 1 + x \equiv 0, \text{ and}$$

$$(x^2 + 1)^4 + (x^2 + 1) + 1 \equiv (x^4)^2 + 1 + x^2 \equiv (x + 1)^2 + 1 + x^2 \equiv x^2 + 1 + 1 + x^2 \equiv 0.$$

Thus $x^4 + x + 1$ factors as a product of 4 linear terms.

Chapter 5

Commutative Rings

SOLUTIONS TO THE 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 and commutativity of multiplication).

Solution: It is clear that the set is closed under addition, and the following computation checks closure under multiplication.

$$\begin{bmatrix} a & 0 & 0 \\ 0 & a & 0 \\ b & c & a \end{bmatrix} \begin{bmatrix} x & 0 & 0 \\ 0 & x & 0 \\ y & z & x \end{bmatrix} = \begin{bmatrix} ax & 0 & 0 \\ 0 & ax & 0 \\ bx + ay & cx + az & ax \end{bmatrix}$$

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 isomorphic to either of the rings \mathbf{Z}_4 or $\mathbf{Z}_2 \oplus \mathbf{Z}_2$.

Solution: In R we have $a + a = 0$, for all $a \in R$, 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. Find all ring homomorphisms from \mathbf{Z}_{120} into \mathbf{Z}_{42} .

Solution: Let $\phi : \mathbf{Z}_{120} \rightarrow \mathbf{Z}_{42}$ be a ring homomorphism. 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 idempotent, and 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 $3\mathbf{Z}_{120}$.

4. Are \mathbf{Z}_9 and $\mathbf{Z}_3 \oplus \mathbf{Z}_3$ isomorphic as rings?

Solution: The answer is no. The argument can be given using either addition or multiplication. Addition in the two rings is different, since the additive group of \mathbf{Z}_9 is cyclic, while that of $\mathbf{Z}_3 \oplus \mathbf{Z}_3$ is not. Multiplication is also different, since in \mathbf{Z}_9 there is a nonzero solution to the equation $x^2 = 0$, while in $\mathbf{Z}_3 \oplus \mathbf{Z}_3$ there is not. (In \mathbf{Z}_9 let $x = 3$, while in $\mathbf{Z}_3 \oplus \mathbf{Z}_3$ the equation $(a, b)^2 = (0, 0)$ implies $a^2 = 0$ and $b^2 = 0$, and then $a = 0$ and $b = 0$.)

5. In the group \mathbf{Z}_{180}^\times of units of the ring \mathbf{Z}_{180} , what is the largest possible order of an element?

Solution: Since $180 = 2^2 3^2 5$, it follows from Theorem 3.5.4 that the ring \mathbf{Z}_{180} is isomorphic to the ring $\mathbf{Z}_4 \oplus \mathbf{Z}_9 \oplus \mathbf{Z}_5$. Then Example 5.2.10 shows that

$$\mathbf{Z}_{180}^\times \cong \mathbf{Z}_4^\times \times \mathbf{Z}_9^\times \times \mathbf{Z}_5^\times \cong \mathbf{Z}_2 \times \mathbf{Z}_6 \times \mathbf{Z}_4.$$

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 $\text{lcm}[2, 6, 4] = 12$.

6. For the element $a = (0, 2)$ of the ring $R = \mathbf{Z}_{12} \oplus \mathbf{Z}_8$, find $\text{Ann}(a) = \{r \in R \mid ra = 0\}$. Show 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 .

7. 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: Define $\phi : \mathbf{Z}_2[x]/\langle x^4 + 1 \rangle \rightarrow \mathbf{Z}_2[x]/\langle x^2 + 1 \rangle$ 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.

8. 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 $3\mathbf{Z}_{36}$.

An alternate approach 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 $3\mathbf{Z}_{36}$.

9. Give an example to show that the set of all zero divisors of a 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.

10. 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 $\phi : \mathbf{Z}[x] \rightarrow \mathbf{Z}_2[x]$ 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 not a field, so I is not maximal.

11. Let R be any 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 $\phi : R \rightarrow Re \oplus R(1-e)$ 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 $\phi(r)\phi(s) = (re, r(1-e))(se, s(1-e)) = (rse^2, rs(1-e)^2) = (rse, rs(1-e))$.

12. Let R be the ring $\mathbf{Z}_2[x]/\langle x^3 + 1 \rangle$.

Solution: Note: Table 5.1 gives the multiplication table. It is not necessary

Table 5.1: Multiplication in $\mathbf{Z}_2[x]/\langle x^3 + 1 \rangle$

| \times | 1 | x | x^2 | $x^2 + x + 1$ | $x^2 + x$ | $x + 1$ | $x^2 + 1$ |
|---------------|---------------|---------------|---------------|---------------|-----------|-----------|-----------|
| 1 | 1 | x | x^2 | $x^2 + x + 1$ | $x^2 + x$ | $x + 1$ | $x^2 + 1$ |
| x | x | x^2 | 1 | $x^2 + x + 1$ | $x^2 + 1$ | $x^2 + x$ | $x + 1$ |
| x^2 | x^2 | 1 | x | $x^2 + x + 1$ | $x + 1$ | $x^2 + 1$ | $x^2 + x$ |
| $x^2 + x + 1$ | $x^2 + x + 1$ | $x^2 + x + 1$ | $x^2 + x + 1$ | $x^2 + x + 1$ | 0 | 0 | 0 |
| $x^2 + x$ | $x^2 + x$ | $x^2 + 1$ | $x + 1$ | 0 | $x^2 + x$ | $x + 1$ | $x^2 + 1$ |
| $x + 1$ | $x + 1$ | $x^2 + x$ | $x^2 + 1$ | 0 | $x + 1$ | $x^2 + 1$ | $x^2 + x$ |
| $x^2 + 1$ | $x^2 + 1$ | $x + 1$ | $x^2 + x$ | 0 | $x^2 + 1$ | $x^2 + x$ | $x + 1$ |

to compute the multiplication table in order to solve the problem.

(a) Find all ideals of R .

Solution: By Proposition 5.3.7, 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 generated by $[x + 1]$ and $[x^2 + x + 1]$.

(b) Find the units of R .

Solution: We have $[x]^3 = [1]$, so $[x]$ and $[x^2]$ are units. On the other hand, $[x + 1][x^2 + x + 1] = [x^3 + 1] = [0]$, so $[x + 1]$ and $[x^2 + x + 1]$ cannot be units. This also excludes $[x^2 + x] = [x][x + 1]$ and $[x^2 + 1] = [x^2][1 + x]$. Thus the only units are 1, $[x]$, and $[x^2]$.

(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 $[x^2 + x]$.

13. Let S be the ring $\mathbf{Z}_2[x]/\langle x^3 + x \rangle$.

Solution: Note: Table 5.2 gives the multiplication table. It is not necessary

Table 5.2: Multiplication in $\mathbf{Z}_2[x]/\langle x^3 + x \rangle$

| \times | 1 | $x^2 + x + 1$ | x^2 | x | $x^2 + x$ | $x + 1$ | $x^2 + 1$ |
|---------------|---------------|---------------|-----------|-----------|-----------|-----------|-----------|
| 1 | 1 | $x^2 + x + 1$ | x^2 | x | $x^2 + x$ | $x + 1$ | $x^2 + 1$ |
| $x^2 + x + 1$ | $x^2 + x + 1$ | 1 | x^2 | x | $x^2 + x$ | $x + 1$ | $x^2 + 1$ |
| x^2 | x^2 | x^2 | x^2 | x | $x^2 + x$ | $x^2 + x$ | 0 |
| x | x | x | x | x^2 | $x^2 + x$ | $x^2 + x$ | 0 |
| $x^2 + x$ | $x^2 + x$ | $x^2 + x$ | $x^2 + x$ | $x^2 + x$ | 0 | 0 | 0 |
| $x + 1$ | $x + 1$ | $x + 1$ | $x^2 + x$ | $x^2 + x$ | 0 | $x^2 + 1$ | $x^2 + 1$ |
| $x^2 + 1$ | $x^2 + 1$ | $x^2 + 1$ | 0 | 0 | 0 | $x^2 + 1$ | $x^2 + 1$ |

to compute the multiplication table in order to solve the problem.

- (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 the proper nonzero ideals of S are the principal ideals generated by $[x]$, $[x + 1]$, $[x^2 + 1] = [x + 1]^2$, and $[x^2 + x] = [x][x + 1]$.

$$\langle [x^2 + x] \rangle = \{[0], [x^2 + x]\} \quad \langle [x^2 + 1] \rangle = \{[0], [x^2 + 1]\}$$

$$\langle [x] \rangle = \{[0], [x], [x^2], [x^2 + x]\} \quad \langle [x + 1] \rangle = \{[0], [x + 1], [x^2 + 1], [x^2 + x]\}$$

- (b) Find the units of R .

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 R .

Solution: Since $[x^3] = [1]$, 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.

14. Show that the rings R and S in the two previous problems are isomorphic as abelian groups, but not as rings.

Solution: Both R and S are isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$, as abelian groups. They cannot be isomorphic as rings since R has 3 units, while S has only 2.

15. Let $\mathbf{Z}[i]$ be the subring of the field of complex numbers given by

$$\mathbf{Z}[i] = \{m + ni \in \mathbf{C} \mid m, n \in \mathbf{Z}\}.$$

(a) Define $\phi : \mathbf{Z}[i] \rightarrow \mathbf{Z}_2$ 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: 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 $1 + i$.

(b) For any prime number p , define $\theta : \mathbf{Z}[i] \rightarrow \mathbf{Z}_p[x]/\langle x^2 + 1 \rangle$ 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 $\mathbf{Z}_p[x]/\langle x^2 + 1 \rangle$.

$$\begin{aligned}\theta((a + bi) + (c + di)) &= \theta((a + c) + (b + d)i) = [(a + c) + (b + d)x] \\ \theta((a + bi)) + \theta((c + di)) &= [a + bx] + [c + dx] = [(a + c) + (b + d)x]\end{aligned}$$

$$\begin{aligned}\theta((a + bi)(c + di)) &= \theta((ac - bd) + (ad + bc)i) = [(ac - bd) + (ad + bc)x] \\ \theta((a + bi))\theta((c + di)) &= [a + bx][c + dx] = [ac + (ad + bc)x + bdx^2].\end{aligned}$$

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.

16. Let I and J be ideals in the commutative ring R , and define the function $\phi : R \rightarrow R/I \oplus R/J$ by $\phi(r) = (r + I, r + J)$, for all $r \in R$.

(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 $a - r = a - bx - ay = ax - bx \in I$, 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.

17. Considering $\mathbf{Z}[x]$ to be a subring of $\mathbf{Q}[x]$, show that these two integral domains have the same quotient field.

Solution: An element of the quotient field of $\mathbf{Q}[x]$ has the form $\frac{f(x)}{g(x)}$, for polynomials $f(x)$ and $g(x)$ with rational coefficients. If m is the lcm of the denominators of the coefficients of $f(x)$ and n is the lcm of the denominators of the coefficients of $g(x)$, then we have $\frac{f(x)}{g(x)} = \frac{n}{m} \frac{h(x)}{k(x)}$ for $h(x), k(x) \in \mathbf{Z}[x]$, and this shows that $\frac{f(x)}{g(x)}$ belongs to the quotient field of $\mathbf{Z}[x]$.

18. 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: Show that a root of $x^2 = -1$ leads to an element of order 4 in the multiplicative group \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.

Chapter 6

Fields

SOLUTIONS TO THE REVIEW PROBLEMS

1. 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 $(7 - 2u + u^2)^{-1} = (2 + u)/11 = (2/11) + (1/11)u$.

2. (a) Show that $\mathbf{Q}(\sqrt{2} + i) = \mathbf{Q}(\sqrt{2}, i)$.

Solution: Let $u = \sqrt{2} + i$. Since $(\sqrt{2} + i)(\sqrt{2} - i) = 2 - i^2 = 3$, we have $\sqrt{2} - i = 3(\sqrt{2} + i)^{-1} \in \mathbf{Q}(u)$, 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 $\sqrt{2} + i$ 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 $x^4 - 2x^2 + 9$.

3. Find the minimal polynomial of $1 + \sqrt[3]{2}$ 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.

4. Show that $x^3 + 6x^2 - 12x + 2$ is irreducible over \mathbf{Q} , and remains irreducible over $\mathbf{Q}(\sqrt[5]{2})$.

Solution: Eisenstein's criterion works with $p = 2$. Since $x^5 - 2$ is also irreducible by Eisenstein's criterion, $[\mathbf{Q}(\sqrt[5]{2}) : \mathbf{Q}] = 5$. If $x^3 + 6x^2 - 12x + 2$ could be factored over $\mathbf{Q}(\sqrt[5]{2})$, then it would have a linear factor, and so it would have a root in $\mathbf{Q}(\sqrt[5]{2})$. This root would have degree 3 over \mathbf{Q} , and that is impossible since 3 is not a divisor of 5.

5. 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 in 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 $\{1, \sqrt{5}, \sqrt[3]{5}, \sqrt{5}\sqrt[3]{5}, \sqrt[3]{25}, \sqrt{5}\sqrt[3]{25}\}$.

6. 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

$$\begin{aligned} a(\sqrt{2} + \sqrt[3]{5})^3 + b(\sqrt{2} + \sqrt[3]{5})^2 + c(\sqrt{2} + \sqrt[3]{5}) + d &= \\ a(2\sqrt{2} + 6\sqrt[3]{5} + 3\sqrt{2}\sqrt[3]{25} + 5) + b(2 + 2\sqrt{2}\sqrt[3]{5} + \sqrt[3]{25}) + c(\sqrt{2} + \sqrt[3]{5}) + d &= \\ (5a + 2b + d) \cdot 1 + (6a + c)\sqrt[3]{5} + b\sqrt[3]{25} + (2a + c)\sqrt{2} + 2b\sqrt{2}\sqrt[3]{5} + 3a\sqrt{2}\sqrt[3]{25} &= 0. \end{aligned}$$

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 $[\mathbf{Q}(\sqrt{2} + \sqrt[3]{5}) : \mathbf{Q}] = 6$.

7. 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 $[\mathbf{Q}(\sqrt[7]{2}) : \mathbf{Q}]$.

8. 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 $\alpha = \sqrt[3]{2} + i$, so that $\alpha - i = \sqrt[3]{2}$. Then $(\alpha - i)^3 = 2$, so we have $\alpha^3 - 3i\alpha^2 + 3i^2\alpha - i^3 = 2$, or $\alpha^3 - 3i\alpha^2 - 3\alpha + i = 2$. Solving for i we get $i = (\alpha^3 - 3\alpha - 2)/(3\alpha^2 - 1)$, 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.

BIBLIOGRAPHY

- Allenby, R. B. J. T., *Rings, Fields, and Groups: An Introduction to Abstract Algebra*
London: Edward Arnold, 1983.
- Artin, M., *Algebra*, Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1991
- Birkhoff, G., and S. Mac Lane, *A Survey of Modern Algebra* (4th ed.). New York:
Macmillan Publishing Co., Inc., 1977.
- Fraleigh, J., *A First Course in Abstract Algebra* (6th ed.). Reading, Mass.: Addison-
Wesley Publishing Co., 1999.
- Gallian, J., *Contemporary Abstract Algebra* (4th ed.). Boston: Houghton Mifflin
Co., 1998
- Herstein, I. N., *Abstract Algebra*. (3rd ed.). New York: John Wiley & Sons, Inc.,
1996.
- , *Topics in Algebra* (2nd 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.

Index

- abelian group, 13
- algorithm, division, 1
- algorithm, Euclidean, 35
- alternating group, 22, 77
- annihilator, 30, 94
- associative law, 13, 15, 59, 62

- basis, for an extension field, 33, 102
- binary operation, 13

- cancellation law, 14
- Cayley's theorem, 21
- centralizer, 17, 18, 22, 65, 67, 68, 77
- Chinese remainder theorem, 76
- closure, 15, 57, 62, 64, 65
- combination, linear, 2
- complex numbers, 30, 97
- composite function, 7
- congruence, linear, 5
- congruence, 3–5, 41
- conjugacy class, 25, 82, 83
- coset, 24–26, 81, 82, 86
- criterion, of Eisenstein, 101, 102
- cross product, 14, 57
- cycle, 54
- cyclic, 1, 5, 6, 20, 21, 26, 45, 69, 76, 84, 86
- cyclic group, 17, 23, 24, 65, 81
- cyclic subgroup, 16, 63

- determinant, 8, 51, 65
- digit, units, 5, 43
- dihedral group, 22, 24–26, 77, 78, 82, 83, 86
- direct product, 17
- disjoint cycles, 10, 53, 54
- division algorithm, 1
- division, 14
- dot product, 9, 14, 52, 57

- eigenvalue, 8, 51
- Eisenstein's criterion, 88, 101, 102
- element, idempotent, 5, 6, 29, 30, 44, 45, 93, 94, 96, 97
- element, nilpotent, 6, 29, 44–46, 56, 93, 94
- equivalence relation, 8, 9, 51–53
- Euclidean algorithm, for polynomials, 27, 87, 90
- Euclidean algorithm, matrix form, 36, 46
- Euclidean algorithm, 3, 35, 39, 41, 44, 46
- Euler phi-function, 74
- even permutation, 53

- factor group, 24, 26, 81, 82, 86
- field, 27, 30, 31, 94, 95, 97, 99
- field, finite, 28, 89–91
- field, of quotients, 31, 99
- field, of rational numbers, 27, 28, 87–89
- finite field, 28, 89–91
- finite group, 13
- fractional linear transformation, 15, 60
- function, composite, 7
- function, inverse, 7, 8, 50
- function, one-to-one, 7
- function, onto, 7
- fundamental homomorphism theorem, for groups, 22–24, 80
- fundamental homomorphism theorem, for rings, 30, 95, 99

- Gaussian integers, 30, 98
- gcd, of integers 2, 3, 6, 35, 36, 40, 46
- gcd, of polynomials, 27, 87, 88
- general linear group, 14–18, 20, 26, 64–68, 72, 73, 84, 85
- generator, 21, 65, 69, 74
- group, 1, 13
- group, abelian, 13
- group, alternating, 22, 77
- group, cyclic, 23

- group, dihedral, 22, 24–26, 76, 77, 81, 82, 83, 86
- group, finite, 13
- group, of permutations, 10, 11, 54
- group, symmetric, 21
- group homomorphism, 18, 22, 23, 78–80
- group isomorphism, 23

- homomorphism, of groups, 22, 23, 78–80
- homomorphism, of rings, 29, 31, 94, 95, 98
- horizontal line test, 8, 49

- ideal, 30, 31, 97–99, 101
- ideal, maximal, 30, 95
- ideal, prime, 30, 95
- ideal, principal, 31, 95–98
- idempotent element, 5, 6, 29, 30, 44, 45, 93, 94, 96, 97
- idempotent element, modulo n , 5
- identity element, 13, 15, 57, 58, 60, 62, 65
- image, of a ring homomorphism, 94
- image, 23, 80
- induction, 2, 38, 59
- integers mod n , 5, 14
- inverse element, 7, 8, 15, 50, 60, 62, 64
- inverse, multiplicative, 5, 6, 28, 41, 44, 45, 47, 90
- invertible matrix, 9, 53
- irreducible polynomial, 28, 33, 88, 89, 101, 102
- isomorphic rings, 29, 30, 94, 95, 97, 99
- isomorphism, of groups, 19, 20, 22, 69–73
- isomorphism, of rings, 29, 30, 94, 95, 97, 99

- kernel, of a group homomorphism, 23, 80
- kernel, of a ring homomorphism, 94, 95

- Lagrange's theorem, 16, 77, 99
- lattice diagram, of subgroups, 21, 26, 74, 84
- lattice diagram, 3, 39
- linear combination, 2, 35
- linear congruence, 5
- linear transformation, fractional, 15, 60
- linear transformation, 8, 50, 51
- linearly independent vectors, 51

- matrix, invertible, 9, 53
- matrix, 8, 14, 50, 51
- maximal ideal, 30, 95
- minimal polynomial, 33, 101
- multiplicative inverse, 5, 6, 28, 41, 44, 45, 60, 90
- multiplicative order, modulo n , 5
- multiplicative order, 6, 47

- nilpotent element, 6, 29, 44–46, 56, 93, 94
- nilpotent element, modulo n , 5
- nilpotent element, of a ring, 29, 93
- normal subgroup, 25, 26, 82, 86
- nullity, 50

- one-to-one function, 7, 8, 51
- onto function, 7, 8, 51
- order, 16–18, 21, 66, 74
- order, multiplicative, 5, 6, 47
- order, of a permutation, 10, 11, 54

- parallel plane, 53
- partition, 9
- permutation, 10
- permutation, even, 53
- permutation group, 10, 11, 54
- perpendicular plane, 53
- plane, parallel, 53
- plane, perpendicular, 53
- polynomial, irreducible, 33, 101–103
- polynomial, minimal, 33, 101
- prime ideal, 30, 95
- prime, relatively, 2
- principal ideal, 31, 95–98

- quaternion group, 21, 75
- quotient field, 31, 99

- rank, of a matrix, 50
- rank nullity theorem, 50, 51
- rational roots, 88
- reflexive law, 52
- relatively prime polynomials, 27, 87
- relatively prime, 2
- ring homomorphism, 29, 31, 94, 95, 98
- root, of a polynomial, 33, 101, 102
- root, rational, 88

- subgroup, normal, 25, 26, 82, 86
- subgroup, 15, 17, 65, 66
- subring, 30, 31, 97, 99
- subspace, 15
- symmetric group, 14, 16, 21, 22, 63, 77
- symmetric law, 52
- system of congruences, 4, 6, 42, 47

- theorem, of Lagrange, 99
- transformation, linear, 8, 50
- transitive law, 52

- unit, of a ring, 29, 30, 93, 94, 96, 97
- units, mod 7; 23, 79
- units, mod 9; 14, 21, 58, 74
- units, mod 13; 26, 84
- units, mod 15; 15, 21, 58, 75
- units, mod 17; 19, 23, 69, 79
- units, mod 18; 21, 74
- units, mod 20; 16, 26, 63, 85
- units, mod 21; 16, 21, 63, 75
- units, mod 24; 16, 62
- units, mod 36; 17, 66
- units, mod n , 5, 6, 14, 45
- units, mod p , 16, 23, 64, 80
- units digit, 5, 43

- vector space, 15, 17
- vertical line test, 8, 49

- well-defined function, 24