

A BOOK OF ABSTRACT ALGEBRA

Second Edition

Charles C. Pinter
Professor of Mathematics
Bucknell University

Dover Publications, Inc., Mineola, New York

Copyright © 1982, 1990 by Charles C. Pinter
All rights reserved.

Bibliographical Note

This Dover edition, first published in 2010, is an unabridged republication of the 1990 second edition of the work originally published in 1982 by the McGraw-Hill Publishing Company, Inc., New York.

Library of Congress Cataloging-in-Publication Data

Pinter, Charles C, 1932–

A book of abstract algebra / Charles C. Pinter. — Dover ed.

p. cm.

Originally published: 2nd ed. New York : McGraw-Hill, 1990.

Includes bibliographical references and index.

ISBN-13: 978-0-486-47417-5

ISBN-10: 0-486-47417-8

1. Algebra, Abstract. I. Title.

QA162.P56 2010

512'.02—dc22

2009026228

Manufactured in the United States by Courier Corporation
47417803

www.doverpublications.com

Preface

Chapter 1 Why Abstract Algebra?

History of Algebra. New Algebras. Algebraic Structures. Axioms and Axiomatic Algebra. Abstraction in Algebra.

Chapter 2 Operations

Operations on a Set. Properties of Operations.

Chapter 3 The Definition of Groups

Groups. Examples of Infinite and Finite Groups. Examples of Abelian and Nonabelian Groups. Group Tables.

Theory of Coding: Maximum-Likelihood Decoding.

Chapter 4 Elementary Properties of Groups

Uniqueness of Identity and Inverses. Properties of Inverses.

Direct Product of Groups.

Chapter 5 Subgroups

Definition of Subgroup. Generators and Defining Relations.

Cayley Diagrams. Center of a Group. Group Codes; Hamming Code.

Chapter 6 Functions

Injective, Surjective, Bijective Function. Composite and Inverse of Functions.

Finite-State Machines. Automata and Their Semigroups.

Chapter 7 Groups of Permutations

Symmetric Groups. Dihedral Groups.

An Application of Groups to Anthropology.

Chapter 8 Permutations of a Finite Set

Decomposition of Permutations into Cycles. Transpositions. Even and Odd Permutations. Alternating Groups.

Chapter 9 Isomorphism

The Concept of Isomorphism in Mathematics. Isomorphic and Nonisomorphic Groups. Cayley's Theorem.

Chapter 10 Order of Group Elements

Powers/Multiples of Group Elements. Laws of Exponents. Properties of the Order of Group Elements.

Chapter 11 Cyclic Groups

Finite and Infinite Cyclic Groups. Isomorphism of Cyclic Groups. Subgroups of Cyclic Groups.

Chapter 12 Partitions and Equivalence Relations

Chapter 13 Counting Cosets

Lagrange's Theorem and Elementary Consequences.

Survey of Groups of Order ≤ 10 .

Number of Conjugate Elements. Group Acting on a Set.

Chapter 14 Homomorphisms

Elementary Properties of Homomorphisms. Normal Subgroups. Kernel and Range.

Inner Direct Products. Conjugate Subgroups.

Chapter 15 Quotient Groups

Quotient Group Construction. Examples and Applications.

The Class Equation. Induction on the Order of a Group.

Chapter 16 The Fundamental Homomorphism Theorem

Fundamental Homomorphism Theorem and Some Consequences.

The Isomorphism Theorems. The Correspondence Theorem. Cauchy's Theorem. Sylow Subgroups. Sylow's Theorem. Decomposition Theorem for Finite Abelian Groups.

Chapter 17 Rings: Definitions and Elementary Properties

Commutative Rings. Unity. Invertibles and Zero-Divisors. Integral Domain. Field.

Chapter 18 Ideals and Homomorphisms

Chapter 19 Quotient Rings

Construction of Quotient Rings. Examples. Fundamental Homomorphism Theorem and Some Consequences. Properties of Prime and Maximal Ideals.

Chapter 20 Integral Domains

Characteristic of an Integral Domain. Properties of the Characteristic. Finite Fields. Construction of the Field of Quotients.

Chapter 21 The Integers

Ordered Integral Domains. Well-ordering. Characterization of $\mathbf{Z}$ Up to Isomorphism. Mathematical Induction. Division Algorithm.

Chapter 22 Factoring into Primes

Ideals of $\mathbb{Z}$. Properties of the GCD. Relatively Prime Integers. Primes. Euclid's Lemma. Unique Factorization.

Chapter 23 Elements of Number Theory (Optional)

Properties of Congruence. Theorems of Fermat and Euler. Solutions of Linear Congruences. Chinese Remainder Theorem.

Wilson's Theorem and Consequences. Quadratic Residues. The Legendre Symbol. Primitive Roots.

Chapter 24 Rings of Polynomials

Motivation and Definitions. Domain of Polynomials over a Field. Division Algorithm.

Polynomials in Several Variables. Fields of Polynomial Quotients.

Chapter 25 Factoring Polynomials

Ideals of $F[x]$. Properties of the GCD. Irreducible Polynomials. Unique factorization.

Euclidean Algorithm.

Chapter 26 Substitution in Polynomials

Roots and Factors. Polynomial Functions. Polynomials over $\mathbb{Q}$. Eisenstein's Irreducibility Criterion. Polynomials over the Reals. Polynomial Interpolation.

Chapter 27 Extensions of Fields

Algebraic and Transcendental Elements. The Minimum Polynomial. Basic Theorem on Field Extensions.

Chapter 28 Vector Spaces

Elementary Properties of Vector Spaces. Linear Independence. Basis. Dimension. Linear Transformations.

Chapter 29 Degrees of Field Extensions

Simple and Iterated Extensions. Degree of an Iterated Extension.

Fields of Algebraic Elements. Algebraic Numbers. Algebraic Closure.

Chapter 30 Ruler and Compass

Constructible Points and Numbers. Impossible Constructions.

Constructible Angles and Polygons.

Chapter 31 Galois Theory: Preamble

Multiple Roots. Root Field. Extension of a Field. Isomorphism.

Roots of Unity. Separable Polynomials. Normal Extensions.

Chapter 32 Galois Theory: The Heart of the Matter

Field Automorphisms. The Galois Group. The Galois Correspondence. Fundamental Theorem of Galois Theory.

Computing Galois Groups.

Chapter 33 Solving Equations by Radicals

Radical Extensions. Abelian Extensions. Solvable Groups. Insolubility of the Quintic.

Appendix A	Review of Set Theory
Appendix B	Review of the Integers
Appendix C	Review of Mathematical Induction
	Answers to Selected Exercises
	Index

* Italic headings indicate topics discussed in the exercise sections.

RINGS: DEFINITIONS AND ELEMENTARY PROPERTIES

In presenting scientific knowledge it is elegant as well as enlightening to begin with the simple and move toward the more complex. If we build upon a knowledge of the simplest things, it is easier to understand the more complex ones. In the first part of this book we dedicated ourselves to the study of groups—surely one of the simplest and most fundamental of all algebraic systems. We will now move on, and, using the knowledge and insights gained in the study of groups, we will begin to examine algebraic systems which have *two* operations instead of just one.

The most basic of the two-operational systems is called a *ring*: it will be defined in a moment. The surprising fact about rings is that, despite their having *two* operations and being more complex than groups, their fundamental properties follow exactly the pattern already laid out for groups. With remarkable, almost compelling ease, we will find two-operational analogs of the notions of subgroup and quotient group, homomorphism and isomorphism—as well as other algebraic notions—and we will discover that rings behave just like groups with respect to these notions.

The two operations of a ring are traditionally called *addition* and *multiplication*, and are denoted as usual by $+$ and $\cdot$, respectively. We must remember, however, that the elements of a ring are not necessarily numbers (for example, there are rings of functions, rings of switching circuits, and so on); and therefore “addition” does not necessarily refer to the conventional addition of numbers, nor does multiplication necessarily refer to the conventional operation of multiplying numbers. In fact, $+$ and $\cdot$ are nothing more than symbols denoting the two operations of a ring.

By a ring we mean a set A with operations called addition and multiplication which satisfy the following axioms:

- (i) *A with addition alone is an abelian group.*
- (ii) *Multiplication is associative.*
- (iii) *Multiplication is distributive over addition. That is, for all a, b , and c in A ,*

$$a(b + c) = ab + ac$$

and

$$(b + c)a = ba + ca$$

Since A with addition alone is an abelian group, there is in A a neutral element for addition: it is called the *zero* element and is written 0 . Also, every element has an additive inverse called its *negative*; the

negative of a is denoted by $-a$. Subtraction is defined by

$$a - b = a + (-b)$$

The easiest examples of rings are the traditional number systems. The set $\mathbf{Z}$ of the integers, with conventional addition and multiplication, is a ring called the *ring of the integers*. We designate this ring simply with the letter $\mathbf{Z}$. (The context will make it clear whether we are referring to the *ring* of the integers or the additive *group* of the integers.)

Similarly, $\mathbf{Q}$ is the ring of the rational numbers, $\mathbf{R}$ the ring of the real numbers, and $\mathbf{C}$ the ring of the complex numbers. In each case, the operations are conventional addition and multiplication.

Remember that $\mathcal{F}(\mathbf{R})$ represents the set of all the functions from $\mathbf{R}$ to $\mathbf{R}$; that is, the set of all real-valued functions of a real variable. In calculus we learned to add and multiply functions: if f and g are any two functions from $\mathbf{R}$ to $\mathbf{R}$, their sum $f + g$ and their *product* fg are defined as follows:

$$[f + g](x) = f(x) + g(x) \quad \text{for every real number } x$$

and

$$[fg](x) = f(x)g(x) \quad \text{for every real number } x$$

$\mathcal{F}(\mathbf{R})$ with these operations for adding and multiplying functions is a ring called the *ring of real functions*. It is written simply as $\mathcal{F}(\mathbf{R})$. On page 46 we saw that $\mathcal{F}(\mathbf{R})$ with only addition of functions is an abelian group. It is left as an exercise for you to verify that multiplication of functions is associative and distributive over addition of functions.

The rings $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, and $\mathcal{F}(\mathbf{R})$ are all *infinite rings*, that is, rings with infinitely many elements. There are also *finite rings*: rings with a finite number of elements. As an important example, consider the group $\mathbf{Z}_n$, and define an operation of multiplication on $\mathbf{Z}_n$ by allowing the product ab to be the remainder of the usual product of integers a and b after division by n . (For example, in $\mathbf{Z}_5$, $2 \cdot 4 = 3$, $3 \cdot 3 = 4$, and $4 \cdot 3 = 2$.) This operation is called *multiplication modulo n* . $\mathbf{Z}_n$ with addition and multiplication modulo n is a ring: the details are given in [Chapter 19](#).

Let A be any ring. Since A with addition alone is an abelian group, everything we know about abelian groups applies to it. However, it is important to remember that A with addition is an abelian group *in additive notation* and, therefore, before applying theorems about groups to A , these theorems must be translated into additive notation. For example, [Theorems 1, 2, and 3](#) of [Chapter 4](#) read as follows when the notation is additive and the group is abelian:

$$a + b = a + c \quad \text{implies} \quad b = c \quad (1)$$

$$a + b = 0 \quad \text{implies} \quad a = -b \quad \text{and} \quad b = -a \quad (2)$$

$$-(a + b) = -(a) + -(b) \quad \text{and} \quad -(-a) = a \quad (3)$$

Therefore Conditions (1), (2), and (3) are true in every ring.

What happens in a ring when we multiply elements by zero? What happens when we multiply elements by the *negatives* of other elements? The next theorem answers these questions.

Theorem 1 *Let a and b be any elements of a ring A .*

$$(i) \ a0 = 0 \quad \text{and} \quad 0a = 0$$

$$(ii) \ a(-b) = -(ab) \quad \text{and} \quad (-a)b = -(ab)$$

$$(iii) \ (-a)(-b) = ab$$

Part (i) asserts that multiplication by zero always yields zero, and parts (ii) and (iii) state the familiar rules of signs.

PROOF: To prove (i) we note that

$$\begin{aligned} aa + 0 &= aa \\ &= a(a + 0) && \text{because } a = a + 0 \\ &= aa + a0 && \text{by the distributive law} \end{aligned}$$

Thus, $aa + 0 = aa + a0$. By Condition (1) above we may eliminate the term aa on both sides of this equation, and therefore $0 = a0$.

To prove (ii), we have

$$\begin{aligned} a(-b) + ab &= a[(-b) + b] && \text{by the distributive law} \\ &= a0 \\ &= 0 && \text{by part (i)} \end{aligned}$$

Thus, $a(-b) + ab = 0$. By Condition (2) above we deduce that $a(-b) = -(ab)$. The twin formula $(-a)b = -(-ab)$ is deduced analogously.

We prove part (iii) by using part (ii) twice:

$$(-a)(-b) = -[a(-b)] = -[-(ab)] = ab \blacksquare$$

The general definition of a ring is sparse and simple. However, particular rings may also have “optional features” which make them more versatile and interesting. Some of these options are described next.

By definition, addition is commutative in every ring but mutiplication is not. When multiplication *also* is commutative in a ring, we call that ring a *commutative ring*.

A ring A does not necessarily have a neutral element for multiplication. If there *is* in A a neutral element for multiplication, it is called the *unity* of A , and is denoted by the symbol 1 . Thus, $a \cdot 1 = a$ and $1 \cdot a = a$ for every a in A . If A has a unity, we call A a *ring with unity*. The rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, and $\mathcal{F}(\mathbb{R})$ are all examples of commutative rings with unity.

Incidentally, a ring whose only element is 0 is called a *trivial ring*; a ring with more than one element is *nontrivial*. In a nontrivial ring with unity, necessarily $1 \neq 0$. This is true because if $1 = 0$ and x is any element of the ring, then

$$x = x1 = x0 = 0$$

In other words, if $1 = 0$ then every element of the ring is equal to 0 ; hence 0 is the only element of the ring.

If A is a ring with unity, there may be elements in A which *have a multiplicative inverse*. Such elements are said to be *invertible*. Thus, an element a is invertible in a ring if there is some x in the ring such that

$$ax = xa = 1$$

For example, in $\mathbb{R}$ every nonzero element is invertible: its multiplicative inverse is its reciprocal. On the other hand, in $\mathbb{Z}$ the only invertible elements are 1 and -1 .

Zero is never an invertible element of a ring except if the ring is trivial; for if zero had a multiplicative inverse x , we would have $0x = 1$, that is, $0 = 1$.

If A is a *commutative ring with unity in which every nonzero element is invertible*, A is called a *field*. Fields are of the utmost importance in mathematics; for example, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields. There are also *finite* fields, such as $\mathbb{Z}_5$ (it is easy to check that every nonzero element of $\mathbb{Z}_5$ is invertible). Finite fields have beautiful properties and fascinating applications, which will be examined later in this book.

In elementary mathematics we learned the commandment that if the product of two numbers is equal to zero, say

$$ab = 0$$

then one of the two factors, either a or b (or both) must be equal to zero. This is certainly true if the numbers are real (or even complex) numbers, but the rule is *not* inviolable in every ring. For example, in $\mathbb{Z}_6$,

$$2 \cdot 3 = 0$$

even though the factors 2 and 3 are both nonzero. Such numbers, when they exist, are called *divisors of zero*.

*In any ring, a nonzero element a is called a **divisor of zero** if there is a nonzero element b in the ring such that the product ab or ba is equal to zero.*

(Note carefully that *both* factors have to be nonzero.) Thus, 2 and 3 are divisors of zero in $\mathbb{Z}_6$; 4 is also a divisor of zero in $\mathbb{Z}_6$, because $4 \cdot 3 = 0$. For another example, let $\mathcal{M}_2(\mathbb{R})$ designate the set of all 2×2 matrices of real numbers, with addition and multiplication of matrices as described on page 8. The simple task of checking that $\mathcal{M}_2(\mathbb{R})$ satisfies the ring axioms is assigned as [Exercise C1](#) at the end of this chapter. $\mathcal{M}_2(\mathbb{R})$ is rampant with examples of divisors of zero. For instance,

$$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

hence

$$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

are both divisors of zero in $\mathcal{M}_2(\mathbb{R})$.

Of course, there are rings which have no divisors of zero at all! For example, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ do not have any divisors of zero. It is important to note carefully what it means for a ring to have *no divisors of zero*: it means that *if the product of two elements in the ring is equal to zero, at least one of the factors is zero*. (Our commandment from elementary mathematics!)

It is also decreed in elementary algebra that a nonzero number a may be canceled in the equation $ax = ay$ to yield $x = y$. While undeniably true in the number systems of mathematics, this rule is not true

in every ring. For example, in $\mathbf{z}_6$,

$$2.5 = 2.2$$

yet we cannot cancel the common factor 2. A similar example involving 2×2 matrices may be seen on page 9. When cancellation is possible, we say the ring has the “cancellation property.”

*A ring is said to have the **cancellation property** if*

$$ab = ac \quad \text{or} \quad ba = ca \quad \text{implies} \quad b = c$$

for any elements a, b , and c in the ring if $a \neq 0$.

There is a surprising and unexpected connection between the cancellation property and divisors of zero:

Theorem 2 *A ring has the cancellation property iff it has no divisors of zero.*

PROOF: The proof is very straightforward. Let A be a ring, and suppose first that A has the cancellation property. To prove that A has no divisors of zero we begin by letting $ab = 0$, and show that a or b is equal to 0. If $a = 0$, we are done. Otherwise, we have

$$ab = 0 = a0$$

so by the cancellation property (cancelling a), $b=0$.

Conversely, assume A has no divisors of zero. To prove that A has the cancellation property, suppose $ab = ac$ where $a \neq 0$. Then

$$ab - ac = a(b - c) = 0$$

Remember, there are no divisors of zero! Since $a \neq 0$, necessarily $b - c = 0$, so $b = c$. ■

An *integral domain* is defined to be a commutative ring with unity having the cancellation property. By [Theorem 2](#), an integral domain may also be defined as a commutative ring with unity having no divisors of zero. It is easy to see that every field is an integral domain. The converse, however, is not true: for example, $\mathbf{z}$ is an integral domain but not a field. We will have a lot to say about integral domains in the following chapters.

EXERCISES

A. Examples of Rings

In each of the following, a set A with operations of addition and multiplication is given. *Prove that A satisfies all the axioms to be a commutative ring with unity. Indicate the zero element, the unity, and the negative of an arbitrary a .*

1 A is the set $\mathbf{z}$ of the integers, with the following “addition” $\oplus$ and “multiplication” $\odot$:

$$a \oplus b = a + b - 1 \qquad a \odot b = ab - (a + b) + 2$$

2 A is the set $\mathbf{Q}$ of the rational numbers, and the operations are $\oplus$ and $\odot$ defined as follows:

$$a \oplus b = a + b + 1 \qquad a \odot b = ab + a + b$$

3 A is the set $\mathbb{Q} \times \mathbb{Q}$ of ordered pairs of rational numbers, and the operations are the following addition $\oplus$ and multiplication $\odot$:

$$(a, b) \oplus (c, d) = (a + c, b + d)$$

$$(a, b) \odot (c, d) = (ac - bd, ad + bc)$$

4 $A = \{x + y\sqrt{2} : x, y \in \mathbb{Z}\}$ with conventional addition and multiplication.

5 Prove that the ring in part 1 is an integral domain.

6 Prove that the ring in part 2 is a field, and indicate the multiplicative inverse of an arbitrary nonzero element.

7 Do the same for the ring in part 3.

B. Ring of Real Functions

1 Verify that $\mathcal{F}(\mathbb{R})$ satisfies all the axioms for being a commutative ring with unity. Indicate the zero and unity, and describe the negative of any f .

2 Describe the divisors of zero in $\mathcal{F}(\mathbb{R})$.

3 Describe the invertible elements in $\mathcal{F}(\mathbb{R})$.

4 Explain why $\mathcal{F}(\mathbb{R})$ is neither a field nor an integral domain.

C. Ring of 2×2 Matrices

Let $\mathcal{M}_2(\mathbb{R})$ designate the set of all 2×2 matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

whose entries are real numbers a, b, c , and d , with the following addition and multiplication:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} a + r & b + s \\ c + t & d + u \end{pmatrix}$$

and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} ar + bt & as + bu \\ cr + dt & cs + du \end{pmatrix}$$

1 Verify that $\mathcal{M}_2(\mathbb{R})$ satisfies the ring axioms.

2 Show that $\mathcal{M}_2(\mathbb{R})$ is not commutative and has a unity.

3 Explain why $\mathcal{M}_2(\mathbb{R})$ is not an integral domain or a field.

D. Rings of Subsets of a Set

If D is a set, then the power set of D is the set P_D of all the subsets of D . Addition and multiplication are defined as follows: If A and B are elements of P_D (that is, subsets of D), then

$$A + B = (A - B) \cup (B - A) \quad \text{and} \quad AB = A \cap B$$

It was shown in [Chapter 3, Exercise C](#), that P_D with addition alone is an abelian group.

- # **1** Prove: P_D is a commutative ring with unity. (You may assume $\cap$ is associative; for the distributive law, use the same diagram and approach as was used to prove that addition is associative in [Chapter 3, Exercise C](#).)
- 2** Describe the divisors of zero in P_D .
- 3** Describe the invertible elements in P_D .
- 4** Explain why P_D is neither a field nor an integral domain. (Assume D has more than one element.)
- 5** Give the tables of P_3 , that is, P_D where $D = \{a, b, c\}$.

E. Ring of Quaternions

A *quaternion* (in matrix form) is a 2×2 matrix of complex numbers of the form

$$\alpha = \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}$$

- 1** Prove that the set of all the quaternions, with the matrix addition and multiplication explained on pages 7 and 8, is a ring with unity. This ring is denoted by the symbol $\mathcal{Q}$. Find an example to show that $\mathcal{Q}$ is not commutative. (You may assume matrix addition and multiplication are associative and obey the distributive law.)

2 Let

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Show that the quaternion α , defined previously, may be written in the form

$$\alpha = a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$$

(This is the standard notation for quaternions.)

3 Prove the following formulas:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1} \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k} \quad \mathbf{jk} = -\mathbf{kj} = \mathbf{i} \quad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}$$

4 The *conjugate* of α is

$$\bar{\alpha} = \begin{pmatrix} a - bi & -c - di \\ c - di & a + bi \end{pmatrix}$$

The *norm* of α is $a^2 + b^2 + c^2 + d^2$, and is written $\|\alpha\|$. Show directly (by matrix multiplication) that

$$\bar{\alpha}\alpha = \alpha\bar{\alpha} = \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix} \quad \text{where } t = \|\alpha\|$$

Conclude that the multiplicative inverse of α is $(1/t)\bar{\alpha}$.

5 A *skew field* is a (not necessarily commutative) ring with unity in which every nonzero element has a multiplicative inverse. Conclude from parts 1 and 4 that $\mathcal{Q}$ is a skew field.

F. Ring of Endomorphisms

Let G be an abelian group in additive notation. An *endomorphism* of G is a homomorphism from G to G . Let $\text{End}(G)$ denote the set of all the endomorphisms of G , and define addition and multiplication of endomorphisms as follows:

$$[f + g](x) = f(x) + g(x) \quad \text{for every } x \text{ in } G$$

$$fg = f \circ g \quad \text{the composite of } f \text{ and } g$$

- 1 Prove that $\text{End}(G)$ with these operations is a ring with unity.
- 2 List the elements of $\text{End}(\mathbf{z}_4)$, then give the addition and multiplication tables for $\text{End}(\mathbf{z}_4)$.

REMARK: The endomorphisms of $\mathbf{z}_4$ are easy to find. Any endomorphisms of $\mathbf{z}_4$ will carry 1 to either 0, 1, 2, or 3. For example, take the last case: if

$$1 \xrightarrow{f} 3$$

then necessarily

$$1 + 1 \xrightarrow{f} 3 + 3 = 2 \quad 1 + 1 + 1 \xrightarrow{f} 3 + 3 + 3 = 1 \quad \text{and} \quad 0 \xrightarrow{f} 0$$

hence f is completely determined by the fact that

$$1 \xrightarrow{f} 3$$

G. Direct Product of Rings

If A and B are rings, their *direct product* is a new ring, denoted by $A \times B$, and defined as follows: $A \times B$ consists of all the ordered pairs (x, y) where x is in A and y is in B . Addition in $A \times B$ consists of adding corresponding components:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

Multiplication in $A \times B$ consists of multiplying corresponding components:

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2, y_1 y_2)$$

- 1 If A and B are rings, verify that $A \times B$ is a ring.
- 2 If A and B are commutative, show that $A \times B$ is commutative. If A and B each has a unity, show that $A \times B$ has a unity.
- 3 Describe carefully the divisors of zero in $A \times B$.
- # 4 Describe the invertible elements in $A \times B$.
- 5 Explain why $A \times B$ can never be an integral domain or a field. (Assume A and B each have more than one element.)

H. Elementary Properties of Rings

Prove parts 1–4:

- 1 In any ring, $a(b - c) = ab - ac$ and $(b - c)a = ba - ca$.
- 2 In any ring, if $ab = -ba$, then $(a + b)^2 = (a - b)^2 = a^2 + b^2$.
- 3 In any integral domain, if $a^2 = b^2$, then $a = \pm b$.
- 4 In any integral domain, only 1 and -1 are their own multiplicative inverses. (Note that $x = x^{-1}$ iff $x^2 = 1$.)
- 5 Show that the commutative law for addition need not be assumed in defining a ring with unity: it may be proved from the other axioms. [HINT: Use the distributive law to expand $(a + b)(1 + 1)$ in two different ways.]
- # 6 Let A be any ring. Prove that if the additive group of A is cyclic, then A is a commutative ring.
- 7 Prove: In any integral domain, if $a^n = 0$ for some integer n , then $a = 0$.

I. Properties of Invertible Elements

Prove that parts 1–5 are true in a nontrivial ring with unity.

- 1 If a is invertible and $ab = ac$, then $b = c$.
- 2 An element a can have no more than *one* multiplicative inverse.
- 3 If $a^2 = 0$ then $a + 1$ and $a - 1$ are invertible.
- 4 If a and b are invertible, their product ab is invertible.
- 5 The set S of all the invertible elements in a ring is a multiplicative group.
- 6 By part 5, the set of all the nonzero elements in a field is a multiplicative group. Now use Lagrange's theorem to prove that in a finite field with m elements, $x^{m-1} = 1$ for every $x \neq 0$.
- 7 If $ax = 1$, x is a *right inverse* of a ; if $ya = 1$, y is a *left inverse* of a . Prove that if a has a right inverse y and a left inverse x , then a is invertible, and its inverse is equal to x and to y . (First show that $yaxa = 1$.)
- 8 Prove: In a commutative ring, if ab is invertible, then a and b are both invertible.

J. Properties of Divisors of Zero

Prove that each of the following is true in a nontrivial ring.

- 1 If $a \neq \pm 1$ and $a^2 = 1$, then $a + 1$ and $a - 1$ are divisors of zero.
- # 2 If ab is a divisor of zero, then a or b is a divisor of zero.
- 3 In a commutative ring with unity, a divisor of zero cannot be invertible.
- 4 Suppose $ab \neq 0$ in a commutative ring. If either a or b is a divisor of zero, so is ab .
- 5 Suppose a is neither 0 nor a divisor of zero. If $ab = ac$, then $b = c$.
- 6 $A \times B$ always has divisors of zero.

K. Boolean Rings

A ring A is a boolean ring if $a^2 = a$ for every $a \in A$. Prove that parts 1 and 2 are true in any boolean ring A .

- 1 For every $a \in A$, $a = -a$. [HINT: Expand $(a + a)^2$.]
- 2 Use part 1 to prove that A is a commutative ring. [HINT: Expand $(a + b)^2$.]

In parts 3 and 4, assume A has a unity and prove:

3 Every element except 0 and 1 is a divisor of zero. [Consider $x(x - 1)$.]

4 1 is the only invertible element in A .

5 Letting $a \vee b = a + b + ab$ we have the following in A :

$$a \vee bc = (a \vee b)(a \vee c) \quad a \vee (1 + a) = 1 \quad a \vee a = a \quad a(a \vee b) = a$$

L. The Binomial Formula

An important formula in elementary algebra is the binomial expansion formula for an expression $(a + b)^n$. The formula is as follows:

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$$

where the binomial coefficient

$$\binom{n}{k} = \frac{n(n-1)(n-2) \cdots (n-k+1)}{k!}$$

This theorem is true in every commutative ring. (If K is any positive integer and a is an element of a ring, ka refers to the sum $a + a + \cdots + a$ with k terms, as in elementary algebra.) The proof of the binomial theorem in a commutative ring is no different from the proof in elementary algebra. We shall review it here.

The proof of the binomial formula is by induction on the exponent n . The formula is trivially true for $n = 1$. In the induction step, we *assume* the expansion for $(a + b)^n$ is as above, and we must prove that

$$(a + b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k$$

Now,

$$\begin{aligned} (a + b)^{n+1} &= (a + b)(a + b)^n \\ &= (a + b) \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k \\ &= \sum_{k=0}^n \binom{n}{k} a^{n+1-k} b^k + \sum_{k=0}^n \binom{n}{k} a^{n-k} b^{k+1} \end{aligned}$$

Collecting terms, we find that the coefficient of $a^{n+1-k} b^k$ is

$$\binom{n}{k} + \binom{n}{k-1}$$

By direct computation, show that

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$$

It will follow that $(a + b)^{n+1}$ is as claimed, and the proof is complete.

M. Nilpotent and Unipotent Elements

An element a of a ring is *nilpotent* if $a^n = 0$ for some positive integer n .

1 In a ring with unity, prove that if a is nilpotent, then $a + 1$ and $a - 1$ are both invertible. [HINT: Use the factorization

$$1 - a^n = (1 - a)(1 + a + a^2 + \dots + a^{n-1})$$

for $1 - a$, and a similar formula for $1 + a$.]

2 In a commutative ring, prove that any product xa of a nilpotent element a by any element x is nilpotent.

3 In a commutative ring, prove that the sum of two nilpotent elements is nilpotent. (HINT: You must use the binomial formula; see [Exercise L](#).)

An element a of a ring is *unipotent* iff $1 - a$ is nilpotent.

4 In a commutative ring, prove that the product of two unipotent elements a and b is unipotent. [HINT: Use the binomial formula to expand $1 - ab = (1 - a) + a(1 - b)$ to power $n + m$.]

5 In a ring with unity, prove that every unipotent element is invertible. (HINT: Use Part 1.)

IDEALS AND HOMOMORPHISMS

We have already seen several examples of smaller rings contained within larger rings. For example, $\mathbf{Z}$ is a ring inside the larger ring $\mathbf{Q}$, and $\mathbf{Q}$ itself is a ring inside the larger ring $\mathbf{R}$. When a ring B is part of a larger ring A , we call B a *subring* of A . The notion of subring is the precise analog for rings of the notion of subgroup for groups. Here are the relevant definitions:

Let A be a ring, and B a nonempty subset of A . If the sum of any two elements of B is again in B , then B is *closed with respect to addition*. If the negative of every element of B is in B , then B is *closed with respect to negatives*. Finally, if the product of any two elements of B is again in B , then B is *closed with respect to multiplication*. B is called a *subring* of A if B is closed with respect to addition, multiplication, and negatives. Why is B then called a subring of A ? Quite elementary:

If a nonempty subset $B \subseteq A$ is closed with respect to addition, multiplication, and negatives, then B with the operations of A is a ring.

This fact is easy to check: If a , b , and c are any three elements of B , then a , b , and c are also elements of A because $B \subseteq A$. But A is a ring, so

$$\begin{aligned} a + (b + c) &= (a + b) + c \\ a(bc) &= (ab)c \\ a(b + c) &= ab + ac \\ \text{and} \quad (b + c)a &= ba + ca \end{aligned}$$

Thus, in B addition and multiplication are associative and the distributive law is satisfied. Now, B was assumed to be nonempty, so there is an element $b \in B$ but B is closed with respect to negatives, so $-b$ is also in B . Finally, B is closed with respect to addition; hence $b + (-b) \in B$. That is, 0 is in B . Thus, B satisfies all the requirements for being a ring.

For example, $\mathbf{Q}$ is a subring of $\mathbf{R}$ because the sum of two rational numbers is rational, the product of two rational numbers is rational, and the negative of every rational number is rational.

By the way, if B is a nonempty subset of A , there is a more compact way of checking that B is a subring of A :

B is a subring of A if and only if B is closed with respect to subtraction and multiplication.

The reason is that B is *closed with respect to subtraction* iff B is closed with respect to both addition and negatives. This last fact is easy to check, and is given as an exercise.

Awhile back, in our study of groups, we singled out certain special subgroups called *normal subgroups*. We will now describe certain special subrings called *ideals* which are the counterpart of normal subgroups: that is, ideals are in rings as normal subgroups are in groups.

Let A be a ring, and B a nonempty subset of A . We will say that B *absorbs products in A* (or, simply, B *absorbs products*) if, whenever we multiply an element in B by an element in A (regardless of whether the latter is inside B or outside B), their product is always in B . In other words,

$$\text{for all } b \in B \text{ and } x \in A, xb \text{ and } bx \text{ are in } B.$$

A nonempty subset B of a ring A is called an ideal of A if B is closed with respect to addition and negatives, and B absorbs products in A .

A simple example of an ideal is the set $\mathbb{E}$ of the even integers. $\mathbb{E}$ is an ideal of $\mathbb{Z}$ because the sum of two even integers is even, the negative of any even integer is even, and, finally, the product of an even integer by *any* integer is always even.

In a commutative ring with unity, the simplest example of an ideal is the set of all the multiples of a fixed element a by all the elements in the ring. In other words, the set of all the products

$$xa$$

as a remains fixed and x ranges over all the elements of the ring. This set is obviously an ideal because

$$xa + ya = (x + y)a$$

$$-(xa) = (-x)a$$

and

$$y(xa) = (yx)a$$

This ideal is called the *principal ideal generated by a* , and is denoted by

$$\langle a \rangle$$

As in the case of subrings, if B is a nonempty subset of A , there is a more compact way of checking that B is an ideal of A :

B is an ideal of A if and only if B is closed with respect to subtraction and B absorbs products in A .

We shall see presently that ideals play an important role in connection with homomorphism

Homomorphisms are almost the same for rings as for groups.

*A **homomorphism** from a ring A to a ring B is a function $f: A \rightarrow B$ satisfying the identities*

$$f(x_1 + x_2) = f(x_1) + f(x_2)$$

and

$$f(x_1 x_2) = f(x_1) f(x_2)$$

There is a longer but more informative way of writing these two identities:

1. If $f(x_1) = y_1$ and $f(x_2) = y_2$ then $f(x_1 + x_2) = y_1 + y_2$.
2. If $f(x_1) = y_1$ and $f(x_2) = y_2$ then $f(x_1 x_2) = y_1 y_2$

In other words, if f happens to carry x_1 to y_1 and x_2 to y_2 , then, necessarily, it must carry $x_1 + x_2$ to $y_1 + y_2$ and x_1x_2 to y_1y_2 . Symbolically,

If $x_1 \xrightarrow{f} y_1$ and $x_2 \xrightarrow{f} y_2$, then necessarily

$$x_1 + x_2 \xrightarrow{f} y_1 + y_2 \qquad \text{and} \qquad x_1x_2 \xrightarrow{f} y_1y_2$$

One can easily confirm for oneself that a function f with this property will transform the addition and multiplication tables of its domain into the addition and multiplication tables of its range. (We may imagine infinite rings to have “nonterminating” tables.) Thus, a homomorphism from a ring A onto a ring B is a function which transforms A into B .

For example, the ring $\mathbf{z}_6$ is transformed into the ring $\mathbf{z}_3$ by

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$$

as we may verify by comparing their tables. The addition tables are compared on page 136, and we may do the same with their multiplication tables:

·	0	1	2	3	4	5		·	0	1	2	0	1	2
0	0	0	0	0	0	0	Replace x by $f(x)$ →	0	0	0	0	0	0	0
1	0	1	2	3	4	5		1	0	1	2	0	1	2
2	0	2	4	0	2	4		2	0	2	1	0	2	1
3	0	3	0	3	0	3		0	0	0	0	0	0	0
4	0	4	2	0	1	2		1	0	1	2	0	1	2
5	0	5	4	3	2	1		2	0	2	1	0	2	1
Eliminate duplicate information → (For example, $2 \cdot 2 = 1$ appears four separate times in table above.)								·	0	1	2			
								0	0	0	0			
								1	0	1	2			
								2	0	2	1			

If there is a homomorphism from A onto B , we call B a *homomorphic image* of A . If f is a homomorphism from a ring A to a ring B , not necessarily *onto*, the range of f is a subring of B . (This fact is routine to verify.) Thus, the range of a ring homomorphism is always a ring. And obviously, the range of a homomorphism is always a homomorphic image of its domain.

Intuitively, if B is a homomorphic image of A , this means that certain features of A are faithfully preserved in B while others are deliberately lost. This may be illustrated by developing further an example described in [Chapter 14](#). The *parity ring* P consists of two elements, e and o , with addition and

multiplication given by the tables

$+$	e	o
e	e	o
o	o	e

and

$\cdot$	e	o
e	e	e
o	e	o

We should think of e as “even” and o as “odd,” and the tables as describing the rules for adding and multiplying odd and even integers. For example, even + odd = odd, even *times* odd = even, and so on.

The function $f: \mathbf{z} \rightarrow P$ which carries every even integer to e and every odd integer to o is easily seen to be a homomorphism from $\mathbf{z}$ to P this is made clear on page 137. Thus, P is a homomorphic image of $\mathbf{z}$. Although the ring P is very much smaller than the ring $\mathbf{z}$, and therefore few of the features of $\mathbf{z}$ can be expected to reappear in P , nevertheless *one* aspect of the structure of $\mathbf{z}$ is retained absolutely intact in P , namely, the structure of odd and even numbers. As we pass from $\mathbf{z}$ to P , the *parity* of the integers (their being even or odd), with its arithmetic, is faithfully preserved while all else is lost. Other examples will be given in the exercises.

If f is a homomorphism from a ring A to a ring B , the *kernel* of f is the set of all the elements of A which are carried by f onto the zero element of B . In symbols, the kernel of f is the set

$$K = \{x \in A : f(x) = 0\}$$

It is a very important fact that the *kernel of f is an ideal of A* . (The simple verification of this fact is left as an exercise.)

If A and B are rings, an *isomorphism* from A to B is a homomorphism which is a one-to-one correspondence from A to B . In other words, it is an injective and surjective homomorphism. If there *is* an isomorphism from A to B we say that A is *isomorphic to B* , and this fact is expressed by writing

$$A \cong B$$

EXERCISES

A. Examples of Subrings

Prove that each of the following is a subring of the indicated ring:

1 $\{x + \sqrt{3}y : x, y \in \mathbf{z}\}$ is a subring of $\mathbb{R}$.

2 $\{x + 2^{1/3}y + 2^{2/3}z : x, y, z \in \mathbf{z}\}$ is a subring of $\mathbb{R}$.

3 $\{x2^y : x, y \in \mathbf{z}\}$ is a subring of $\mathbb{R}$.

4 Let $\mathcal{C}(\mathbb{R})$ be the set of all the functions from $\mathbb{R}$ to $\mathbb{R}$ which are continuous on $(-\infty, \infty)$ and let $\mathcal{D}(\mathbb{R})$ be the set of all the functions from $\mathbb{R}$ to $\mathbb{R}$ which are differentiable on $(-\infty, \infty)$. Then $\mathcal{C}(\mathbb{R})$ and $\mathcal{D}(\mathbb{R})$ are subrings of $\mathcal{F}(\mathbb{R})$.

5 Let $\mathcal{U}(\mathbf{z})$ be the set of all functions from $\mathbb{R}$ to $\mathbb{R}$ which are continuous on the interval $[0,1]$. Then $\mathcal{U}(\mathbb{R})$ is a subring of $\mathcal{F}(\mathbb{R})$, and $\mathcal{C}(\mathbb{R})$ is a subring of $\mathcal{U}(\mathbb{R})$.

6 The subset of $\mathcal{M}_2(\mathbb{R})$ consisting of all matrices of the form

$$\begin{pmatrix} 0 & 0 \\ 0 & x \end{pmatrix}$$

is a subring of $M_2(\mathbb{R})$.

B. Examples of Ideals

1 Identify which of the following are ideals of $\mathbb{Z} \times \mathbb{Z}$, and explain: $\{(n, n) : n \in \mathbb{Z}\}$; $\{(5n, 0) : n \in \mathbb{Z}\}$; $\{(n, m) : n + m \text{ is even}\}$; $\{(n, m) : nm \text{ is even}\}$; $\{(2n, 3m) : n, m \in \mathbb{Z}\}$.

2 List all the ideals of $\mathbb{Z}_{12}$.

3 Explain why every subring of $\mathbb{Z}_n$ is necessarily an ideal.

4 Explain why the subring of [Exercise A6](#) is not an ideal.

5 Explain why $\mathcal{C}(\mathbb{R})$ is not an ideal of $\mathcal{F}(\mathbb{R})$.

6 Prove that each of the following is an ideal of $\mathcal{F}(\mathbb{R})$:

(a) The set of all f such that $f(x) = 0$ for every rational x .

(b) The set of all f such that $f(0) = 0$.

7 List all the ideals of P_3 . (P_3 is defined in [Chapter 17, Exercise D](#).)

8 Give an example of a subring of P_3 which is not an ideal.

9 Give an example of a subring of $\mathbb{Z}_3 \times \mathbb{Z}_3$ which is not an ideal.

C. Elementary Properties of Subrings

Prove parts 1–6:

1 A nonempty subset B of a ring A is closed with respect to addition and negatives iff B is closed with respect to subtraction.

2 Conclude from part 1 that B is a subring of A iff B is closed with respect to subtraction and multiplication.

3 If A is a finite ring and B is a subring of A , then the order of B is a divisor of the order of A .

4 If a subring B of an integral domain A contains 1, then B is an integral domain. (B is then called a *subdomain* of A .)

5 Every subring containing the unity of a field is an integral domain.

6 If a subring B of a field F is closed with respect to multiplicative inverses, then B is a field. (B is then called a *subfield* of F .)

7 Find subrings of $\mathbb{Z}_{18}$ which illustrate each of the following:

(a) A is a ring with unity, B is a subring of A , but B is not a ring with unity.

(b) A and B are rings with unity, B is a subring of A , but the unity of B is not the same as the unity of A .

8 Let A be a ring, $f: A \rightarrow A$ a homomorphism, and $B = \{x \in A : f(x) = x\}$. Prove that B is a subring of A .

9 The *center* of a ring A is the set of all the elements $a \in A$ such that $ax = xa$ for every $x \in A$. Prove that the center of A is a subring of A .

D. Elementary Properties of Ideals

Let A be a ring and J a nonempty subset of A .

- 1 Using [Exercise C1](#), explain why J is an ideal of A iff J is closed with respect to subtraction and J absorbs products in A .
- 2 If A is a ring with unity, prove that J is an ideal of A iff J is closed with respect to addition and J absorbs products in A .
- 3 Prove that the intersection of any two ideals of A is an ideal of A .
- 4 Prove that if J is an ideal of A and $1 \in J$, then $J = A$.
- 5 Prove that if J is an ideal of A and J contains an invertible element a of A , then $J = A$.
- 6 Explain why a field F can have no nontrivial ideals (that is, no ideals except $\{0\}$ and F).

E. Examples of Homomorphisms

Prove that each of the functions in parts 1–6 is a homomorphism. Then describe its kernel and its range.

1 $\phi : \mathcal{F}(\mathbb{R}) \rightarrow \mathbb{R}$ given by $\phi(f) = f(0)$.

2 $h : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ given by $h(x, y) = x$.

3 $h : \mathbb{R} \rightarrow \mathcal{M}_2(\mathbb{R})$ given by

$$h(x) = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$$

4 $h : \mathbb{R} \times \mathbb{R} \rightarrow \mathcal{M}_2(\mathbb{R})$ given by

$$h(x, y) = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$$

5 Let A be the set $\mathbb{R} \times \mathbb{R}$ with the usual addition and the following “multiplication”:

$$(a, b) \odot (c, d) = (ac, bc)$$

Granting that A is a ring, let $f : A \rightarrow \mathcal{M}_2(\mathbb{R})$ be given by

$$f(x, y) = \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix}$$

6 $h : P_c \rightarrow P_c$ given by $h(A) = A \cap D$, where D is a fixed subset of C .

7 List all the homomorphisms from $\mathbf{Z}_2$ to $\mathbf{Z}_4$; from $\mathbf{Z}_3$ to $\mathbf{Z}_6$.

F. Elementary Properties of Homomorphisms

Let A and B be rings, and $f : A \rightarrow B$ a homomorphism. Prove each of the following:

1 $f(A) = \{f(x) : x \in A\}$ is a subring of B .

2 The kernel of f is an ideal of A .

3 $f(0) = 0$, and for every $a \in A$, $f(-a) = -f(a)$.

4 f is injective iff its kernel is equal to $\{0\}$.

5 If B is an integral domain, then either $f(1) = 1$ or $f(1) = 0$. If $f(1) = 0$, then $f(x) = 0$ for every $x \in A$. If $f(1) = 1$, the image of every invertible element of A is an invertible element of B .

6 Any homomorphic image of a commutative ring is a commutative ring. Any homomorphic image of a field is a field.

7 If the domain A of the homomorphism f is a field, and if the range of f has more than one element, then f is injective. (HINT: Use [Exercise D6](#).)

G. Examples of Isomorphisms

1 Let A be the ring of [Exercise A2](#) in [Chapter 17](#). Show that the function $f(x) = x - 1$ is an isomorphism from $\mathbf{Q}$ to A hence $\mathbf{Q} \cong A$.

2 Let $\mathcal{S}$ be the following subset of $M_2(\mathbb{R})$:

$$\mathcal{S} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$$

Prove that the function

$$f(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

is an isomorphism from $\mathbb{C}$ to $\mathcal{S}$. [REMARK: You must begin by checking that f is a well-defined function; that is, if $a + bi = c + di$, then $f(a + bi) = f(c + di)$. To do this, note that if $a + bi = c + di$ then $a - c = (d - b)i$; this last equation is impossible unless both sides are equal to zero, for otherwise it would assert that a given real number is equal to an imaginary number.]

3 Prove that $\{(x, x) : x \in \mathbf{Z}\}$ is a subring of $\mathbf{Z} \times \mathbf{Z}$, and show $\{(x, x) : x \in \mathbf{Z}\} \cong \mathbf{Z}$.

4 Show that the set of all 2×2 matrices of the form

$$\begin{pmatrix} 0 & 0 \\ 0 & x \end{pmatrix}$$

is a subring of $M_2(\mathbb{R})$, then prove this subring is isomorphic to $\mathbb{R}$.

For any integer k , let $k\mathbf{Z}$ designate the subring of $\mathbf{Z}$ which consists of all the multiples of k .

5 Prove that $\mathbf{Z} \not\subseteq 2\mathbf{Z}$ then prove that $2\mathbf{Z} \not\subseteq 3\mathbf{Z}$. Finally, explain why if $k \neq l$, then $k\mathbf{Z} \not\subseteq l\mathbf{Z}$. (REMEMBER: How do you show that two rings, or groups, are *not* isomorphic?)

H. Further Properties of Ideals

Let A be a ring, and let J and K be ideals of A .

Prove parts 1-4. (In parts 2-4, assume A is a commutative ring.)

1 If $J \cap K = \{0\}$, then $jk = 0$ for every $j \in J$ and $k \in K$.

2 For any $a \in A$, $I_a = \{ax + j + k : x \in A, j \in J, k \in K\}$ is an ideal of A .

3 The *radical* of J is the set $\text{rad } J = \{a \in A : a^n \in J \text{ for some } n \in \mathbf{Z}\}$. For any ideal J , $\text{rad } J$ is an ideal of A .

4 For any $a \in A$, $\{x \in A : ax = 0\}$ is an ideal (called the *annihilator* of a).

Furthermore, $\{x \in A : ax = 0 \text{ for every } a \in A\}$ is an ideal (called the *annihilating ideal* of A). If A is a ring with unity, its annihilating ideal is equal to $\{0\}$.

5 Show that $\{0\}$ and A are ideals of A . (They are *trivial* ideals; every other ideal of A is a *proper* ideal.)

A proper ideal J of A is called *maximal* if it is not strictly contained in any strictly larger proper ideal: that is, if $J \subseteq K$, where K is an ideal containing some element not in J , then necessarily $K = A$. Show that the following is an example of a maximal ideal: In $\mathcal{F}(\mathbb{R})$, the ideal $J = \{f : f(0) = 0\}$. [HINT: Use [Exercise D5](#). Note that if $g \in K$ and $g(0) \neq 0$ (that is, $g \notin J$), then the function $h(x) = g(x) - g(0)$ is in J hence $h(x) - g(x) \in K$. Explain why this last function is an invertible element of $\mathcal{F}(\mathbb{R})$.]

I. Further Properties of Homomorphisms

Let A and B be rings. Prove each of the following:

- 1 If $f : A \rightarrow B$ is a homomorphism from A onto B with kernel K , and J is an ideal of A such that $K \cap J = \{0\}$, then $f(J)$ is an ideal of B .
- 2 If $f : A \rightarrow B$ is a homomorphism from A onto B , and B is a *field*, then the kernel of f is a maximal ideal. (HINT: Use part 1, with [Exercise D6](#). Maximal ideals are defined in [Exercise H5](#).)
- 3 There are no nontrivial homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$. [The trivial homomorphisms are $f(x) = 0$ and $f(x) = x$.]
- 4 If n is a multiple of m , then $\mathbb{Z}_m$ is a homomorphic image of $\mathbb{Z}_n$.
- 5 If n is odd, there is an injective homomorphism from $\mathbb{Z}_2$ into $\mathbb{Z}_{2n}$.

† J. A Ring of Endomorphisms

Let A be a commutative ring. Prove each of the following:

- 1 For each element a in A , the function π_a defined by $\pi_a(x) = ax$ satisfies the identity $\pi_a(x + y) = \pi_a(x) + \pi_a(y)$. (In other words, π_a is an endomorphism of the additive group of A .)
- 2 π_a is injective iff a is not a divisor of zero. (Assume $a \neq 0$.)
- 3 π_a is surjective iff a is invertible. (Assume A has a unity.)
- 4 Let $\mathcal{A}$ denote the set $\{\pi_a : a \in A\}$ with the two operations

$$[\pi_a + \pi_b](x) = \pi_a(x) + \pi_b(x) \quad \text{and} \quad \pi_a \pi_b = \pi_a \circ \pi_b$$

Verify that $\mathcal{A}$ is a ring.

- 5 If $\phi : A \rightarrow \mathcal{A}$ is given by $\phi(a) = \pi_a$, then ϕ is a homomorphism.
- 6 If A has a unity, then ϕ is an isomorphism. Similarly, if A has no divisors of zero then ϕ is an isomorphism.

QUOTIENT RINGS

We continue our journey into the elementary theory of rings, traveling a road which runs parallel to the familiar landscape of groups. In our study of groups we discovered a way of actually *constructing* all the homomorphic images of any group G . We constructed quotient groups of G , and showed that every quotient group of G is a homomorphic image of G . We will now imitate this procedure and construct *quotient rings*.

We begin by defining cosets of rings:

Let A be a ring, and J an ideal of A . For any element $a \in A$, the symbol $J + a$ denotes the set of all sums $j + a$, as a remains fixed and j ranges over J . That is,

$$J + a = \{j + a : j \in J\}$$

*$J + a$ is called a **coset** of J in A .*

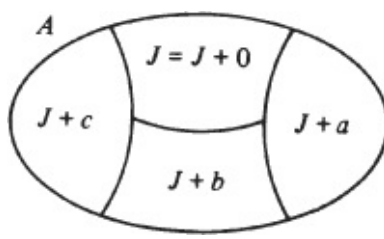
It is important to note that, if we provisionally ignore multiplication, A with addition alone is an abelian group and J is a subgroup of A . Thus, the cosets we have just defined are (if we ignore multiplication) *precisely the cosets of the subgroup J in the group A , with the notation being additive*. Consequently, everything we already know about group cosets continues to apply in the present case—only, care must be taken to translate known facts about group cosets into *additive notation*. For example, Property (1) of [Chapter 13](#), with [Theorem 5](#) of [Chapter 15](#), reads as follows in additive notation:

$$a \in J + b \quad \text{iff} \quad J + a = J + b \quad (1)$$

$$J + a = J + b \quad \text{iff} \quad a - b \in J \quad (2)$$

$$J + a = J \quad \text{iff} \quad a \in J \quad (3)$$

We also know, by the reasoning which leads up to Lagrange's theorem, that the family of all the cosets $J + a$, as a ranges over A , is a partition of A .



There is a way of *adding* and *multiplying cosets* which works as follows:

$$(J + a) + (J + b) = J + (a + b)$$

$$(J + a)(J + b) = J + ab$$

In other words, the sum of the coset of a and the coset of b is the coset of $a + b$; the product of the coset of a and the coset of b is the coset of ab .

It is important to know that the sum and product of cosets, defined in this fashion, are determined without ambiguity. Remember that $J + a$ may be the same coset as $J + c$ [by Condition (1) this happens iff c is an element of $J + a$], and, likewise, $J + b$ may be the same coset as $J + d$. Therefore, we have the equations

$$\begin{array}{ccc} (J + a) + (J + b) = J + (a + b) & & (J + a)(J + b) = J + ab \\ \parallel & & \parallel \\ (J + c) + (J + d) = J + (c + d) & \text{and} & (J + c)(J + d) = J + cd \end{array}$$

Obviously we must be absolutely certain that $J + (a + b) = J + (c + d)$ and $J + ab = J + cd$. The next theorem provides us with this important guarantee.

Theorem 1 *Let J be an ideal of A . If $J + a = J + c$ and $J + b = J + d$, then*

- (i) $J + (a + b) = J + (c + d)$, and
- (ii) $J + ab = J + cd$.

PROOF: We are given that $J + a = J + c$ and $J + b = J + d$; hence by Condition (2),

$$a - c \in J \quad \text{and} \quad b - d \in J$$

Since J is closed with respect to addition, $(a - c) + (b - d) = (a + b) - (c + d)$ is in J . It follows by Condition (2) that $J + (a + b) = J + (c + d)$, which proves (i). On the other hand, since J absorbs products in A ,

$$\underbrace{(a - c)b}_{ab - cb} \in J \quad \text{and} \quad \underbrace{c(b - d)}_{cb - cd} \in J$$

and therefore $(ab - cb) + (cb - cd) = ab - cd$ is in J . It follows by Condition (2) that $J + ab = J + cd$. This proves (ii). ■

Now, think of the set which consists of *all the cosets of J in A* . This set is conventionally denoted by the symbol A/J . For example, if $J + a, J + b, J + c, \dots$ are cosets of J , then

$$A/J = \{J + a, J + b, J + c, \dots\}$$

We have just seen that coset addition and multiplication are valid operations on this set. In fact,

Theorem 2 A/J with coset addition and multiplication is a ring.

PROOF: Coset addition and multiplication are associative, and multiplication is distributive over addition. (These facts may be routinely checked.) The zero element of A/J is the coset $J = J + 0$, for if $J + a$ is any coset,

$$(J + a) + (J + 0) = J + (a + 0) = J + a$$

Finally, the negative of $J + a$ is $J + (-a)$, because

$$(J + a) + (J + (-a)) = J + (a + (-a)) = J + 0 \blacksquare$$

The ring A/J is called the *quotient ring* of A by J .

And now, the crucial connection between quotient rings and homomorphisms :

Theorem 3 A/J is a homomorphic image of A .

Following the plan already laid out for groups, the *natural homomorphism* from A onto A/J is the function f which carries every element to its own coset, that is, the function f given by

$$f(x) = J + x$$

This function is very easily seen to be a homomorphism.

Thus, when we construct quotient rings of A , we are, in fact, constructing homomorphic images of A . The quotient ring construction is useful because it is a way of actually manufacturing homomorphic images of any ring A .

The quotient ring construction is now illustrated with an important example. Let $\mathbf{z}$ be the ring of the integers, and let $\langle 6 \rangle$ be the ideal of $\mathbf{z}$ which consists of all the multiples of the number 6. The elements of the quotient ring $\mathbf{z}/\langle 6 \rangle$ are all the cosets of the ideal $\langle 6 \rangle$, namely:

$$\langle 6 \rangle + 0 = \{ \dots, -18, -12, -6, 0, 6, 12, 18, \dots \} = \bar{0}$$

$$\langle 6 \rangle + 1 = \{ \dots, -17, -11, -5, 1, 7, 13, 19, \dots \} = \bar{1}$$

$$\langle 6 \rangle + 2 = \{ \dots, -16, -10, -4, 2, 8, 14, 20, \dots \} = \bar{2}$$

$$\langle 6 \rangle + 3 = \{ \dots, -15, -9, -3, 3, 9, 15, 21, \dots \} = \bar{3}$$

$$\langle 6 \rangle + 4 = \{ \dots, -14, -8, -2, 4, 10, 16, 22, \dots \} = \bar{4}$$

$$\langle 6 \rangle + 5 = \{ \dots, -13, -7, -1, 5, 11, 17, 23, \dots \} = \bar{5}$$

We will represent these cosets by means of the simplified notation $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$. The rules for adding and multiplying cosets give us the following tables:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

One cannot fail to notice the analogy between the quotient ring $\mathbf{Z}/\langle 6 \rangle$ and the ring $\mathbf{Z}_6$. In fact, we will regard them as one and the same. More generally, for every positive integer n , we consider $\mathbf{Z}_n$ to be the same as $\mathbf{Z}/\langle n \rangle$. In particular, this makes it clear that $\mathbf{Z}_n$ is a homomorphic image of $\mathbf{Z}$.

By [Theorem 3](#), any quotient ring A/J is a homomorphic image of A . Therefore the quotient ring construction is a way of actually producing homomorphic images of any ring A . In fact, as we will now see, it is a way of producing *all* the homomorphic images of A .

Theorem 4 *Let $f: A \rightarrow B$ be a homomorphism from a ring A onto a ring B , and let K be the kernel of f . Then $B \cong A/K$.*

PROOF: To show that A/K is isomorphic with B , we must look for an isomorphism from A/K to B . Mimicking the procedure which worked successfully for groups, we let ϕ be the function from A/K to B which matches each coset $K + x$ with the element $f(x)$; that is,

$$\phi(K + x) = f(x)$$

Remember that if we ignore multiplication for just a moment, A and B are groups and f is a group homomorphism from A onto B , with kernel K . Therefore we may apply [Theorem 2](#) of [Chapter 16](#): ϕ is a well-defined, bijective function from A/K to B . Finally,

$$\begin{aligned} \phi((K + a) + (K + b)) &= \phi(K + (a + b)) = f(a + b) \\ &= f(a) + f(b) = \phi(K + a) + \phi(K + b) \end{aligned}$$

and

$$\begin{aligned} \phi((K + a)(K + b)) &= \phi(K + ab) = f(ab) \\ &= f(a)f(b) = \phi(K + a)\phi(K + b) \end{aligned}$$

Thus, ϕ is an isomorphism from A/K onto B . ■

[Theorem 4](#) is called the *fundamental homomorphism theorem* for rings. [Theorems 3](#) and [4](#) together assert that every quotient ring of A is a homomorphic image of A , and, conversely, every homomorphic image of A is isomorphic to a quotient ring of A . Thus, for all practical purposes, quotients and homomorphic images of a ring are the same.

As in the case of groups, there are many practical instances in which it is possible to select an ideal J of A so as to “factor out” unwanted traits of A , and obtain a quotient ring A/J with “desirable” features.

As a simple example, let A be a ring, not necessarily commutative, and let J be an ideal of A which contains all the differences

$$ab - ba$$

as a and b range over A . It is quite easy to show that the quotient ring A/J is then commutative. Indeed, to say that A/J is commutative is to say that for any two cosets $J + a$ and $J + b$,

$$(J + a)(J + b) = (J + b)(J + a) \quad \text{that is} \quad J + ab = J + ba$$

By Condition (2) this last equation is true iff $ab - ba \in J$. Thus, if every difference $ab - ba$ is in J , then any two cosets commute.

A number of important quotient ring constructions, similar in principle to this one, are given in the exercises.

An ideal J of a commutative ring is said to be a *prime ideal* if for any two elements a and b in the ring,

$$\text{If } ab \in J \text{ then } a \in J \text{ or } b \in J$$

Whenever J is a prime ideal of a commutative ring with unity A , the quotient ring A/J is an integral domain. (The details are left as an exercise.)

An ideal of a ring is called *proper* if it is not equal to the whole ring. A proper ideal J of a ring A is called a *maximal ideal* if there exists no proper ideal K of A such that $J \subseteq K$ with $J \neq K$ (in other words, J is not contained in any strictly larger proper ideal). It is an important fact that if A is a commutative ring with unity, then J is a maximal ideal of A iff A/J is a field.

To prove this assertion, let J be a maximal ideal of A . If A is a commutative ring with unity, it is easy to see that A/J is one also. In fact, it should be noted that the unity of A/J is the coset $J + 1$, because if $J + a$ is any coset, $(J + a)(J + 1) = J + a1 = J + a$. Thus, to prove that A/J is a field, it remains only to show that if $J + a$ is any nonzero coset, there is a coset $J + x$ such that $(J + a)(J + x) = J + 1$.

The zero coset is J . Thus, by Condition (3), to say that $J + a$ is *not* zero, is to say that $a \notin J$. Now, let K be the set of all the sums

$$xa + j$$

as x ranges over A and j ranges over J . It is easy to check that K is an ideal. Furthermore, K contains a because $a = 1a + 0$, and K contains every element $j \in J$ because j can be written as $0a + j$. Thus, K is an ideal which contains J and is strictly larger than J (for remember that $a \in K$ but $a \notin J$). But J is a maximal ideal! Thus, K must be the whole ring A .

It follows that $1 \in K$, so $1 = xa + j$ for some $x \in A$ and $j \in J$. Thus, $1 - xa = j \in J$, so by Condition (2), $J + 1 = J + xa = (J + x)(J + a)$. In the quotient ring A/J , $J + x$ is therefore the multiplicative inverse of $J + a$.

The converse proof consists, essentially, of “unraveling” the preceding argument; it is left as an entertaining exercise.

EXERCISES

A. Examples of Quotient Rings

In each of the following, A is a ring and J is an ideal of A . List the elements of A/J , and then write the addition and multiplication tables of A/J .

Example $A = \mathbb{Z}_6$, $J = \{0, 3\}$.

The elements of A/J are the three cosets $J = J + 0 = \{0,3\}$, $J + 1 = \{1,4\}$, and $J + 2 = \{2,5\}$. The tables for A/J are as follows:

+	J	J + 1	J + 2	·	J	J + 1	J + 2
J	J	J + 1	J + 2	J	J	J	J
J + 1	J + 1	J + 2	J	J + 1	J	J + 1	J + 2
J + 2	J + 2	J	J + 1	J + 2	J	J + 2	J + 1

- $1\ A = \mathbb{Z}_{10}, J = \{0,5\}$.
- $2\ A = P_3, J = \{0, \{a\}\}$. (P_3 is defined in [Chapter 17, Exercise D](#).)
- $3\ A = \mathbb{Z}_2 \times \mathbb{Z}_6; J = \{(0,0), (0,2), (0,4)\}$.

B. Examples of the Use of the FHT

In each of the following, use the FHT (fundamental homomorphism theorem) to prove that the two given groups are isomorphic. Then display their tables.

Example $\mathbb{Z}_2$ and $\mathbb{Z}_6/\langle 2 \rangle$.

The following function is a homomorphism from $\mathbb{Z}_6$ onto $\mathbb{Z}_2$:

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

(Do not prove that J is a homomorphism.)

The kernel of f is $\{0, 2, 4\} = (2)$. Thus:

$$\mathbb{Z}_6 \xrightarrow{\langle 2 \rangle} \mathbb{Z}_2$$

It follows by the FHT that $\mathbb{Z}_2 \cong \mathbb{Z}_6/\langle 2 \rangle$.

- $1\ \mathbb{Z}_5$ and $\mathbb{Z}_{20}/\langle 5 \rangle$.
- $2\ \mathbb{Z}_3$ and $\mathbb{Z}_6/\langle 3 \rangle$.
- $3\ P_2$ and P_3/K , where $K = \{0, \{c\}\}$. [HINT: See [Chapter 18, Exercise E6](#). Consider the function $f(X) = X \cap \{a, b\}$.]
- $4\ \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2/K$, where $K = \{(0, 0), (0,1)\}$.

C. Quotient Rings and Homomorphic Images in $\mathcal{F}(\mathbb{R})$

- 1 Let ϕ be the function from $\mathcal{F}(\mathbb{R})$ to $\mathbb{R} \times \mathbb{R}$ defined by $\phi(f) = (f(0), f(1))$. Prove that ϕ is a homomorphism from $\mathcal{F}(\mathbb{R})$ onto $\mathbb{R} \times \mathbb{R}$, and describe its kernel.
- 2 Let J be the subset of $\mathcal{F}(\mathbb{R})$ consisting of all f whose graph passes through the points $(0,0)$ and $(1,0)$. Referring to part 1, explain why J is an ideal of $\mathcal{F}(\mathbb{R})$, and $\mathcal{F}(\mathbb{R})/J \cong \mathbb{R} \times \mathbb{R}$.
- 3 Let ϕ be the function from $\mathcal{F}(\mathbb{R})$ to $\mathcal{F}(\mathbb{Q}, \mathbb{R})$ defined as follows:

$$\phi(f) = f_{\mathbb{Q}} = \text{the restriction of } f \text{ to } \mathbb{Q}$$

(NOTE: The domain of $f_{\mathbf{Q}}$ is $\mathbf{Q}$ and on this domain $f_{\mathbf{Q}}$ is the same function as f .) Prove that ϕ is a homomorphism from $\mathcal{F}(\mathbf{R})$ onto $\mathcal{F}(\mathbf{Q}, \mathbf{R})$, and describe the kernel of ϕ . [$\mathcal{F}(\mathbf{Q}, \mathbf{R})$ is the ring of functions from $\mathbf{Q}$ to $\mathbf{R}$.]

4 Let J be the subset of $\mathcal{F}(\mathbf{R})$ consisting of all f such that $f(x) = 0$ for every rational x . Referring to part 3, explain why J is an ideal of $\mathcal{F}(\mathbf{R})$ and $\mathcal{F}(\mathbf{R})/J \cong \mathcal{F}(\mathbf{Q})$.

D. Elementary Applications of the Fundamental Homomorphism Theorem

In each of the following let A be a commutative ring. If $a \in A$ and n is a positive integer, the notation na will stand for

$$a + a + \dots + a \quad (n \text{ terms})$$

1 Suppose $2x = 0$ for every $x \in A$. Prove that $(x + y)^2 = x^2 + y^2$ for all x and y in A . Conclude that the function $h(x) = x^2$ is a homomorphism from A to A . If $J = \{x \in A : x^2 = 0\}$ and $B = \{x^2 : x \in A\}$, explain why J is an ideal of A , B is a subring of A , and $A/J \cong B$.

2 Suppose $6x = 0$ for every $x \in A$. Prove that the function $h(x) = 3x$ is a homomorphism from A to A . If $J = \{x : 3x = 0\}$ and $B = \{3x : x \in A\}$, explain why J is an ideal of A , B is a subring of A , and $A/J \cong B$.

3 If a is an idempotent element of A (that is, $a^2 = a$), prove that the function $\pi_a(x) = ax$ is a homomorphism from A into A . Show that the kernel of π_a is I_a , the annihilator of a (defined in [Exercise H4](#) of [Chapter 18](#)). Show that the range of π_a is $\langle a \rangle$. Conclude by the FHT that $A/I_a = \langle a \rangle$.

4 For each $a \in A$, let π_a be the function given by $\pi_a(x) = ax$. Define the following addition and multiplication on $\bar{A} = \{\pi_a : a \in A\}$:

$$\pi_a + \pi_b = \pi_{a+b} \text{ and } \pi_a \pi_b = \pi_{ab}$$

($\bar{A}$ is a ring; however, do not prove this.) Show that the function $\phi(a) = \pi_a$ is a homomorphism from A onto $\bar{A}$. Let I designate the annihilating ideal of A (defined in [Exercise H4](#) of [Chapter 18](#)). Use the FHT to show that $A/I \cong \bar{A}$.

E. Properties of Quotient Rings A/J in Relation to Properties of J

Let A be a ring and J an ideal of A . Use Conditions (1), (2), and (3) of this chapter. Prove each of the following:

1 Every element of A/J has a square root iff for every $x \in A$, there is some $y \in A$ such that $x - y^2 \in J$.

2 Every element of A/J is its own negative iff $x + x \in J$ for every $x \in A$.

3 A/J is a boolean ring iff $x^2 - x \in J$ for every $x \in A$. (A ring S is called a boolean ring iff $s^2 = s$ for every $s \in S$.)

4 If J is the ideal of all the nilpotent elements of a commutative ring A , then A/J has no nilpotent elements (except zero). (Nilpotent elements are defined in [Chapter 17](#), [Exercise M](#); by M2 and M3 they form an ideal.)

5 Every element of A/J is nilpotent iff J has the following property: for every $x \in A$, there is a positive integer n such that $x^n \in J$.

6 A/J has a unity element iff there exists an element $a \in A$ such that $ax - x \in J$ and $xa - x \in J$ for every $x \in A$.

F. Prime and Maximal Ideals

Let A be a commutative ring with unity, and J an ideal of A . Prove each of the following:

- 1 A/J is a commutative ring with unity.
- 2 J is a prime ideal iff A/J is an integral domain.
- 3 Every maximal ideal of A is a prime ideal. (HINT: Use the fact, proved in this chapter, that if J is a maximal ideal then A/J is a field.)
- 4 If A/J is a field, then J is a maximal ideal. (HINT: See [Exercise I2](#) of [Chapter 18](#).)

G. Further Properties of Quotient Rings in Relation to Their Ideals

Let A be a ring and J an ideal of A . (In parts 1–3 and 5 assume that A is a commutative ring with unity.)

- # 1 Prove that A/J is a field iff for every element $a \in A$, where $a \notin J$, there is some $b \in A$ such that $ab - 1 \in J$.
- 2 Prove that every nonzero element of A/J is either invertible or a divisor of zero iff the following property holds, where $a, x \in A$: For every $a \notin J$, there is some $x \notin J$ such that either $ax \in J$ or $ax - 1 \in J$.
- 3 An ideal J of a ring A is called *primary* iff for all $a, b \in A$, if $ab \in J$, then either $a \in J$ or $b^n \in J$ for some positive integer n . Prove that every zero divisor in A/J is nilpotent iff J is primary.
- 4 An ideal J of a ring A is called *semiprime* iff it has the following property: For every $a \in A$, if $a^n \in J$ for some positive integer n , then necessarily $a \in J$. Prove that J is semiprime iff A/J has no nilpotent elements (except zero).
- 5 Prove that an integral domain can have no nonzero nilpotent elements. Then use part 4, together with [Exercise F2](#), to prove that every prime ideal in a commutative ring is semiprime.

H. $\mathbf{Z}_n$ as a Homomorphic Image of $\mathbf{Z}$

Recall that the function

$$f(a) = \bar{a}$$

is the natural homomorphism from $\mathbf{Z}$ onto $\mathbf{Z}_n$. If a polynomial equation $p = 0$ is satisfied in $\mathbf{Z}$, necessarily $f(p) = f(0)$ is true in $\mathbf{Z}_n$. Let us take a specific example; there are integers x and y satisfying $11x^2 - 8y^2 + 29 = 0$ (we may take $x = 3$ and $y = 4$). It follows that there must be elements $\bar{x}$ and $\bar{y}$ in $\mathbf{Z}_6$ which satisfy $\overline{11} \bar{x}^2 - \overline{8} \bar{y}^2 + \overline{29} = \bar{0}$ in $\mathbf{Z}_6$, that is, $\bar{5} \bar{x}^2 - \bar{2} \bar{y}^2 + \bar{5} = \bar{0}$. (We take $\bar{x} = \bar{3}$ and $\bar{y} = \bar{4}$.) The problems which follow are based on this observation.

- 1 Prove that the equation $x^2 - 7y^2 - 24 = 0$ has no integer solutions. (HINT: If there are integers x and y satisfying this equation, what equation will $\bar{x}$ and $\bar{y}$ satisfy in $\mathbf{Z}_7$?)
- 2 Prove that $x^2 + (x + 1)^2 + (x + 2)^2 = y^2$ has no integer solutions.
- 3 Prove that $x^2 + 10y^2 = n$ (where n is an integer) has no integer solutions if the last digit of n is 2, 3, 7, or 8.
- 4 Prove that the sequence 3, 8, 13, 18, 23, ... does not include the square of any integer. (HINT: The

image of each number on this list, under the natural homomorphism from $\mathbf{z}$ to $\mathbf{z}_5$, is 3.)

5 Prove that the sequence 2, 10, 18, 26, ... does not include the cube of any integer.

6 Prove that the sequence 3, 11, 19, 27, ... does not include the sum of two squares of integers.

7 Prove that if n is a product of two consecutive integers, its units digit must be 0, 2, or 6.

8 Prove that if n is the product of three consecutive integers, its units digit must be 0, 4, or 6.

INTEGRAL DOMAINS

Let us recall that an integral domain is a commutative ring with unity having the cancellation property, that is,

$$\text{if } a \neq 0 \text{ and } ab = ac \text{ then } b = c \quad (1)$$

At the end of [Chapter 17](#) we saw that an integral domain may also be defined as a commutative ring with unity having no divisors of zero, which is to say that

$$\text{if } ab = 0 \text{ then } a = 0 \text{ or } b = 0 \quad (2)$$

for as we saw, (1) and (2) are equivalent properties in any commutative ring.

The system $\mathbf{z}$ of the integers is the exemplar and prototype of integral domains. In fact, the term “integral domain” means a system of algebra (“domain”) having *integerlike* properties. However, $\mathbf{z}$ is not the only integral domain: there are a great many integral domains different from $\mathbf{z}$.

Our first few comments will apply to rings generally. To begin with, we introduce a convenient notation for multiples, which parallels the *exponent notation* for powers. Additively, the sum

$$a + a + \cdots + a$$

of n equal terms is written as $n \cdot a$. We also define $0 \cdot a$ to be 0, and let $(-n) \cdot a = -(n \cdot a)$ for all positive integers n . Then

$$m \cdot a + n \cdot a = (m + n) \cdot a \quad \text{and} \quad m \cdot (n \cdot a) = (mn) \cdot a$$

for every element a of a ring and all integers m and n . These formulas are the translations into additive notation of the *laws of exponents* given in [Chapter 10](#).

If A is a ring, A with addition alone is a group. Remember that in additive notation the *order* of an element a in A is the least positive integer n such that $n \cdot a = 0$. If there is no such positive integer n , then a is said to have order infinity. To emphasize the fact that we are referring to the order of a in terms

of *addition*, we will call it the *additive order* of a .

In a ring with unity, if 1 has additive order n , we say the ring has “characteristic n .” In other words, if A is a ring with unity,

*the **characteristic** of A is the least positive integer n such that*

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$$

*If there is no such positive integer n , A has **characteristic 0**.*

These concepts are especially simple in an integral domain. Indeed,

Theorem 1 *All the nonzero elements in an integral domain have the same additive order.*

PROOF: That is, every $a \neq 0$ has the same additive order as the additive order of 1. The truth of this statement becomes transparently clear as soon as we observe that

$$n \cdot a = a + a + \cdots + a = 1a + \cdots + 1a = (1 + \cdots + 1)a = (n \cdot 1)a$$

hence $n \cdot a = 0$ iff $n \cdot 1 = 0$. (Remember that in an integral domain, if the product of two factors is equal to 0, at least one factor must be 0.) ■

It follows, in particular, that if the characteristic of an integral domain is a positive integer n , then

$$n \cdot x = 0$$

for every element x in the domain.

Furthermore,

Theorem 2 *In an integral domain with nonzero characteristic, the characteristic is a prime number.*

PROOF: If the characteristic were a composite number mn , then by the distributive law,

$$(m \cdot 1)(n \cdot 1) = \underbrace{(1 + \cdots + 1)}_{m \text{ terms}} \underbrace{(1 + \cdots + 1)}_{n \text{ terms}} = \underbrace{1 + 1 + \cdots + 1}_{mn \text{ terms}} = (mn) \cdot 1 = 0$$

Thus, either $m \cdot 1 = 0$ or $n \cdot 1 = 0$, which is impossible because mn was chosen to be the *least* positive integer such that $(mn) \cdot 1 = 0$. ■

A very interesting rule of arithmetic is valid in integral domains whose characteristic is not zero.

Theorem 3 *In any integral domain of characteristic p ,*

$$(a + b)^p = a^p + b^p \quad \text{for all elements } a \text{ and } b$$

PROOF: This formula becomes clear when we look at the binomial expansion of $(a + b)^p$. Remember that by the binomial formula,

$$(a + b)^p = a^p + \binom{p}{1} \cdot a^{p-1}b + \cdots + \binom{p}{p-1} \cdot ab^{p-1} + b^p$$

where the binomial coefficient

$$\binom{p}{k} = \frac{p(p-1)(p-2) \cdots (p-k+1)}{k!}$$

It is demonstrated in [Exercise L](#) of [Chapter 17](#) that the binomial formula is correct in every commutative ring.

Note that if p is a prime number and $0 < k < p$, then

$$\binom{p}{k} \text{ is a multiple of } p$$

because every factor of the denominator is less than p , hence p does not cancel out. Thus, each term of the binomial expansion above, except for the first and last terms, is of the form px , which is equal to 0 because the domain has characteristic p . Thus, $(a + b)^p = a^p + b^p$. ■

It is obvious that every field is an integral domain: for if $a \neq 0$ and $ax = ay$ in a field, we can multiply both sides of this equation by the multiplicative inverse of a to cancel a . However, not every integral domain is a field: for example, $\mathbf{Z}$ is not a field. Nevertheless,

Theorem 4 *Every finite integral domain is a field.*

List the elements of the integral domain in the following manner:

$$0, 1, a_1, a_2, \dots, a_n$$

In this manner of listing, there are $n + 2$ elements in the domain. Take any a_i , and show that it is invertible: to begin with, note that the products

$$a_i 0, a_i 1, a_i a_1, a_i a_2, \dots, a_i a_n$$

are all distinct: for if $a_i x = a_i y$, then $x = y$. Thus, there are $n + 2$ *distinct* products $a_i x$; but there are exactly $n + 2$ elements in the domain, so every element in the domain is equal to one of these products. In particular, $1 = a_i x$ for some x ; hence a_i is invertible.

OPTIONAL

The integral domain $\mathbf{Z}$ is not a field because it does not contain the quotients m/n of integers. However, $\mathbf{Z}$ can be *enlarged* to a field by adding to it all the quotients of integers; the resulting field, of course, is $\mathbf{Q}$, the field of the rational numbers. $\mathbf{Q}$ consists of all quotients of integers, and it contains $\mathbf{Z}$ (or rather, an isomorphic copy of $\mathbf{Z}$) when we identify each integer n with the quotient $n/1$. We say that $\mathbf{Q}$ is *the field of quotients* of $\mathbf{Z}$.

It is a fascinating fact that the method for constructing $\mathbf{Q}$ from $\mathbf{Z}$ can be applied to any integral domain. Starting from any integral domain A , it is possible to construct a field which contains A : a field of quotients of A . This is not merely a mathematical curiosity, but a valuable addition to our knowledge. In applications it often happens that a system of algebra we are dealing with lacks a needed property, but is contained in a larger system which *has* that property—and that is almost as good! In the present case, A is not a field but may be enlarged to one.

Thus, if A is any integral domain, we will proceed to construct a field A^* consisting of all the quotients of elements in A ; and A^* will contain A , or rather an isomorphic copy of A , when we identify each element a of A with the quotient $a/1$. The construction will be carefully outlined and the busy work left as an exercise.

Given A , let S denote the set of all ordered pairs (a, b) of elements of A , where $b \neq 0$. That is,

$$S = \{(a, b): a, b \in A \text{ and } b \neq 0\}$$

In order to understand the next step, we should think of (a, b) as a/b . [It is too early in the proof to introduce fractional notation; nevertheless each ordered pair (a, b) should be *thought of* as a fraction a/b .] Now a problem of representation arises here, because it is obvious that the quotient xa/xb is equal to the quotient a/b ; to put the same fact differently, the quotients a/b and c/d are equal whenever $ad = bc$. That is, if $ad = bc$, then a/b and c/d are two different ways of writing the *same* quotient. Motivated by this observation, we *define* $(a, b) \sim (c, d)$ to mean that $ad = bc$, and easily verify that $\sim$ is an equivalence relation on the set S . (Equivalence relations are explained in [Chapter 12](#).) Then we let $[a, b]$ denote the *equivalence class* of (a, b) , that is,

$$[a, b] = \{(c, d) \in S : (c, d) \sim (a, b)\}$$

Intuitively, all the pairs which represent a given quotient are lumped together in one equivalence class; thus, *each quotient is represented by exactly one equivalence class*.

Let us recapitulate the formal details of our construction up to this point: Given the set S of ordered pairs of elements in A , we define an equivalence relation — in S by letting $(a, b) \sim (c, d)$ iff $ad = bc$. We let $[a, b]$ designate the equivalence class of (a, b) , and finally, we let A^* denote the set of all the equivalence classes $[a, b]$. The elements of A^* will be called *quotients*.

Before going on, observe carefully that

$$[a, b] = [r, s] \quad \text{iff} \quad (a, b) \sim (r, s) \quad \text{iff} \quad as = br \quad (3)$$

As our next step, we define operations of addition and multiplication in A^* :

$$[a, b] + [c, d] = [ad + bc, bd]$$

and

$$[a, b] \cdot [c, d] = [ac, bd]$$

To understand these definitions, simply remember the formulas

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

We must make certain these definitions are unambiguous; that is, if $[a, b] = [r, s]$ and $[c, d] = [t, u]$, we have equations

$$\begin{array}{ccc} [a, b] + [c, d] = [ad + bc, bd] & & [a, b] \cdot [c, d] = [ac, bd] \\ \parallel & \parallel & \parallel \\ [r, s] + [t, u] = [ru + st, su] & \text{and} & [r, s] \cdot [t, u] = [ru, su] \end{array}$$

and we must therefore verify that $[ad + bc, bd] = [ru + st, su]$ and $[ac, bd] = [rt, su]$. This is left as an exercise. It is also left for the student to verify that addition and multiplication are associative and commutative and the distributive law is satisfied.

The zero element is $[0, 1]$, because $[a, b] + [0, 1] = [a, b]$. The negative of $[a, b]$ is $[-a, b]$, for $[a, b] + [-a, b] = [0, b^2] = [0, 1]$. [The last equation is true because of [Equation \(3\)](#).] The unity is $[1, 1]$, and the multiplicative inverse of $[a, b]$ is $[b, a]$, for $[a, b] \cdot [b, a] = [ab, ab] = [1, 1]$. Thus, A^* is a field!

Finally, if A' is the subset of A^* which contains every $[a, 1]$, we let ϕ be the function from A to A' defined by $\phi(a) = [a, 1]$. This function is injective because, by Equation (3), if $[a, 1] = [b, 1]$ then $a = b$. It is obviously surjective and is easily shown to be a homomorphism. Thus, ϕ is an isomorphism from A to A' so A^* contains an isomorphic copy A' of A .

EXERCISES

A. Characteristic of an Integral Domain

Let A be a finite integral domain. Prove each of the following:

- 1 Let a be any nonzero element of A . If $n \cdot a = 0$, where $n \neq 0$, then n is a multiple of the characteristic of A .
- 2 If A has characteristic zero, $n \neq 0$, and $n \cdot a = 0$, then $a = 0$.
- 3 If A has characteristic 3, and $5 \cdot a = 0$, then $a = 0$.
- 4 If there is a nonzero element a in A such that $256 \cdot a = 0$, then A has characteristic 2.
- 5 If there are distinct nonzero elements a and b in A such that $125 \cdot a = 125 \cdot b$, then A has characteristic 5.
- 6 If there are nonzero elements a and b in A such that $(a + b)^2 = a^2 + b^2$, then A has characteristic 2.
- 7 If there are nonzero elements a and b in A such that $10a = 0$ and $14b = 0$, then A has characteristic 2.

B. Characteristic of a Finite Integral Domain

Let A be an integral domain. Prove each of the following:

- 1 If A has characteristic q , then q is a divisor of the order of A .
- 2 If the order of A is a prime number p , then the characteristic of A must be equal to p .
- 3 If the order of A is p^m , where p is a prime, the characteristic of A must be equal to p .
- 4 If A has 81 elements, its characteristic is 3.
- 5 If A , with addition alone, is a cyclic group, the order of A is a prime number.

C. Finite Rings

Let A be a finite commutative ring with unity.

- 1 Prove: Every nonzero element of A is either a divisor of zero or invertible. (HINT: Use an argument analogous to the proof of [Theorem 4](#).)
- 2 Prove: If $a \neq 0$ is not a divisor of zero, then some positive power of a is equal to 1. (HINT: Consider $a, a^2, a^3, \dots$. Since A is finite, there must be positive integers $n < m$ such that $a^n = a^m$.)

3 Use part 2 to prove: If a is invertible, then a^{-1} is equal to a positive power of a .

D. Field of Quotients of an Integral Domain

The following questions refer to the construction of a field of quotients of A , as outlined on pages 203 to 205.

- 1** If $[a, b] = [r, s]$ and $[c, d] = [t, u]$, prove that $[a, b] + [c, d] = [r, s] + [t, u]$.
- 2** If $[a, b] = [r, s]$ and $[c, d] = [t, u]$, prove that $[a, b][c, d] = [r, s][t, u]$.
- 3** If $(a, b) \sim (c, d)$ means $ad = bc$, prove that $\sim$ is an equivalence relation on S .
- 4** Prove that addition in A^* is associative and commutative.
- 5** Prove that multiplication in A^* is associative and commutative.
- 6** Prove the distributive law in A^* .
- 7** Verify that $\phi: A \rightarrow A'$ is a homomorphism.

E. Further Properties of the Characteristic of an Integral Domain

Let A be an integral domain. Prove parts 1-4:

- 1** Let $a \in A$. If A has characteristic p , and $n \cdot a = 0$ where n is *not* a multiple of p , then $a = 0$.
 - 2** If p is a prime, and there is a nonzero element $a \in A$ such that $p \cdot a = 0$, then A has characteristic p .
 - 3** If p is a prime, and there is a nonzero element $a \in A$ such that $p^m \cdot a = 0$ for some integer m , then A has characteristic p .
 - 4** If A has characteristic p , then the function $f(a) = a^p$ is a homomorphism from A to A .
- # **5** Let A have order p , where p is a prime. Explain why

$$A = \{0, 1, 2 \cdot 1, 3 \cdot 1, \dots, (p-1) \cdot 1\}$$

Prove that $A \cong \mathbb{Z}_p$.

- # **6** If A has characteristic p , prove that for any positive integer n ,

$$(a) (a + b)^{p^n} = a^{p^n} + b^{p^n}$$

$$(b) (a_1 + a_2 + \dots + a_r)^{p^n} = a_1^{p^n} + \dots + a_r^{p^n}$$

- 7** Let $A \subseteq B$ where A and B are integral domains. Prove: A has characteristic p iff B has characteristic p .

F. Finite Fields

By [Theorem 4](#), “finite integral domain” and “finite field” are the same.

- 1** Prove: Every finite field has nonzero characteristic.
- 2** Prove that if A is a finite field of characteristic p , the function $f(a) = a^p$ is an automorphism of A ; that is, an isomorphism from A to A . (HINT: Use [Exercise E4](#) above and [Exercise F7](#) of [Chapter 18](#). To show that f is surjective, compare the number of elements in the domain and in the range of f .)

*The function $f(a) = a^p$ is called the **Frobenius automorphism**.*

- 3** Use part 2 to prove: In a finite field of characteristic p , every element has a p -th root.