

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.

CHAPTER TWENTY-FOUR

RINGS OF POLYNOMIALS

In elementary algebra an important role is played by polynomials in an unknown x . These are expressions such as

$$2x^3 - \frac{1}{2}x^2 + 3$$

whose terms are grouped in powers of x . The exponents, of course, are positive integers and the coefficients are real or complex numbers.

Polynomials are involved in countless applications—applications of every kind and description. For example, polynomial functions are the easiest functions to compute, and therefore one commonly attempts to approximate arbitrary functions by polynomial functions. A great deal of effort has been expended by mathematicians to find ways of achieving this.

Aside from their uses in science and computation, polynomials come up very naturally in the general study of rings, as the following example will show:

Suppose we wish to enlarge the ring $\mathbf{z}$ by adding to it the number π . It is easy to see that we will have to adjoin to $\mathbf{z}$ other new numbers besides just π ; for the enlarged ring (containing π as well as all the integers) will also contain such things as $-\pi$, $\pi + 7$, $6\pi^2 - 11$, and so on.

As a matter of fact, any ring which contains $\mathbf{z}$ as a subring and which also contains the number π will have to contain every number of the form

$$a\pi^n + b\pi^{n-1} + \dots + k\pi + l$$

where $a, b, \dots, k, l$ are integers. In other words, it will contain *all the polynomial expressions in π with integer coefficients*.

But the set of all the polynomial expressions in π with integer coefficients is a ring. (It is a subring of $\mathbb{R}$ because it is obvious that the sum and product of any two polynomials in π is again a polynomial in π .) This ring contains $\mathbf{z}$ because every integer a is a polynomial with a constant term only, and it also contains π .

Thus, if we wish to enlarge the ring $\mathbf{z}$ by adjoining to it the new number π , it turns out that the

“next largest” ring after $\mathbf{z}$ which contains $\mathbf{z}$ as a subring and includes π , is exactly the ring of all the polynomials in π with coefficients in $\mathbf{z}$.

As this example shows, aside from their practical applications, polynomials play an important role in the scheme of ring theory because they are precisely what we need when we wish to enlarge a ring by adding new elements to it.

In elementary algebra one considers polynomials whose coefficients are real numbers, or in some cases, complex numbers. As a matter of fact, the properties of polynomials are pretty much independent of the exact nature of their coefficients. All we need to know is that the coefficients are contained in some ring. For convenience, we will assume this ring is a commutative ring with unity.

Let A be a commutative ring with unity. Up to now we have used letters to denote elements or sets, but now we will use the letter x in a different way. In a polynomial expression such as $ax^2 + bx + c$, where $a, b, c \in A$, we do not consider x to be an element of A , but rather x is a symbol which we use in an entirely formal way. Later we will allow the substitution of other things for x , but at present x is simply a placeholder.

Notationally, the terms of a polynomial may be listed in either ascending or descending order. For example, $4x^3 - 3x^2 + x + 1$ and $1 + x - 3x^2 + 4x^3$ denote the same polynomial. In elementary algebra descending order is preferred, but for our purposes ascending order is more convenient.

Let A be a commutative ring with unity, and x an arbitrary symbol. Every expression of the form

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

*is called a **polynomial in x with coefficients in A** , or more simply, a **polynomial in x over A** . The expressions a_kx^k , for $k \in \{1, \dots, n\}$, are called the **terms** of the polynomial.*

Polynomials in x are designated by symbols such as $a(x)$, $b(x)$, $q(x)$, and so on. If $a(x) = a_0 + a_1x + \cdots + a_nx^n$ is any polynomial and a_kx^k is any one of its terms, a_k is called the *coefficient* of x^k . By the *degree* of a polynomial $a(x)$ we mean the *greatest n such that the coefficient of x^n is not zero*. In other words, if $a(x)$ has degree n , this means that $a_n \neq 0$ but $a_m = 0$ for every $m > n$. The degree of $a(x)$ is symbolized by

$$\deg a(x)$$

For example, $1 + 2x - 3x^2 + x^3$ is a polynomial degree 3.

The polynomial $0 + 0x + 0x^2 + \cdots$ all of whose coefficients are equal to zero is called the *zero polynomial*, and is symbolized by 0. It is the only polynomial whose *degree is not defined* (because it has no nonzero coefficient).

If a nonzero polynomial $a(x) = a_0 + a_1x + \cdots + a_nx^n$ has degree n , then a_n is called its *leading coefficient*: it is the last nonzero coefficient of $a(x)$. The term a_nx^n is then called its *leading term*, while a_0 is called its *constant term*.

If a polynomial $a(x)$ has degree zero, this means that its constant term a_0 is its only nonzero term: $a(x)$ is a *constant polynomial*. Beware of confusing a polynomial of degree zero with the zero polynomial.

Two polynomials $a(x)$ and $b(x)$ are *equal* if they have the same degree and corresponding coefficients are equal. Thus, if $a(x) = a_0 + \cdots + a_nx^n$ is of degree n , and $b(x) = b_0 + \cdots + b_mx^m$ is of degree

m , then $a(x) = b(x)$ iff $n = m$ and $a_k = b_k$ for each k from 0 to n .

The familiar sigma notation for sums is useful for polynomials. Thus,

$$a(x) = a_0 + a_1x + \cdots + a_nx^n = \sum_{k=0}^n a_kx^k$$

with the understanding that $x^0 = 1$.

Addition and multiplication of polynomials is familiar from elementary algebra. We will now define these operations formally. Throughout these definitions we let $a(x)$ and $b(x)$ stand for the following polynomials:

$$a(x) = a_0 + a_1x + \cdots + a_nx^n$$

$$b(x) = b_0 + b_1x + \cdots + b_nx^n$$

Here we do *not* assume that $a(x)$ and $b(x)$ have the same degree, but allow ourselves to insert zero coefficients if necessary to achieve uniformity of appearance.

We add polynomials by adding corresponding coefficients. Thus,

$$a(x) + b(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$$

Note that the degree of $a(x) + b(x)$ is less than or equal to the *higher* of the two degrees, $\deg a(x)$ and $\deg b(x)$.

Multiplication is more difficult, but quite familiar:

$$\begin{aligned} a(x)b(x) \\ = a_0b_0 + (a_0b_1 + b_0a_1)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots + a_nb_nx^{2n} \end{aligned}$$

In other words, the product of $a(x)$ and $b(x)$ is the polynomial

$$c(x) = c_0 + c_1x + \cdots + c_{2n}x^{2n}$$

whose k th coefficient (for any k from 0 to $2n$) is

$$c_k = \sum_{i+j=k} a_ib_j$$

This is the sum of all the a_ib_j for which $i + j = k$. Note that $\deg [a(x)b(x)] \leq \deg a(x) + \deg b(x)$.

If A is any ring, the symbol

$$A[x]$$

designates the set of all the polynomials in x whose coefficients are in A , with addition and multiplication of polynomials as we have just defined them.

Theorem 1 *Let A be a commutative ring with unity. Then $A[x]$ is a commutative ring with unity.*

PROOF: To prove this theorem, we must show systematically that $A[x]$ satisfies all the axioms of a

commutative ring with unity. Throughout the proof, let $a(x)$, $b(x)$, and $c(x)$ stand for the following polynomials:

$$\begin{aligned} a(x) &= a_0 + a_1x + \cdots + a_nx^n \\ b(x) &= b_0 + b_1x + \cdots + b_nx^n \\ \text{and} \quad c(x) &= c_0 + c_1x + \cdots + c_nx^n \end{aligned}$$

The axioms which involve only addition are easy to check: for example, addition is commutative because

$$\begin{aligned} a(x) + b(x) &= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n \\ &= (b_0 + a_0) + (b_1 + a_1)x + \cdots + (b_n + a_n)x^n \\ &= b(x) + a(x) \end{aligned}$$

The associative law of addition is proved similarly, and is left as an exercise. The zero polynomial has already been described, and the negative of $a(x)$ is

$$-a(x) = (-a_0) + (-a_1)x + \cdots + (-a_n)x^n$$

To prove that multiplication is associative requires some care. Let $b(x)c(x) = d(x)$, where $d(x) = d_0 + d_1x + \cdots + d_{2n}x^{2n}$. By the definition of polynomial multiplication, the k th coefficient of $b(x)c(x)$ is

$$d_k = \sum_{i+j=k} b_i c_j$$

Then $a(x)[b(x)c(x)] = a(x)d(x) = e(x)$, where $e(x) = e_0 + e_1x + \cdots + e_{3n}x^{3n}$. Now, the l th coefficient of $a(x)d(x)$ is

$$e_l = \sum_{h+k=l} a_h d_k = \sum_{h+k=l} a_h \left(\sum_{i+j=k} b_i c_j \right)$$

It is easy to see that the sum on the right consists of all the terms $a_h b_i c_j$ such that $h + i + j = l$. Thus,

$$e_l = \sum_{h+i+j=l} a_h b_i c_j$$

For each l from 0 to $3n$, e_l is the l th coefficient of $a(x)[b(x)c(x)]$.

If we repeat this process to find the l th coefficient of $[a(x) b(x)]c(x)$, we discover that it, too, is e_l . Thus,

$$a(x)[b(x)c(x)] = [a(x)b(x)]c(x)$$

To prove the distributive law, let $a(x)[b(x) + c(x)] = d(x)$ where $d(x) = d_0 + d_1x + \cdots + d_{2n}x^{2n}$. By the definitions of polynomial addition and multiplication, the k th coefficient $a(x)[b(x) + c(x)]$ is

$$\begin{aligned}
 d_k &= \sum_{i+j=k} a_i(b_j + c_j) = \sum_{i+j=k} (a_i b_j + a_i c_j) \\
 &= \sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_j
 \end{aligned}$$

But $\sum_{i+j=k} a_i b_j$ is exactly the k th coefficient of $a(x) b(x)$, and $\sum_{i+j=k} a_i c_j$ is the k th coefficient of $a(x)c(x)$, hence d_k is equal to the k th coefficient of $a(x) b(x) + a(x)c(x)$. This proves that

$$a(x)[b(x) + c(x)] = a(x)b(x) + a(x)c(x)$$

The commutative law of multiplication is simple to verify and is left to the student. Finally, the unity polynomial is the constant polynomial 1. ■

Theorem 2 *If A is an integral domain, then $A[x]$ is an integral domain.*

PROOF: If $a(x)$ and $b(x)$ are nonzero polynomials, we must show that their product $a(x) b(x)$ is not zero. Let a_n be the leading coefficient of $a(x)$, and b_m the leading coefficient of $b(x)$. By definition, $a_n \neq 0$, and $b_m \neq 0$. Thus $a_n b_m \neq 0$ because A is an integral domain. It follows that $a(x) b(x)$ has a nonzero coefficient (namely, $a_n b_m$), so it is not the zero polynomial. ■

If A is an integral domain, we refer to $A[x]$ as a *domain of polynomials*, because $A[x]$ is an integral domain. Note that by the preceding proof, if a_n and b_m are the leading coefficients of $a(x)$ and $b(x)$, then $a_n b_m$ is the leading coefficient of $a(x) b(x)$. Thus, $\deg a(x)b(x) = n + m$: *In a domain of polynomials $A[x]$, where A is an integral domain,*

$$\deg[a(x) \cdot b(x)] = \deg a(x) + \deg b(x)$$

In the remainder of this chapter we will look at a property of polynomials which is of special interest when all the coefficients lie in a field. Thus, from this point forward, let F be a field, and let us consider polynomials belonging to $F[x]$.

It would be tempting to believe that if F is a field then $F[x]$ also is a field. However, this is not so, for one can easily see that the multiplicative inverse of a polynomial is not generally a polynomial. Nevertheless, by [Theorem 2](#), $F[x]$ is an integral domain.

Domains of polynomials over a *field* do, however, have a very special property: any polynomial $a(x)$ may be divided by any nonzero polynomial $b(x)$ to yield a quotient $q(x)$ and a remainder $r(x)$. The remainder is either 0, or if not, its degree is less than the degree of the divisor $b(x)$. For example, x^2 may be divided by $x - 2$ to give a quotient of $x + 2$ and a remainder of 4:

$$\underbrace{x^2}_{a(x)} = \underbrace{(x-2)}_{b(x)} \underbrace{(x+2)}_{q(x)} + \underbrace{4}_{r(x)}$$

This kind of polynomial division is familiar to every student of elementary algebra. It is customarily set up as follows:

$$\begin{array}{rcl}
 \text{Divisor} \longrightarrow x-2 & \overline{\begin{array}{r} x+2 \\ x^2 \\ x^2-2x \\ 2x \\ 2x-4 \\ 4 \end{array}} & \longleftarrow \begin{array}{l} \text{Quotient } q(x) \\ \text{Dividend } b(x) \end{array} \\
 a(x) & & \\
 & & \longleftarrow \text{Remainder } r(x)
 \end{array}$$

The process of polynomial division is formalized in the next theorem.

Theorem 3: Division algorithm for polynomials *If $a(x)$ and $b(x)$ are polynomials over a field F , and $b(x) \neq 0$, there exist polynomials $q(x)$ and $r(x)$ over F such that*

$$a(x) = b(x)q(x) + r(x)$$

and

$$r(x) = 0 \quad \text{or} \quad \deg r(x) < \deg b(x)$$

PROOF: Let $b(x)$ remain fixed, and let us show that every polynomial $a(x)$ satisfies the following condition:

There exist polynomials $q(x)$ and $r(x)$ over F such that $a(x) = b(x)q(x) + r(x)$, and $r(x) = 0$ or $\deg r(x) < \deg b(x)$.

We will assume there are polynomials $a(x)$ which do *not* fulfill the condition, and from this assumption we will derive a contradiction. Let $a(x)$ be a polynomial of *lowest degree* which fails to satisfy the conditions. Note that $a(x)$ cannot be zero, because we can express 0 as $0 = b(x) \cdot 0 + 0$, whereby $a(x)$ would satisfy the conditions. Furthermore, $\deg a(x) \geq \deg b(x)$, for if $\deg a(x) < \deg b(x)$ then we could write $a(x) = b(x) \cdot 0 + a(x)$, so again $a(x)$ would satisfy the given conditions.

Let $a(x) = a_0 + \dots + a_n x^n$ and $b(x) = b_0 + \dots + b_m x^m$. Define a new polynomial

$$\begin{aligned}
 A(x) &= a(x) - \frac{a_n}{b_m} x^{n-m} b(x) \\
 &= a(x) - \left(b_0 \frac{a_n}{b_m} x^{n-m} + b_1 \frac{a_n}{b_m} x^{n-m+1} + \dots + b_m \frac{a_n}{b_m} x^{n-m+m} \right)
 \end{aligned} \tag{1}$$

This expression is the difference of two polynomials both of degree n and both having the same leading term $a_n x^n$. Because $a_n x^n$ cancels in the subtraction, $A(x)$ has degree *less than* n .

Remember that $a(x)$ is a polynomial of *least degree* which fails to satisfy the given condition; hence $A(x)$ *does satisfy* it. This means there are polynomials $p(x)$ and $r(x)$ such that

$$A(x) = b(x)p(x) + r(x)$$

where $r(x) = 0$ or $\deg r(x) < \deg b(x)$. But then

$$a(x) = A(x) + \frac{a_n}{b_m} x^{n-m} b(x) \quad \text{by Equation (1)}$$

$$= b(x)p(x) + r(x) + \frac{a_n}{b_m} x^{n-m} b(x)$$

$$= b(x) \left[p(x) + \frac{a_n}{b_m} x^{n-m} \right] + r(x)$$

If we let $p(x) + (a_n/b_m)x^{n-m}$ be renamed $q(x)$, then $a(x) = b(x)q(x) + r(x)$, so $a(x)$ fulfills the given condition. This is a contradiction, as required. ■

EXERCISES

A. Elementary Computation in Domains of Polynomials

REMARK ON NOTATION: In some of the problems which follow, we consider polynomials with coefficients in $\mathbf{z}_n$ for various n . To simplify notation, we denote the elements of $\mathbf{z}_n$ by $1, 2, \dots, n-1$ rather than the more correct $\overline{1}, \overline{2}, \dots, \overline{n-1}$.

1 Let $a(x) = 2x^2 + 3x + 1$ and $b(x) = x^3 + 5x^2 + x$. Compute $a(x) + b(x)$, $a(x) - b(x)$ and $a(x)b(x)$ in $\mathbf{z}[x]$, $\mathbf{z}_5[x]$, $\mathbf{z}_6[x]$, and $\mathbf{z}_7[x]$.

2 Find the quotient and remainder when $x^3 + x^2 + x + 1$ is divided by $x^2 + 3x + 2$ in $\mathbf{z}[x]$ and in $\mathbf{z}_5[x]$.

3 Find the quotient and remainder when $x^3 + 2$ is divided by $2x^2 + 3x + 4$ in $\mathbf{z}[x]$, in $\mathbf{z}_3[x]$, and in $\mathbf{z}_5[x]$.

We call $b(x)$ a *factor* of $a(x)$ if $a(x) = b(x)q(x)$ for some $q(x)$, that is, if the remainder when $a(x)$ is divided by $b(x)$ is equal to zero.

4 Show that the following is true in $A[x]$ for any ring A : For any odd n ,

(a) $x + 1$ is a factor of $x^n + 1$.

(b) $x + 1$ is a factor of $x^n + x^{n-1} + \dots + x + 1$.

5 Prove the following: In $\mathbf{z}_3[x]$, $x + 2$ is a factor of $x^m + 2$, for all m . In $\mathbf{z}_n[x]$, $x + (x - 1)$ is a factor of $x^m + (n - 1)$, for all m and n .

6 Prove that there is no integer m such that $3x^2 + 4x + m$ is a factor of $6x^4 + 50$ in $\mathbf{z}[x]$.

7 For what values of n is $x^2 + 1$ a factor of $x^5 + 5x + 6$ in $\mathbf{z}_n[x]$?

B. Problems Involving Concepts and Definitions

1 Is $x^8 + 1 = x^3 + 1$ in $\mathbf{z}_5[x]$? Explain your answer.

2 Is there any ring A such that in $A[x]$, some polynomial of degree 2 is equal to a polynomial of degree 4? Explain.

3 Write all the quadratic polynomials in $\mathbf{z}_5[x]$. How many are there? How many cubic polynomials are there in $\mathbf{z}_5[x]$? More generally, how many polynomials of degree m are there in $\mathbf{z}_n[x]$?

4 Let A be an integral domain; prove the following:

If $(x + 1)^2 = x^2 + 1$ in $A[x]$, then A must have characteristic 2.

If $(x + 1)^4 = x^4 + 1$ in $A[x]$, then A must have characteristic 2.

If $(x + 1)^6 = x^6 + 2x^3 + 1$ in $A[x]$, then A must have characteristic 3.

5 Find an example of each of the following in $\mathbf{z}_8[x]$: a divisor of zero, an invertible element. (Find nonconstant examples.)

6 Explain why x cannot be invertible in any $A[x]$, hence no domain of polynomials can ever be a field.

7 There are rings such as P_3 in which every element $\neq 0, 1$ is a divisor of zero. Explain why this cannot happen in any ring of polynomials $A[x]$, even when A is *not* an integral domain.

8 Show that in every $A[x]$, there are elements $\neq 0, 1$ which are not idempotent, and elements $\neq 0, 1$ which are not nilpotent.

C. Rings $A[x]$ Where A Is Not an Integral Domain

1 Prove: If A is not an integral domain, neither is $A[x]$.

2 Give examples of divisors of zero, of degrees 0, 1, and 2, in $\mathbf{z}_4[x]$.

3 In $\mathbf{z}_{10}[x]$, $(2x + 2)(2x + 2) = (2x + 2)(5x^3 + 2x + 2)$, yet $(2x + 2)$ cannot be canceled in this equation. Explain why this is possible in $\mathbf{z}_{10}[x]$, but not in $\mathbf{z}_5[x]$.

4 Give examples in $\mathbf{z}_4[x]$, in $\mathbf{z}_6[x]$, and in $\mathbf{Z}_9[x]$ of polynomials $a(x)$ and $b(x)$ such that $\deg a(x)b(x) < \deg a(x) + \deg b(x)$.

5 If A is an integral domain, we have seen that in $A[x]$,

$$\deg a(x)b(x) = \deg a(x) + \deg b(x)$$

Show that if A is *not* an integral domain, we can always find polynomials $a(x)$ and $b(x)$ such that $\deg a(x)b(x) < \deg a(x) + \deg b(x)$.

6 Show that if A is an integral domain, the only invertible elements in $A[x]$ are the constant polynomials with inverses in A . Then show that in $\mathbf{z}_4[x]$ there are invertible polynomials of all degrees.

7 Give all the ways of factoring x^2 into polynomials of degree 1 in $\mathbf{z}_9[x]$; in $\mathbf{z}_5[x]$. Explain the difference in behavior.

8 Find all the square roots of $x^2 + x + 4$ in $\mathbf{z}_5[x]$. Show that in $\mathbf{z}_8[x]$, there are infinitely many square roots of 1.

D. Domains $A[x]$ Where A Has Finite Characteristic

In each of the following, let A be an integral domain:

1 Prove that if A has characteristic p , then $A[x]$ has characteristic p .

2 Use part 1 to give an example of an infinite integral domain with finite characteristic.

3 Prove: If A has characteristic 3, then $x + 2$ is a factor of $x^m + 2$ for all m . More generally, if A has characteristic p , then $x + (p - 1)$ is a factor of $x^m + (p - 1)$ for all m .

4 Prove that if A has characteristic p , then in $A[x]$, $(x + c)^p = x^p + c^p$. (You may use essentially the same argument as in the proof of [Theorem 3, Chapter 20](#).)

5 Explain why the following “proof of part 4 is not valid: $(x + c)^p = x^p + c^p$ in $A[x]$ because $(a + c)^p = a^p + c^p$ for all $a, c \in A$. (Note the following example: in $\mathbb{Z}_2$, $a^2 + 1 = a^4 + 1$ for every a , yet $x^2 + 1 \neq x^4 + 1$ in $\mathbb{Z}_2[x]$.)

6 Use the same argument as in part 4 to prove that if A has characteristic p , then $[a(x) + b(x)]^p = a(x)^p + b(x)^p$ for any $a(x), b(x) \in A[x]$. Use this to prove:

$$(a_0 + a_1x + \cdots + a_nx^n)^p = a_0^p + a_1^p x^p + \cdots + a_n^p x^{np}$$

E. Subrings and Ideals in $A[x]$

1 Show that if B is a subring of A , then $B[x]$ is a subring of $A[x]$.

2 If B is an *ideal* of A , $B[x]$ is an ideal of $A[x]$.

3 Let S be the set of all the polynomials $a(x)$ in $A[x]$ for which every coefficient a_i for *odd* i is equal to zero. Show that S is a subring of $A[x]$. Why is the same not true when “odd” is replaced by “even”?

4 Let J consist of all the elements in $A[x]$ whose constant coefficient is equal to zero. Prove that J is an ideal of $A[x]$.

5 Let J consist of all the polynomials $a_0 + a_1x + \cdots + a_nx^n$ in $A[x]$ such that $a_0 + a_1 + \cdots + a_n = 0$. Prove that J is an ideal of $A[x]$.

6 Prove that the ideals in both parts 4 and 5 are *prime* ideals. (Assume A is an integral domain.)

F. Homomorphisms of Domains of Polynomials

Let A be an integral domain.

1 Let $h : A[x] \rightarrow A$ map every polynomial to its constant coefficient; that is,

$$h(a_0 + a_1x + \cdots + a_nx^n) = a_0$$

Prove that h is a homomorphism from $A[x]$ onto A , and describe its kernel.

2 Explain why the kernel of h in part 1 consists of all the products $xa(x)$, for all $a(x) \in A[x]$. Why is this the same as the principal ideal $\langle x \rangle$ in $A[x]$?

3 Using parts 1 and 2, explain why $A[x]/\langle x \rangle \cong A$.

4 Let $g : A[x] \rightarrow A$ send every polynomial to the sum of its coefficients. Prove that g is a surjective homomorphism, and describe its kernel.

5 If $c \in A$, let $h : A[x] \rightarrow A[x]$ be defined by $h(a(x)) = a(cx)$, that is,

$$h(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1cx + a_2c^2x^2 + \cdots + a_nc^nx^n$$

Prove that h is a homomorphism and describe its kernel.

6 If h is the homomorphism of part 5, prove that h is an automorphism (isomorphism from $A[x]$ to itself) iff c is invertible.

G. Homomorphisms of Polynomial Domains Induced by a Homomorphism of the Ring of Coefficients

Let A and B be rings and let $h : A \rightarrow B$ be a homomorphism with kernel K . Define $\bar{h} : A[x] \rightarrow B[x]$ by

$$\bar{h}(a_0 + a_1x + \cdots + a_nx^n) = h(a_0) + h(a_1)x + \cdots + h(a_n)x^n$$

(We say that $\bar{h}$ is *induced by* h .)

- 1 Prove that $\bar{h}$ is a homomorphism from $A[x]$ to $B[x]$.
- 2 Describe the kernel $\bar{K}$ of $\bar{h}$.
- # 3 Prove that $\bar{h}$ is surjective iff h is surjective.
- 4 Prove that $\bar{h}$ is injective iff h is injective.
- 5 Prove that if $a(x)$ is a factor of $b(x)$, then $\bar{h}(a(x))$ is a factor of $\bar{h}(b(x))$.
- 6 If $h : \mathbf{Z} \rightarrow \mathbf{Z}_n$ is the natural homomorphism, let $\bar{h} : \mathbf{Z}[x] \rightarrow \mathbf{Z}_n[x]$ be the homomorphism induced by h . Prove that $\bar{h}(a(x)) = 0$ iff n divides every coefficient of $a(x)$.
- 7 Let $\bar{h}$ be as in part 6, and let n be a prime. Prove that if $a(x)b(x) \in \ker \bar{h}$, then either $a(x)$ or $b(x)$ is in $\ker \bar{h}$. (HINT: Use [Exercise F2](#) of [Chapter 19](#).)

H. Polynomials in Several Variables

$A[x_1, x_2]$ denotes the ring of all the polynomials in *two letters* x_1 and x_2 with coefficients in A . For example, $x^2 - 2xy + y^2 + x - 5$ is a quadratic polynomial in $\mathbf{Q}[x, y]$. More generally, $A[x_1, \dots, x_n]$ is the ring of the polynomials in n *letters* $x_1, \dots, x_n$ with coefficients in A . Formally it is defined as follows: Let $A[x_1]$ be denoted by A_1 ; then $A_1[x_2]$ is $A[x_1, x_2]$. Continuing in this fashion, we may adjoin one new letter x_i at a time, to get $A[x_1, \dots, x_n]$.

- 1 Prove that if A is an integral domain, then $A[x_1, \dots, x_n]$ is an integral domain.
- 2 Give a reasonable definition of the *degree* of any polynomial $p(x, y)$ in $A[x, y]$ and then list all the polynomials of degree ≤ 3 in $\mathbf{Z}_3[x, y]$.

Let us denote an arbitrary polynomial $p(x, y)$ in $A[x, y]$ by $\sum a_{ij}x^i y^j$ where Σ ranges over *some* pairs i, j of nonnegative integers.

- 3 Imitating the definitions of sum and product of polynomials in $A[x]$, give a definition of sum and product of polynomials in $A[x, y]$.
- 4 Prove that $\deg a(x, y)b(x, y) = \deg a(x, y) + \deg b(x, y)$ if A is an integral domain.

I. Fields of Polynomial Quotients

Let A be an integral domain. By the closing part of [Chapter 20](#), every integral domain can be extended to a “field of quotients.” Thus, $A[x]$ can be extended to a field of polynomial quotients, which is denoted by $A(x)$. Note that $A(x)$ consists of all the fractions $a(x)/b(x)$ for $a(x)$ and $b(x) \neq 0$ in $A[x]$, and these fractions are added, subtracted, multiplied, and divided in the customary way.

- 1 Show that $A(x)$ has the same characteristic as A .
- 2 Using part 1, explain why there is an infinite field of characteristic p , for every prime p .
- 3 If A and B are integral domains and $h : A \rightarrow B$ is an isomorphism, prove that h determines an

isomorphism $\bar{h} : A(x) \rightarrow B(x)$.

J. Division Algorithm: Uniqueness of Quotient and Remainder

In the division algorithm, prove that $q(x)$ and $r(x)$ are uniquely determined. [HINT: Suppose $a(x) = b(x)q_1(x) + r_1(x) = b(x)q_2(x) + r_2(x)$, and subtract these two expressions, which are both equal to $a(x)$.]

FACTORING POLYNOMIALS

Just as every integer can be factored into primes, so every polynomial can be factored into “irreducible” polynomials which cannot be factored further. As a matter of fact, polynomials behave very much like integers when it comes to factoring them. This is especially true when the polynomials have all their coefficients in a *field*.

Throughout this chapter, we let F represent some field and we consider polynomials over F . It will be found that $F[x]$ has a considerable number of properties in common with $\mathbf{Z}$. To begin with, all the ideals of $F[x]$ are principal ideals, which was also the case for the ideals of $\mathbf{Z}$.

Note carefully that in $F[x]$, the principal ideal generated by a polynomial $a(x)$ consists of all the products $a(x)s(x)$ as $a(x)$ remains fixed and $s(x)$ ranges over all the members of $F[x]$.

Theorem 1 *Every ideal of $F[x]$ is principal.*

PROOF: Let J be any ideal of $F[x]$. If J contains nothing but the zero polynomial, J is the principal ideal generated by 0. If there are nonzero polynomials in J , let $b(x)$ be any polynomial of *lowest degree* in J . We will show that $J = \langle (b(x)) \rangle$, which is to say that every element of J is a polynomial multiple $b(x)q(x)$ of $b(x)$.

Indeed, if $a(x)$ is any element of J , we may use the division algorithm to write $a(x) = b(x)q(x) + r(x)$, where $r(x) = 0$ or $\deg r(x) < \deg b(x)$. Now, $r(x) = a(x) - b(x)q(x)$; but $a(x)$ was chosen in J , and $b(x) \in J$; hence $b(x)q(x) \in J$. It follows that $r(x)$ is in J .

If $r(x) \neq 0$, its degree is less than the degree of $b(x)$. But this is impossible because $b(x)$ is a polynomial of lowest degree in J . Therefore, of necessity, $r(x) = 0$.

Thus, finally, $a(x) = b(x)q(x)$; so every member of J is a multiple of $b(x)$, as claimed. ■

It follows that every ideal J of $F[x]$ is principal. In fact, as the proof above indicates, J is generated by any one of its members of lowest degree.

Throughout the discussion which follows, remember that we are considering polynomials in a fixed domain $F[x]$ where F is a *field*.

Let $a(x)$ and $b(x)$ be in $F[x]$. We say that $b(x)$ is a *multiple* of $a(x)$ if

$$b(x) = a(x)s(x)$$

for some polynomial $s(x)$ in $F[x]$. If $b(x)$ is a multiple of $a(x)$, we also say that $a(x)$ is a *factor* of $b(x)$, or

that $a(x)$ divides $b(x)$. In symbols, we write

$$a(x)|b(x)$$

Every nonzero constant polynomial divides every polynomial. For if $c \neq 0$ is constant and $a(x) = a_0 + \dots + a_n x^n$, then

$$a_0 + a_1 x + \dots + a_n x^n = c \left(\frac{a_0}{c} + \frac{a_1}{c} x + \dots + \frac{a_n}{c} x^n \right)$$

hence $c | a(x)$. A polynomial $a(x)$ is invertible iff it is a divisor of the unity polynomial 1. But if $a(x)b(x) = 1$, this means that $a(x)$ and $b(x)$ both have degree 0, that is, are constant polynomials: $a(x) = a$, $b(x) = b$, and $ab = 1$. Thus,

the invertible elements of $F[x]$ are all the nonzero constant polynomials.

A pair of nonzero polynomials $a(x)$ and $b(x)$ are called *associates* if they divide one another: $a(x)|b(x)$ and $b(x)|a(x)$. That is to say,

$$a(x) = b(x)c(x) \quad \text{and} \quad b(x) = a(x)d(x)$$

for some $c(x)$ and $d(x)$. If this happens to be the case, then

$$a(x) = b(x)c(x) = a(x)d(x)c(x)$$

hence $d(x)c(x) = 1$ because $F[x]$ is an integral domain. But then $c(x)$ and $d(x)$ are constant polynomials, and therefore $a(x)$ and $b(x)$ are constant multiples of each other. Thus, in $F[x]$,

$a(x)$ and $b(x)$ are associates iff they are constant multiples of each other.

If $a(x) = a_0 + \dots + a_n x^n$, the associates of $a(x)$ are all its nonzero constant multiples. Among these multiples is the polynomial

$$\frac{a_0}{a_n} + \frac{a_1}{a_n} x + \dots + x^n$$

which is equal to $(1/a_n)a(x)$, and which has 1 as its leading coefficient. Any polynomial whose leading coefficient is equal to 1 is called *monic*. Thus, *every nonzero polynomial $a(x)$ has a unique monic associate*. For example, the monic associate of $3 + 4x + 2x^3$ is $\frac{3}{2} + 2x + x^3$.

A polynomial $d(x)$ is called a *greatest common divisor* of $a(x)$ and $b(x)$ if $d(x)$ divides $a(x)$ and $b(x)$, and is a multiple of any other common divisor of $a(x)$ and $b(x)$; in other words,

- (i) $d(x)|a(x)$ and $d(x)|b(x)$, and
- (ii) For any $u(x)$ in $F[x]$, if $u(x)|a(x)$ and $u(x)|b(x)$, then $u(x)|d(x)$. According to this definition, two different gcd's of $a(x)$ and $b(x)$ divide each other, that is, are associates. Of all the possible gcd's of $a(x)$ and $b(x)$, we select the monic one, call it *the* gcd of $a(x)$ and $b(x)$, and denote it by $\gcd[a(x), b(x)]$.

It is important to know that any pair of polynomials always *has* a greatest common divisor.

Theorem 2 *Any two nonzero polynomials $a(x)$ and $b(x)$ in $F[x]$ have a gcd $d(x)$. Furthermore, $d(x)$ can be expressed as a “linear combination”*

$$d(x) = r(x)a(x) + s(x)b(x)$$

where $r(x)$ and $s(x)$ are in $F[x]$.

PROOF: The proof is analogous to the proof of the corresponding theorem for integers. If J is the set of all the linear combinations

$$u(x)a(x) + v(x)b(x)$$

as $u(x)$ and $v(x)$ range over $F[x]$, then J is an ideal of $F[x]$, say the ideal $\langle d(x) \rangle$ generated by $d(x)$. Now $a(x) = 1a(x) + 0b(x)$ and $b(x) = 0a(x) + 1b(x)$, so $a(x)$ and $b(x)$ are in J . But every element of J is a multiple of $d(x)$, so

$$d(x)|a(x) \quad \text{and} \quad d(x)|b(x)$$

If $k(x)$ is any common divisor of $a(x)$ and $b(x)$, this means there are polynomials $f(x)$ and $g(x)$ such that $a(x) = k(x)f(x)$ and $b(x) = k(x)g(x)$. Now, $d(x) \in J$, so $d(x)$ can be written as a linear combination

$$\begin{aligned} d(x) &= r(x)a(x) + s(x)b(x) \\ &= r(x)k(x)f(x) + s(x)k(x)g(x) \\ &= k(x)[r(x)f(x) + s(x)g(x)] \end{aligned}$$

hence $k(x)|d(x)$. This confirms that $d(x)$ is the gcd of $a(x)$ and $b(x)$. ■

Polynomials $a(x)$ and $b(x)$ in $F[x]$ are said to be *relatively prime* if their gcd is equal to 1. (This is equivalent to saying that their only common factors are constants in F .)

A polynomial $a(x)$ of positive degree is said to be *reducible over F* if there are polynomials $b(x)$ and $c(x)$ in $F[x]$, both of positive degree, such that

$$a(x) = b(x)c(x)$$

Because $b(x)$ and $c(x)$ both have positive degrees, and the sum of their degrees is $\deg a(x)$, *each has degree less than $\deg a(x)$* .

A polynomial $p(x)$ of positive degree in $F[x]$ is said to be *irreducible over F* if it cannot be expressed as the product of two polynomials of positive degree in $F[x]$. Thus, $p(x)$ is irreducible iff it is not reducible.

When we say that a polynomial $p(x)$ is irreducible, it is important that we specify *irreducible over the field F* . A polynomial may be irreducible over F , yet reducible over a larger field E . For example, $p(x) = x^2 + 1$ is irreducible over $\mathbb{R}$; but over $\mathbb{C}$ it has factors $(x + i)(x - i)$.

We next state the analogs for polynomials of Euclid's lemma and its corollaries. The proofs are almost identical to their counterparts in $\mathbb{Z}$; therefore they are left as exercises.

Euclid's lemma for polynomials *Let $p(x)$ be irreducible. If $p(x) | a(x)b(x)$, then $p(x) | a(x)$ or $p(x) | b(x)$.*

Corollary 1 *Let $p(x)$ be irreducible. If $p(x) | a_1(x)a_2(x) \cdots a_n(x)$, then $p(x) | a_i(x)$ for one of the factors $a_i(x)$ among $a_1(x), \dots, a_n(x)$.*

Corollary 2 *Let $q_1(x), \dots, q_r(x)$ and $p(x)$ be monic irreducible polynomials. If $p(x) | q_1(x) \cdots q_r(x)$, then $p(x)$ is equal to one of the factors $q_1(x), \dots, q_r(x)$.*

Theorem 3: Factorization into irreducible polynomials *Every polynomial $a(x)$ of positive degree in $F[x]$ can be written as a product*

$$a(x) = kp_1(x)p_2(x) \cdots p_r(x)$$

where k is a constant in F and $p_1(x), \dots, p_r(x)$ are monic irreducible polynomials of $F[x]$.

If this were not true, we could choose a polynomial $a(x)$ of lowest degree among those which cannot be factored into irreducibles. Then $a(x)$ is reducible, so $a(x) = b(x)c(x)$ where $b(x)$ and $c(x)$ have lower degree than $a(x)$. But this means that $b(x)$ and $c(x)$ can be factored into irreducibles, and therefore $a(x)$ can also.

Theorem 4: Unique factorization *If $a(x)$ can be written in two ways as a product of monic irreducibles, say*

$$a(x) = kp_1(x) \cdots p_r(x) = lq_1(x) \cdots q_s(x)$$

then $k = l$, $r = s$, and each $p_i(x)$ is equal to a $q_j(x)$.

The proof is the same, in all major respects, as the corresponding proof for $\mathbf{z}$; it is left as an exercise.

In the next chapter we will be able to improve somewhat on the last two results in the special cases of $\mathbf{R}[x]$ and $\mathbf{C}[x]$. Also, we will learn more about factoring polynomials into irreducibles.

EXERCISES

A. Examples of Factoring into Irreducible Factors

1 Factor $x^4 - 4$ into irreducible factors over $\mathbf{Q}$, over $\mathbf{R}$, and over $\mathbf{C}$.

2 Factor $x^6 - 16$ into irreducible factors over $\mathbf{Q}$, over $\mathbf{R}$, and over $\mathbf{C}$.

3 Find all the irreducible polynomials of degree ≤ 4 in $\mathbf{z}_2[x]$.

4 Show that $x^2 + 2$ is irreducible in $\mathbf{z}_5[x]$. Then factor $x^4 - 4$ into irreducible factors in $\mathbf{z}_5[x]$. (By Theorem 3, it is sufficient to search for monic factors.)

5 Factor $2x^3 + 4x + 1$ in $\mathbf{z}_5[x]$. (Factor it as in Theorem 3.)

6 In $\mathbf{z}_6[x]$, factor each of the following into two polynomials of degree 1 : x , $x + 2$, $x + 3$. Why is this possible?

B. Short Questions Relating to Irreducible Polynomials

Let F be a field. Explain why each of the following is true in $F[x]$:

1 Every polynomial of degree 1 is irreducible.

2 If $a(x)$ and $b(x)$ are distinct monic polynomials, they cannot be associates.

3 Any two distinct irreducible polynomials are relatively prime.

4 If $a(x)$ is irreducible, any associate of $a(x)$ is irreducible.

5 If $a(x) \neq 0$, $a(x)$ cannot be an associate of 0.

6 In $\mathbf{z}_p[x]$, every nonzero polynomial has exactly $p - 1$ associates.

7 $x^2 + 1$ is reducible in $\mathbf{z}_p[x]$ iff $p = a + b$ where $ab \equiv 1 \pmod{p}$.

C. Number of Irreducible Quadratics over a Finite Field

1 Without finding them, determine *how many* reducible monic quadratics there are in $\mathbf{z}_5[x]$. [HINT: Every reducible monic quadratic can be uniquely factored as $(x + a)(x + b)$.]

2 How many reducible quadratics are there in $\mathbf{z}_5[x]$? How many irreducible quadratics?

3 Generalize: How many irreducible quadratics are there over a finite field of n elements?

4 How many irreducible cubics are there over a field of n elements?

D. Ideals in Domains of Polynomials

Let F be a field, and let J designate any ideal of $F[x]$. Prove parts 1–4.

1 Any two generators of J are associates.

2 J has a *unique* monic generator $m(x)$. An arbitrary polynomial $a(x) \in F[x]$ is in J iff $m(x) \mid a(x)$.

3 J is a prime ideal iff it has an irreducible generator.

4 If $p(x)$ is irreducible, then $\langle p(x) \rangle$ is a *maximal* ideal of $F[x]$. (See [Chapter 18](#), [Exercise H5](#).)

5 Let S be the set of all polynomials $a_0 + a_1x + \dots + a_nx^n$ in $F[x]$ which satisfy $a_0 + a_1 + \dots + a_n = 0$. It has been shown ([Chapter 24](#), [Exercise E5](#)) that S is an ideal of $F[x]$. Prove that $x - 1 \in S$, and explain why it follows that $S = \langle -1 \rangle$.

6 Conclude from part 5 that $F[x]/\langle x - 1 \rangle \cong F$. (See [Chapter 24](#), [Exercise F4](#).)

7 Let $F[x, y]$ denote the domain of all the polynomials $\sum a_{ij}x^i y^j$ in *two* letters x and y , with coefficients in F . Let J be the ideal of $F[x, y]$ which contains all the polynomials whose constant coefficient is zero. Prove that J is not a principal ideal. Conclude that [Theorem 1](#) is not true in $F[x, y]$.

E. Proof of the Unique Factorization Theorem

1 Prove Euclid's lemma for polynomials.

2 Prove the two corollaries of Euclid's lemma.

3 Prove the unique factorization theorem for polynomials.

F. A Method for Computing the gcd

Let $a(x)$ and $b(x)$ be polynomials of positive degree. By the division algorithm, we may divide $a(x)$ by $b(x)$:

$$a(x) = b(x)q_1(x) + r_1(x)$$

1 Prove that every common divisor of $a(x)$ and $b(x)$ is a common divisor of $b(x)$ and $r_1(x)$.

It follows from part 1 that the gcd of $a(x)$ and $b(x)$ is the same as the gcd of $b(x)$ and $r_1(x)$. This procedure can now be repeated on $b(x)$ and $r_1(x)$; divide $b(x)$ by $r_1(x)$:

$$b(x) = r_1(x)q_2(x) + r_2(x)$$

Next

$$r_1(x) = r_2(x)q_3(x) + r_3(x)$$

$$\vdots$$

Finally,

$$r_{n-1}(x) = r_n(x)q_{n+1}(x) + 0$$

In other words, we continue to divide each remainder by the succeeding remainder. Since the remainders continually decrease in degree, there must ultimately be a zero remainder. But we have seen that

$$\gcd[a(x), b(x)] = \gcd[b(x), r_1(x)] = \cdots = \gcd[r_{n-1}(x), r_n(x)]$$

Since $r_n(x)$ is a divisor of $r_{n-1}(x)$, it must be the gcd of $r_n(x)$ and r_{n-1} . Thus,

$$r_n(x) = \gcd[a(x), b(x)]$$

This method is called the *euclidean algorithm* for finding the gcd.

2 Find the gcd of $x^3 + 1$ and $x^4 + x^3 + 2x^2 + x - 1$. Express this gcd as a linear combination of the two polynomials.

3 Do the same for $x^{24} - 1$ and $x^{15} - 1$.

4 Find the gcd of $x^3 + x^2 + x + 1$ and $x^4 + x^3 + 2x^2 + 2x$ in $\mathbb{Z}_3[x]$.

G. A Transformation of $F[x]$

Let G be the subset of $F[x]$ consisting of all polynomials whose constant term is nonzero. Let $h : G \rightarrow G$ be defined by

$$h(a_0 + a_1x + \cdots + a_nx^n) = a_n + a_{n-1}x + \cdots + a_0x^n$$

Prove parts 1–3:

1 h preserves multiplication, that is, $h[a(x)b(x)] = h[a(x)]h[b(x)]$.

2 h is injective and surjective and $h \circ h = \varepsilon$.

3 $a_0 + a_1x + \cdots + a_nx^n$ is irreducible iff $a_n + a_{n-1}x + \cdots + a_0x^n$ is irreducible.

4 Let $a_0 + a_1x + \cdots + a_nx^n = (b_0 + \cdots + b_mx^m)(c_0 + \cdots + c_qx^q)$. Factor

$$a_n + a_{n-1}x + \cdots + a_0x^n$$

5 Let $a(x) = a_0 + a_1x + \cdots + a_nx^n$ and $\hat{a}(x) = a_n + a_{n-1}x + \cdots + a_0x^n$. If $c \in F$, prove that $a(c) = 0$ iff $\hat{a}(1/c) = 0$.

SUBSTITUTION IN POLYNOMIALS

Up to now we have treated polynomials as formal expressions. If $a(x)$ is a polynomial over a field F , say

$$a(x) = a_0 + a_1x + \cdots + a_nx^n$$

this means that the coefficients $a_0, a_1, \dots, a_n$ are elements of the field F , while the letter x is a *placeholder* which plays no other role than to occupy a given position.

When we dealt with polynomials in elementary algebra, it was quite different. The letter x was called an *unknown* and was allowed to assume numerical values. This made $a(x)$ into a function having x as its independent variable. Such a function is called a *polynomial function*.

This chapter is devoted to the study of polynomial functions. We begin with a few careful definitions.

Let $a(x) = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial over F . If c is any element of F , then

$$a_0 + a_1c + \cdots + a_nc^n$$

is also an element of F , obtained by *substituting* c for x in the polynomial $a(x)$. This element is denoted by $a(c)$. Thus,

$$a(c) = a_0 + a_1c + \cdots + a_nc^n$$

Since we may substitute any element of F for x , we may regard $a(x)$ as a function from F to F . As such, it is called a *polynomial function on F* .

The difference between a polynomial and a polynomial function is mainly a difference of viewpoint. Given $a(x)$ with coefficients in F : if x is regarded merely as a placeholder, then $a(x)$ is a polynomial; if x is allowed to assume values in F , then $a(x)$ is a polynomial function. The difference is a small one, and we will not make an issue of it.

If $a(x)$ is a polynomial with coefficients in F , and c is an element of F such that

$$a(c) = 0$$

then we call c a *root* of $a(x)$. For example, 2 is a root of the polynomial $3x^2 + x - 14 \in \mathbb{R}[x]$, because $3 \cdot 2^2 + 2 - 14 = 0$.

There is an absolutely fundamental connection between *roots* of a polynomial and *factors* of that polynomial. This connection is explored in the following pages, beginning with the next theorem:

Let $a(x)$ be a polynomial over a field F .

Theorem 1 c is a root of $a(x)$ iff $x - c$ is a factor of $a(x)$.

PROOF: If $x - c$ is a factor of $a(x)$, this means that $a(x) = (x - c)q(x)$ for some $q(x)$. Thus, $a(c) = (c - c)q(c) = 0$, so c is a root of $a(x)$. Conversely, if c is a root of $a(x)$, we may use the division algorithm to divide $a(x)$ by $x - c$: $a(x) = (x - c)q(x) + r(x)$. The remainder $r(x)$ is either 0 or a polynomial of lower degree than $x - c$; but *lower degree than $x - c$* means that $r(x)$ is a constant polynomial: $r(x) = r \geq 0$. Then

$$0 = a(c) = (c - c) q(c) + r = 0 + r = r$$

Thus, $r = 0$, and therefore $x - c$ is a factor of $a(x)$. ■

[Theorem 1](#) tells us that if c is a root of $a(x)$, then $x - c$ is a *factor* of $a(x)$ (and vice versa). This is easily extended: if c_1 and c_2 are two roots of $a(x)$, then $x - c_1$ and $x - c_2$ are two factors of $a(x)$. Similarly, three roots give rise to three factors, four roots to four factors, and so on. This is stated concisely in the next theorem.

Theorem 2 If $a(x)$ has distinct roots $c_1, \dots, c_m$ in F , then $(x - c_1)(x - c_2) \cdots (x - c_m)$ is a factor of $a(x)$.

PROOF: To prove this, let us first make a simple observation: *if a polynomial $a(x)$ can be factored, any root of $a(x)$ must be a root of one of its factors*. Indeed, if $a(x) = s(x)t(x)$ and $a(c) = 0$, then $s(c)t(c) = 0$, and therefore either $s(c) = 0$ or $t(c) = 0$.

Let $c_1, \dots, c_m$ be distinct roots of $a(x)$. By [Theorem 1](#),

$$a(x) = (x - c_1) q_1(x)$$

By our observation in the preceding paragraph, c_2 must be a root of $x - c_1$ or of $q_1(x)$. It cannot be a root of $x - c_1$ because $c_2 - c_1 \neq 0$; so c_2 is a root of $q_1(x)$. Thus, $q_1(x) = (x - c_2) q_2(x)$, and therefore

$$a(x) = (x - c_1)(x - c_2) q_2(x)$$

Repeating this argument for each of the remaining roots gives us our result. ■

An immediate consequence is the following important fact:

Theorem 3 If $a(x)$ has degree n , it has at most n roots.

PROOF: If $a(x)$ had $n + 1$ roots $c_1, \dots, c_{n+1}$, then by [Theorem 2](#), $(x - c_1) \cdots (x - c_{n+1})$ would be a factor of $a(x)$, and the degree of $a(x)$ would therefore be at least $n + 1$. ■

It was stated earlier in this chapter that the difference between polynomials and polynomial

functions is mainly a difference of viewpoint. *Mainly*, but not entirely! Remember that two polynomials $a(x)$ and $b(x)$ are equal iff corresponding coefficients are equal, whereas two *functions* $a(x)$ and $b(x)$ are equal iff $a(x) = b(x)$ for every x in their domain. These two notions of equality do not always coincide!

For example, consider the following two polynomials in $\mathbb{Z}_5[x]$:

$$a(x) = x^5 + 1$$

$$b(x) = x - 4$$

You may check that $a(0) = b(0)$, $a(1) = b(1)$, ..., $a(4) = b(4)$; hence $a(x)$ and $b(x)$ are equal functions from $\mathbb{Z}_5$ to $\mathbb{Z}_5$. But as polynomials, $a(x)$ and $b(x)$ are quite distinct! (They do not even have the same degree.)

It is reassuring to know that this cannot happen when the field F is infinite. Suppose $a(x)$ and $b(x)$ are polynomials over a field F which has infinitely many elements. If $a(x)$ and $b(x)$ are equal as functions, this means that $a(c) = b(c)$ for every $c \in F$. Define the polynomial $d(x)$ to be the difference of $a(x)$ and $b(x)$: $d(x) = a(x) - b(x)$. Then $d(c) = 0$ for every $c \in F$. Now, if $d(x)$ were not the zero polynomial, it would be a polynomial (with some finite degree n) having *infinitely many roots*, and by [Theorem 3](#) this is impossible! Thus, $d(x)$ is the zero polynomial (all its coefficients are equal to zero), and therefore $a(x)$ is the same polynomial as $b(x)$. (They have the same coefficients.)

This tells us that if F is a field with infinitely many elements (such as $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$), there is no need to distinguish between polynomials and polynomial functions. The difference is, indeed, just a difference of viewpoint.

POLYNOMIALS OVER $\mathbb{Z}$ AND $\mathbb{Q}$

In scientific computation a great many functions can be approximated by polynomials, usually polynomials whose coefficients are integers or rational numbers. Such polynomials are therefore of great practical interest. It is easy to find the rational roots of such polynomials, and to determine if a polynomial over $\mathbb{Q}$ is irreducible over $\mathbb{Q}$. We will do these things next.

First, let us make an important observation:

Let $a(x)$ be a polynomial with rational coefficients, say

$$a(x) = \frac{k_0}{l_0} + \frac{k_1}{l_1}x + \cdots + \frac{k_n}{l_n}x^n$$

We may now factor out s from all but the first term to get

$$a(x) = \frac{1}{l_0 \cdots l_n} \underbrace{(k_0 l_1 \cdots l_n + \cdots + k_n l_0 \cdots l_{n-1} x^n)}_{b(x)}$$

The polynomial $b(x)$ has *integer coefficients*; and since it differs from $a(x)$ only by a constant factor, it has the same roots as $a(x)$. Thus, *for every polynomial with rational coefficients, there is a polynomial with integer coefficients having the same roots*. Therefore, for the present we will confine our attention to polynomials with integer coefficients. The next theorem makes it easy to find all the rational roots of such polynomials:

Let s/t be a rational number in simplest form (that is, the integers s and t do not have a common

factor greater than 1). Let $a(x) = a_0 + \dots + a_n x^n$ be a polynomial with integer coefficients.

Theorem 4 *If s/t is a root of $a(x)$, then $s|a_0$ and $t|a_n$.*

PROOF: If s/t is a root of $a(x)$, this means that

$$a_0 + a_1(s/t) + \dots + a_n(s^n/t^n) = 0$$

Multiplying both sides of this equation by t^n we get

$$a_0 t^n + a_1 s t^{n-1} + \dots + a_n s^n = 0 \quad (1)$$

We may now factor out s from all but the first term to get

$$-a_0 t^n = s(a_1 t^{n-1} + \dots + a_n s^{n-1})$$

Thus, $s | a_0 t^n$; and since s and t have no common factors, $s | a_0$. Similarly, in Equation (1), we may factor out t from all but the last term to get

$$t(a_0 t^{n-1} + \dots + a_{n-1} s^{n-1}) = -a_n s^n$$

Thus, $t | a_n s^n$; and since s and t have no common factors, $t | a_n$. ■

As an example of the way Theorem 4 may be used, let us find the rational roots of $a(x) = 2x^4 + 7x^3 + 5x^2 + 7x + 3$. Any rational root must be a fraction s/t where s is a factor of 3 and t is a factor of 2. The possible roots are therefore ± 1 , ± 3 , $\pm \frac{1}{2}$ and $\pm \frac{3}{2}$. Testing each of these numbers by direct substitution into the equation $a(x) = 0$, we find that $-\frac{1}{2}$ and -3 are roots.

Before going to the next step in our discussion we note a simple but fairly surprising fact.

Lemma *Let $a(x) = b(x)c(x)$, where $a(x)$, $b(x)$, and $c(x)$ have integer coefficients. If a prime number p divides every coefficient of $a(x)$, it either divides every coefficient of $b(x)$ or every coefficient of $c(x)$.*

PROOF: If this is not the case, let b_r be the first coefficient of $b(x)$ not divisible by p , and let c_t be the first coefficient of $c(x)$ not divisible by p . Now, $a(x) = b(x)c(x)$, so

$$a_{r+t} = b_0 c_{r+t} + \dots + b_r c_t + \dots + b_{r+t} c_0$$

Each term on the right, except $b_r c_t$ is a product $b_i c_j$ where either $i > r$ or $j > t$. By our choice of b_r and c_t , if $i > r$ then $p | b_i$, and $j > t$ then $p | c_j$. Thus, p is a factor of every term on the right with the possible exception of $b_r c_t$ but p is also a factor of a_{r+t} . Thus, p must be a factor of $b_r c_t$ hence of either b_r or c_t and this is impossible. ■

We saw (in the discussion immediately preceding Theorem 4) that any polynomial $a(x)$ with rational coefficients has a constant multiple $ka(x)$, with integer coefficients, which has the same roots as $a(x)$. We can go one better; let $a(x) \in \mathbb{Z}[x]$:

Theorem 5 *Suppose $a(x)$ can be factored as $a(x) = b(x)c(x)$, where $b(x)$ and $c(x)$ have rational coefficients. Then there are polynomials $B(x)$ and $C(x)$ with integer coefficients, which are constant*

multiples of $b(x)$ and $c(x)$, respectively, such that $a(x) = B(x)C(x)$.

PROOF. Let k and l be integers such that $kb(x)$ and $lc(x)$ have integer coefficients. Then $kla(x) = [kb(x)][lc(x)]$. By the lemma, each prime factor of kl may now be canceled with a factor of either $kb(x)$ or $lc(x)$. ■

Remember that a polynomial $a(x)$ of positive degree is said to be *reducible over F* if there are polynomials $b(x)$ and $c(x)$ in $F[x]$, both of positive degree, such that $a(x) = b(x)c(x)$. If there are *no* such polynomials, then $a(x)$ is *irreducible over F* .

If we use this terminology, [Theorem 5](#) states that *any polynomial with integer coefficients which is reducible over $\mathbb{Q}$ is reducible already over $\mathbb{Z}$* .

In Chapter 25 we saw that every polynomial can be factored into irreducible polynomials. In order to factor a polynomial completely (that is, into irreducibles), we must be able to recognize an irreducible polynomial when we see one! This is not always an easy matter. But there is a method which works remarkably well for recognizing when a polynomial is irreducible over $\mathbb{Q}$:

Theorem 6: Eisenstein's irreducibility criterion *Let*

$$a(x) = a_0 + a_1x + \cdots + a_nx^n$$

be a polynomial with integer coefficients. Suppose there is a prime number p which divides every coefficient of $a(x)$ except the leading coefficient a_n ; suppose p does not divide a_n and p^2 does not divide a_0 . Then $a(x)$ is irreducible over $\mathbb{Q}$.

PROOF: If $a(x)$ can be factored over $\mathbb{Q}$ as $a(x) = b(x)c(x)$, then by [Theorem 5](#) we may assume $b(x)$ and $c(x)$ have integer coefficients: say

$$b(x) = b_0 + \cdots + b_kx^k \quad \text{and} \quad c(x) = c_0 + \cdots + c_mx^m$$

Now, $a_0 = b_0c_0$; p divides a_0 but p^2 does not, so only *one* of b_0, c_0 is divisible by p . Say $p \mid c_0$ and $p \nmid b_0$. Next, $a_n = b_kc_m$ and $p \nmid a_n$, so $p \nmid c_m$.

Let s be the smallest integer such that $p \nmid c_s$. We have

$$a_s = b_0c_s + b_1c_{s-1} + \cdots + b_sc_0$$

and by our choice of c_s , every term on the right except b_0c_s is divisible by p . But a_s *also* is divisible by p , and therefore b_0c_s must be divisible by p . This is impossible because $p \nmid b_0$ and $p \nmid c_s$. Thus, $a(x)$ cannot be factored. ■

For example, $x^3 + 2x^2 + 4x + 2$ is irreducible over $\mathbb{Q}$ because $p = 2$ satisfies the conditions of Eisenstein's criterion.

POLYNOMIALS OVER $\mathbb{R}$ AND $\mathbb{C}$

One of the most far-reaching theorems of classical mathematics concerns polynomials with complex coefficients. It is so important in the frame work of traditional algebra that it is called the *fundamental theorem of algebra*. It states the following:

Every nonconstant polynomial with complex coefficients has a complex root.

(The proof of this theorem is based upon techniques of calculus and can be found in most books on complex analysis. It is omitted here.)

It follows immediately that *the irreducible polynomials in $\mathbb{C}[x]$ are exactly the polynomials of degree 1*. For if $a(x)$ is a polynomial of degree greater than 1 in $\mathbb{C}[x]$, then by the fundamental theorem of algebra it has a root c and therefore a factor $x - c$.

Now, every polynomial in $\mathbb{C}[x]$ can be factored into irreducibles. Since the irreducible polynomials are all of degree 1, it follows that if $a(x)$ is a polynomial of degree n over $\mathbb{C}$, it can be factored into

$$a(x) = k(x - c_1)(x - c_2) \cdots (x - c_n)$$

In particular, *if $a(x)$ has degree n it has n (not necessarily distinct) complex roots $c_1 \dots c_n$* .

Since every real number a is a complex number ($a = a + 0i$), what has just been stated applies equally to polynomials with real coefficients. Specifically, if $a(x)$ is a polynomial of degree n with real coefficients, it can be factored into $a(x) = k(x - c_1) \cdots (x - c_n)$, where $c_1, \dots, c_n$ are complex numbers (some of which may be real).

For our closing comments, we need the following lemma:

Lemma Suppose $a(x) \in \mathbb{R}[x]$. If $a + bi$ is a root of $a(x)$, so is $a - bi$.

PROOF: Remember that $a - bi$ is called the conjugate of $a + bi$. If r is any complex number, we write $\bar{r}$ for its conjugate. It is easy to see that the function $f(r) = \bar{r}$ is a homomorphism from $\mathbb{C}$ to $\mathbb{C}$ (in fact, it is an isomorphism). For every *real* number a , $f(a) = a$. Thus, if $a(x)$ has real coefficients, then $f(a_0 + a_1r + \cdots + a_nr^n) = a_0 + a_1\bar{r} + \cdots + a_n\bar{r}^n$. Since $f(0) = 0$, it follows that if r is a root of $a(x)$, so is $\bar{r}$. ■

Now let $a(x)$ be any polynomial with real coefficients, and let $r = a + bi$ be a complex root of $a(x)$. Then $\bar{r}$ is also a root of $a(x)$, so

$$(x - r)(x - \bar{r}) = x^2 - 2ax + (a^2 + b^2)$$

and this is a quadratic polynomial *with real coefficients!* We have thus shown that *any polynomial with real coefficients can be factored into polynomials of degree 1 or 2 in $\mathbb{R}[x]$* . In particular, the irreducible polynomials of the linear polynomials and $[x]$ are the linear polynomials and the irreducible quadratics (that is, the $ax^2 + bx + c$ where $b^2 - 4ac < 0$).

EXERCISES

A. Finding Roots of Polynomials over Finite Fields

In order to find a root of $a(x)$ in a finite field F , the simplest method (if F is small) is to test every element of F by substitution into the equation $a(x) = 0$.

1 Find all the roots of the following polynomials in $\mathbb{Z}_5[x]$, and factor the polynomials:

$$x^3 + x^2 + x + 1; \quad 3x^4 + x^2 + 1; \quad x^5 + 1; \quad x^4 + 1; \quad x^4 + 4$$

2 Use Fermat's theorem to find all the roots of the following polynomials in $\mathbb{Z}_7[x]$:

$$x^{100} - 1; \quad 3x^{98} + x^{19} + 3; \quad 2x^{74} - x^{55} + 2x + 6$$

3 Using Fermat's theorem, find polynomials of degree ≤ 6 which determine the same functions as the following polynomials in $\mathbb{Z}_7[x]$:

$$3x^{75} - 5x^{54} + 2x^{13} - x^2; \quad 4x^{108} + 6x^{101} - 2x^{81}; \quad 3x^{103} - x^{73} + 3x^{55} - x^{25}$$

4 Explain why every polynomial in $\mathbb{Z}_p[x]$ has the same roots as a polynomial of degree $< p$.

B. Finding Roots of Polynomials over $\mathbb{Q}$

1 Find all the rational roots of the following polynomials, and factor them into irreducible polynomials in $\mathbb{Q}[x]$:

$$9x^3 + 18x^2 - 4x - 8; \quad 4x^3 - 3x^2 - 8x + 6;$$

$$2x^4 + 3x^3 - 8x - 12; \quad 6x^4 - 7x^3 + 8x^2 - 7x + 2$$

2 Factor each of the preceding polynomials in $\mathbb{R}[x]$ and in $\mathbb{C}[x]$.

3 Find associates with integer coefficients for each of the following polynomials:

$$x^3 + \frac{3}{2}x^2 - \frac{4}{9}x - \frac{2}{3}; \quad \frac{1}{2}x^3 - \frac{1}{4}x^2 - \frac{1}{2}x + \frac{1}{4}; \quad \sqrt{3}x^3 + \frac{1}{\sqrt{3}}x^2 - \sqrt{3}x - \frac{1}{\sqrt{3}}$$

4 Find all the rational roots of the polynomials in part 3 and factor them over $\mathbb{R}$.

5 Does $2x^4 + 3x^2 - 2$ have any rational roots? Can it be factored into two polynomials of lower degree in $\mathbb{Q}[x]$? Explain.

C. Short Questions Relating to Roots

Let F be a field.

Prove that parts 1–3 are true in $F[x]$.

1 The remainder of $p(x)$, when divided by $x - c$, is $p(c)$.

2 $(x - c) \mid (p(x) - p(c))$.

3 Every polynomial has the same roots as any of its associates.

4 If $a(x)$ and $b(x)$ have the same roots in F , are they necessarily associates? Explain.

5 Prove: If $a(x)$ is a monic polynomial of degree n , and $a(x)$ has n roots $c_1, \dots, c_n \in F$, then $a(x) = (x - c_1) \cdots (x - c_n)$.

6 Suppose $a(x)$ and $b(x)$ have degree $< n$. If $a(c) = b(c)$ for n values of c , prove that $a(x) = b(x)$.

7 There are infinitely many irreducible polynomials in $\mathbb{Z}_5[x]$.

8 How many roots does $x^2 - x$ have in $\mathbb{Z}_{10}$? In $\mathbb{Z}_{11}$? Explain the difference.

D. Irreducible Polynomials in $\mathbb{Q}[x]$ by Eisenstein's Criterion (and Variations on the Theme)

1 Show that each of the following polynomials is irreducible over $\mathbb{Q}$:

$$3x^4 - 8x^3 + 6x^2 - 4x + 6; \quad \frac{2}{3}x^5 + \frac{1}{2}x^4 - 2x^2 + \frac{1}{2};$$

$$\frac{1}{5}x^4 - \frac{1}{3}x^3 - \frac{2}{3}x + 1; \quad \frac{1}{2}x^4 + \frac{4}{3}x^3 - \frac{2}{3}x^2 + 1$$

2 It often happens that a polynomial $a(y)$, as it stands, does not satisfy the conditions of Eisenstein's criterion, but with a simple change of variable $y = x + c$, it does. It is important to note that if $a(x)$ can be factored into $p(x)q(x)$, then certainly $a(x + c)$ can be factored into $p(x + c)q(x + c)$. Thus, the irreducibility of $a(x + c)$ implies the irreducibility of $a(x)$.

(a) Use the change of variable $y = x + 1$ to show that $x^4 + 4x + 1$ is irreducible in $\mathbb{Q}[x]$. [In other words, test $(x + 1)^4 + 4(x + 1) + 1$ by Eisenstein's criterion.]

(b) Find an appropriate change of variable to prove that the following are irreducible in $\mathbb{Q}[x]$:

$$x^4 + 2x^2 - 1; \quad x^3 - 3x + 1; \quad x^4 + 1; \quad x^4 - 10x^2 + 1$$

3 Prove that for any prime p , $x^{p-1} + x^{p-2} + \dots + x + 1$ is irreducible in $\mathbb{Q}[x]$. [HINT: By elementary algebra,

$$(x - 1)(x^{p-1} + x^{p-2} + \dots + x + 1) = x^p - 1$$

hence

$$x^{p-1} + x^{p-2} + \dots + x + 1 = \frac{x^p - 1}{x - 1}$$

Use the change of variable $y = x + 1$, and expand by the binomial theorem.

4 By [Exercise G3](#) of [Chapter 25](#), the function

$$h(a_0 + a_1x + \dots + a_nx^n) = a_n + a_{n-1}x + \dots + a_0x^n$$

restricted to polynomials with nonzero constant term matches irreducible polynomials with irreducible polynomials. Use this fact to state a dual version of Eisenstein's irreducibility criterion.

5 Use part 4 to show that each of the following polynomials is irreducible in $\mathbb{Q}[x]$:

$$6x^4 + 4x^3 - 6x^2 - 8x + 5; \quad x^4 - \frac{1}{2}x^2 + \frac{3}{2}x - \frac{4}{3}; \quad x^3 + \frac{1}{2}x^2 - \frac{3}{2}x + \frac{6}{5}$$

E. Irreducibility of Polynomials of Degree ≤ 4

1 Let F be any field. Explain why, if $a(x)$ is a quadratic or cubic polynomial in $F[x]$, $a(x)$ is irreducible in $F[x]$ iff $a(x)$ has no roots in F .

2 Prove that the following polynomials are irreducible in $\mathbb{Q}[x]$:

$$\frac{1}{2}x^3 + 2x - \frac{3}{2}; \quad 3x^2 - 2x - 4; \quad x^3 + x^2 + \frac{3}{2}x + \frac{1}{2}; \quad x^3 + \frac{1}{2}; \quad x^2 - \frac{5}{2}x + \frac{3}{2}$$

3 Suppose a monic polynomial $a(x)$ of degree 4 in $F[x]$ has no roots in F . Then $a(x)$ is reducible iff it is a

product of two quadratics $x^2 + ax + b$ and $x^2 + cx + d$, that is, iff

$$a(x) = x^4 + (a + c)x^3 + (ac + b + d)x^2 + (bc + ad)x + bd$$

If the coefficients of $a(x)$ cannot be so expressed (in terms of *any* $a, b, c, d \in F$) then $a(x)$ must be irreducible.

Example $a(x) = x^4 + 2x^3 + x + 1$; then $bd = 1$, so $b = d = \pm 1$; thus, $bc + ad = \pm(a + c)$, but $a + c = 2$ and $bc + ad = 1$; which is impossible.

Prove that the following polynomials are irreducible in $\mathbb{Q}[x]$ (use [Theorem 5](#), searching only for integer values of a, b, c, d):

$$x^4 - 5x^2 + 1; \quad 3x^4 - x^2 - 2; \quad x^4 + x^3 + 3x + 1$$

4 Prove that the following polynomials are irreducible in $\mathbb{Z}_5[x]$:

$$2x^3 + x^2 + 4x + 1; \quad x^4 + 2; \quad x^4 + 4x^2 + 2; \quad x^4 + 1$$

F. Mapping onto $\mathbb{Z}_n$ to Determine Irreducibility over $\mathbb{Q}$

If $h: \mathbb{Z} \rightarrow \mathbb{Z}_n$ is the natural homomorphism, let $\bar{h}: \mathbb{Z}[x] \rightarrow \mathbb{Z}_n[x]$ be defined by

$$\bar{h}(a_0 + a_1x + \dots + a_nx^n) = h(a_0) + h(a_1)x + \dots + h(a_n)x^n$$

In [Chapter 24, Exercise G](#), it is proved that $\bar{h}$ is a homomorphism. Assume this fact and prove:

1 If $\bar{h}(a(x))$ is irreducible in $\mathbb{Z}_n[x]$ and $a(x)$ is monic, then $a(x)$ is irreducible in $\mathbb{Z}[x]$.

2 $x^4 + 10x^3 + 7$ is irreducible in $\mathbb{Q}[x]$ by using the natural homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_5$.

3 The following are irreducible in $\mathbb{Q}[x]$ (find the right value of n and use the natural homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_n$):

$$x^4 - 10x^2 + 1; \quad x^4 + 7x^3 + 14x^2 + 3; \quad x^5 + 1$$

G. Roots and Factors in $A[x]$ When A Is an Integral Domain

It is a useful fact that [Theorems 1, 2, and 3](#) are still true in $A[x]$ when A is not a field, but merely an integral domain. The proof of [Theorem 1](#) must be altered a bit to avoid using the division algorithm. We proceed as follows:

If $a(x) = a_0 + a_1x + \dots + a_nx^n$ and c is a root of $a(x)$, consider

$$a(x) - a(c) = a_1(x - c) + a_2(x^2 - c^2) + \dots + a_n(x^n - c^n)$$

1 Prove that for $k = 1, \dots, n$:

$$a_k(x^k - c^k) = a_k(x - c)(x^{k-1} + x^{k-2}c + \dots + c^{k-1})$$

2 Conclude from part 1 that $a(x) - a(c) = (x - c)q(x)$ for some $q(x)$.

3 Complete the proof of [Theorem 1](#), explaining why this particular proof is valid when A is an integral domain, not necessarily a field.

4 Check that [Theorems 2](#) and [3](#) are true in $A[x]$ when A is an integral domain.

H. Polynomial Interpolation

One of the most important applications of polynomials is to problems where we are given several values of x (say, $x = a_0, a_1, \dots, a_n$) and corresponding values of y (say, $y = b_0, b_1, \dots, b_n$), and we need to find a function $y = f(x)$ such that $f(a_0) = b_0, f(a_1) = b_1, \dots, f(a_n) = b_n$. The simplest and most useful kind of function for this purpose is a polynomial function of the lowest possible degree.

We now consider a commonly used technique for constructing a polynomial $p(x)$ of degree n which assumes given values $b_0, b_1, \dots, b_n$ at given points $a_0, a_1, \dots, a_n$. That is,

$$p(a_0) = b_0, p(a_1) = b_1, \dots, p(a_n) = b_n$$

First, for each $i = 0, 1, \dots, n$, let

$$q_i(x) = (x - a_0) \cdots (x - a_{i-1})(x - a_{i+1}) \cdots (x - a_n)$$

1 Show that $q_i(a_j) = 0$ for $j \neq i$, and $q_i(a_i) \neq 0$.

Let $q_i(a_i) = c_i$, and define $p(x)$ as follows:

$$p(x) = \sum_{i=0}^n \frac{b_i}{c_i} q_i(x) = \frac{b_0}{c_0} q_0(x) + \cdots + \frac{b_n}{c_n} q_n(x)$$

(This is called the *Lagrange interpolation formula*.)

2 Explain why $p(a_0) = b_0, p(a_1) = b_1, \dots, p(a_n) = b_n$.

3 Prove that there is one and *only* one polynomial $p(x)$ of degree $\leq n$ such that $p(a_0) = b_0, \dots, p(a_n) = b_n$.

4 Use the Lagrange interpolation formula to prove that if F is a finite field, every function from F to F is equal to a polynomial function. (In fact, the degree of this polynomial is less than the number of elements in F .)

5 If $t(x)$ is any polynomial in $F[x]$, and $a_0, \dots, a_n \in F$, the unique polynomial $p(x)$ of degree $\leq n$ such that $p(a_0) = t(a_0), \dots, p(a_n) = t(a_n)$ is called the *Lagrange interpolator* for $t(x)$ and $a_0, \dots, a_n$. Prove that the remainder, when $t(x)$ is divided by $(x - a_0)(x - a_1) \cdots (x - a_n)$, is the Lagrange interpolator.

I. Polynomial Functions over a Finite Field

1 Find three polynomials in $\mathbb{Z}_5[x]$ which determine the same function as

$$x^2 - x + 1$$

2 Prove that $x^p - x$ has p roots in $\mathbb{Z}_p[x]$, for any prime p . Draw the conclusion that in $\mathbb{Z}_p[x]$, $x^p - x$ can be factored as

$$x^p - x = x(x - 1)(x - 2) \cdots [x - (p - 1)]$$

3 Prove that if $a(x)$ and $b(x)$ determine the same function in $\mathbb{Z}_p[x]$, then

$$(x^p - x) | (a(x) - b(x))$$

In the next four parts, let F be any finite field.

4 Let $a(x)$ and $b(x)$ be in $F[x]$. Prove that if $a(x)$ and $b(x)$ determine the same function, and if the number of elements in F exceeds the degree of $a(x)$ as well as the degree of $b(x)$, then $a(x) = b(x)$.

5 Prove: The set of all $a(x)$ which determine the zero function is an ideal of $F[x]$. What is its generator?

6 Let $\mathcal{F}(F)$ be the ring of all functions from F to F , defined in the same way as $\mathcal{F}(\mathbb{R})$. Let $h: F[x] \rightarrow \mathcal{F}(F)$ send every polynomial $a(x)$ to the polynomial function which it determines. Show that h is a homomorphism from $F[x]$ onto $\mathcal{F}(F)$. (NOTE: To show that h is *onto*, use [Exercise H4](#).)

7 Let $F = \{c_1, \dots, c_n\}$ and $p(x) = (x - c_1) \cdots (x - c_n)$. Prove that

$$F[x]/\langle p(x) \rangle \cong \mathcal{F}(F)$$