22.7 Factorization of polynomials in theory

In Chapter 8 we proved that every integer $n \geq 2$ has a unique factorization into primes. In this section we investigate the analogous result for $F[x]$.

First, we note that the existence of non-zero constant polynomials allows trivial factorizations of any polynomial. This is because a non-zero constant α has an inverse β in F, which is also its inverse in $F[x]$, so that

$$f(x) = \alpha \times (\beta f(x))$$

is a factorization of $f(x)$ in $F[x]$. Clearly, we wish to exclude such trivial factorizations from the theory. For this reason, we define a polynomial $f(x)$ in $F[x]$ to be **irreducible** if it is not a constant polynomial and if, whenever

$$f(x) = g(x)h(x) \quad \text{in } F[x],$$

then either $g(x)$ or $h(x)$ is a constant polynomial. The irreducible polynomials play the same rôle in $F[x]$ as do the primes in $\mathbb{Z}$.

The proof of the following theorem follows the same lines as the proof of Theorem 1.8.2, and it will be presented as a sequence of Exercises.

Theorem 22.7 Any non-constant polynomial $f(x)$ in $F[x]$ can be expressed as a product of irreducible polynomials. If there are two such factorizations

$$f(x) = g_1(x)g_2(x)\cdots g_r(x) = h_1(x)h_2(x)\cdots h_s(x)$$

then $r = s$ and we can rearrange the order of factors so that $g_i(x)$ is a constant multiple of $h_i(x)$ $(1 \leq i \leq r)$; that is, $g_i(x) = \alpha_i h_i(x)$ for some non-zero constant polynomial α_i. □

Exercises 22.7

(All polynomials in Exercises 1–5 belong to $F[x]$, where F is a field.)

1 Show that if $r(x)$ is not a constant polynomial then

$$\deg r(x)s(x) > \deg s(x).$$

2 (Existence of factorization.) Show that, if $f(x)$ is a non-constant polynomial, then either $f(x)$ is irreducible or $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are non-constant polynomials whose degrees are less than that of $f(x)$. Hence prove the first assertion of Theorem 22.7 by induction on the degree of $f(x)$.

3 Show that if 1 is a gcd of $r(x)$ and $s(x)$, and $r(x)$ is a divisor of $s(x)t(x)$, then $r(x)$ is a divisor of $t(x)$.

4 Show that if $r(x)$ is irreducible and $r(x)$ is a divisor of $s_1(x)s_2(x)\ldots s_k(x)$, then $r(x)$ is a divisor of $s_i(x)$ for some i in the range $1 \leq i \leq k$.

5 (Uniqueness of factorization.) Prove the uniqueness assertion in Theorem 22.7.

6 Verify that in $\mathbb{Z}_{15}[x]$

$$(x+1)(x+14) = (x+4)(x+11).$$

What is the significance of this result in relation to the theory developed above?

However, when the degree of the polynomial is four or more, other methods may be required.

Example Find the irreducible factors of $x^4 + 1$ in $\mathbb{Z}_3[x]$.

Solution First we use the factor theorem to look for linear factors. Let $f(x) = x^4 + 1$; then

$$f(0) = 0^4 + 1 = 1, \qquad f(1) = 1^4 + 1 = 2, \qquad f(2) = 2^4 + 1 = 2.$$

So there are no linear factors. The only possibility remaining is a factorization into two quadratics given by

$$x^4 + 1 = (x^2 + Ax + B)(x^2 + Cx + D),$$

with A, B, C, D in $\mathbb{Z}_3$. By equating coefficients of corresponding powers of x we obtain the equations

$$\begin{aligned} &\text{(i)} && A + C && = 0, \\ &\text{(ii)} && B + D + AC && = 0, \\ &\text{(iii)} && AD + BC && = 0, \\ &\text{(iv)} && BD && = 1. \end{aligned}$$

It follows from (i) that $A = -C$ and from (iv) that $B = D$. (Why?) Taking $B = D = 1$ we obtain $AC = 1$ in (ii), which contradicts (i). Taking $B = D = 2$ we obtain $AC = 2$; then $A = 1$, $C = 2$ is a solution. Hence the required factorization is

$$x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2). \qquad \square$$

Of course, the method given in the example is very inefficient in most cases. A great deal of work has been done on the development of efficient algorithms for finding the irreducible factors of polynomials, but many of the best methods are beyond the scope of this book.

Exercises 22.8

1 Find the irreducible factors of

(i) $x^2 + 1$ in $\mathbb{Z}_5[x]$;

(ii) $x^3 + 5x^2 + 5$ in $\mathbb{Z}_{11}[x]$;

(iii) $x^4 + 3x^3 + x + 1$ in $\mathbb{Z}_5[x]$.

2 Find all the monic irreducible quadratics in $\mathbb{Z}_3[x]$.

3 Show that the number of monic irreducible cubics in $\mathbb{Z}_p[x]$ is $\frac{1}{3}p(p^2 - 1)$, and list them when $p = 2$.

4 Let $f(x) = f_n x^n + f_{n-1}x^{n-1} + \cdots + f_0$ be a polynomial of degree n in $F[x]$, and let $\alpha \in F$. Explain how $f(\alpha)$ can be evaluated by means of the recursion

$$f_0(\alpha) = f_n, \qquad f_i(\alpha) = \alpha f_{i-1}(\alpha) + f_{n-i} \quad (1 \leq i \leq n).$$

What is the number of multiplications required by this method? (It is sometimes known as *Horner's method*.)

5 Suppose that $f(x)$ and α are as in Ex. 4, and $f(\alpha)$ is evaluated by computing each term $f_i\alpha^i$ individually $(0 \leq i \leq n)$. Find the approximate number of multiplications required if the methods for calculating α^i given in Section 14.7 are used.

22.9 Miscellaneous Exercises

1 Investigate the structures of the groups of invertible elements of $\mathbb{Z}_{15}$ and $\mathbb{Z}_{16}$.

2 Factorize the following into irreducible polynomials in $\mathbb{Z}_5[x]$:

(i) $x^4 + 4$, (ii) $x^4 + 3x^3 + 2x + 4$.

3 Find an irreducible polynomial of degree 4 in $\mathbb{Z}_5[x]$.

4 Show that if the integer r is a root of the equation $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$ in $\mathbb{Z}[x]$ then r is a divisor of a_0.

5 Find the monic gcd of the polynomials $x^3 + 1$ and $x^4 + x^2 + 1$ in $\mathbb{Z}_3[x]$, and in $\mathbb{Z}_7[x]$.

6 Prove that the multiplication in a ring R is commutative if and only if

$$(a + b)^2 = a^2 + 2ab + b^2$$

for all a, b in R.

7 Show by means of an example that if m is not a prime then a quadratic equation in $\mathbb{Z}_m[x]$ may have more than two roots in $\mathbb{Z}_m$.

8 Let p be a prime. Prove that the polynomials $f(x) = x^p$ and $g(x) = x$ in $\mathbb{Z}_p[x]$ define the same function from $\mathbb{Z}_p$ to itself.

9 Let Φ denote the set of all functions f from $\mathbb{Z}$ to itself, and define the addition and multiplication of such functions by the rules $(f + g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)g(x)$. Which of the following subsets of Φ are rings?

(i) The functions satisfying $f(0) = 0$.

(ii) The functions satisfying $f(0) \neq 0$.

(iii) The functions satisfying $f(0) = f(1)$.

(iv) The functions satisfying $f(x) = f(x + 1)$ for all x in $\mathbb{Z}$.

10 Show that when $a \neq 0$ the polynomial $ax^2 + bx + c$ is irreducible in $\mathbb{Z}_p[x]$ (where p is a prime) if and only if $b^2 - 4ac$ is not a square in $\mathbb{Z}_p$.

11 Find the monic gcd in $\mathbb{Z}[x]$ of

$$x^6 + 6x^5 + 8x^4 + x^3 + 4x^2 + 2x + 8$$

and

$$x^4 + 5x^3 + 6x^2 + 9x + 4.$$

12 Let ω denote the complex number $e^{2\pi i/3}$. Show that $1 + \omega + \omega^2 = 0$ and deduce that the set of complex numbers of the form $m + n\omega$ ($m, n \in \mathbb{Z}$) is a ring. (You need not check properties which follow directly from the standard properties of complex numbers.)

13 Describe the group of invertible elements of the ring constructed in the previous exercise.

14 Let F be a field with an infinite number of elements. Show that if $f(x)$ and $g(x)$ are polynomials in $F[x]$ which induce the same function from F to itself, then $f(x) = g(x)$.

15 Let $f(x) = f_0 + f_1x + \cdots + f_nx^n$ be a polynomial with coefficients in a field F. The **derivative** of $f(x)$ is defined to be the polynomial

$$f'(x) = f_1 + 2f_2x + \cdots + nf_nx^{n-1}.$$

Show that

(i) $(f + g)'(x) = f'(x) + g'(x)$;

(ii) $(fg)'(x) = f'(x)g(x) + f(x)g'(x)$.

16 Find all primes p for which the polynomials $x^2 + 3x + 1$ and $x^6 + 2x^5 + x + 1$ define the same function on $\mathbb{Z}_p$.

17 Show that the set of real numbers of the form $m + n\sqrt{2}$, where m and n are integers, is a ring with respect to the usual operations of addition and multiplication. Also show that $m + n\sqrt{2}$ is invertible in this ring if and only if $m^2 - 2n^2 = \pm 1$.

18 Let i, j, k be symbols satisfying the equations

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k,$$
$$jk = -kj = i, \qquad ki = -ik = j.$$

Show that the set Q of expressions of the form $a + bi + cj + dk$, where a, b, c, d are real numbers, satisfies all the axioms for a field except that multiplication is not commutative. (Q is an example of a **skew field**, and its elements are usually known as **quaternions**.)

19 An element x of a ring R is said to be **nilpotent** if $x^n = 0$ in R for some positive integer n. Show that if x and y are nilpotent elements of a ring R with commutative multiplication then $x + y$ is also nilpotent.

20 Find all the nilpotent elements of the rings $\mathbb{Z}_7$, $\mathbb{Z}_8$, and $\mathbb{Z}_9$.

21 Show that any function f from $\mathbb{Z}_2$ to itself may be represented by a polynomial $f(x)$. Does the same result hold for a field $\mathbb{Z}_p$ (p prime)?

can be verified quite easily. What is rather less obvious is that F_9 is actually a field, because every element except 0 has a multiplicative inverse. The sceptical reader is invited to check the following table.

Element:	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
Inverse:	1	2	$2x$	$x+2$	$x+1$	x	$2x+2$	$2x+1$

The general construction of which F_9 is a special case will be explained in Section 23.3. For the moment, we shall emphasize one further property of F_9, concerning its multiplicative group. If we compute the powers of the polynomial $2x + 1$ according to the rules in F_9 we obtain the following results:

$$(2x+1)^1 = 2x+1, \quad (2x+1)^2 = x, \quad (2x+1)^3 = x+1,$$
$$(2x+1)^4 = 2, \quad (2x+1)^5 = x+2, \quad (2x+1)^6 = 2x,$$
$$(2x+1)^7 = 2x+2, \quad (2x+1)^8 = 1.$$

Thus we can express all the non-zero elements of F_9 as powers of $2x + 1$. In other words, the multiplicative group of F_9 is a cyclic group C_8 generated by $2x + 1$:

$$F_9 \backslash \{0\} = U(F_9) = \langle 2x+1 \rangle \approx C_8.$$

In Section 23.4 we shall prove the unexpected result that the multiplicative group of *any* finite field is cyclic.

Exercises 23.1

1 Which members of F_9 can be chosen as the generators of its multiplicative group?

2 Which members of F_9 have square roots in F_9?

3 Without using explicit calculations, prove that the product of all the non-zero elements of F_9 is 2.

4 Show that the additive group of F_9 is not cyclic.

23.2 The order of a finite field

Let F be any field, finite or infinite. Since F is closed under addition, and it contains a multiplicative identity 1, the elements

$$2 = 1+1, \quad 3 = 1+1+1, \quad 4 = 1+1+1+1,$$

and so on, all belong to F. (We do not claim that they are all distinct.) For any positive integer n the sum of n 1's is an element of F; in more formal language we may say that these are the elements of the cyclic subgroup $\langle 1 \rangle$ of the additive group of F.

When F is finite Lagrange's theorem tells us that the order of $\langle 1 \rangle$ is a divisor of $|F|$. This number is called the **characteristic** of F. For example, in the field $\mathbb{Z}_p$ the subgroup $\langle 1 \rangle$ is the whole field, and so the characteristic of $\mathbb{Z}_p$ is p. In general, the characteristic of F is the smallest positive integer m such that $m = 0$ in F, where the latter m denotes the sum of m 1's in F. (When F is infinite the characteristic may or may not be defined.)

Of course, the most immediate result of the theorem is that if a finite field exists then its order must be a prime power. We are familiar with the fields $\mathbb{Z}_p$ (of order p) and we have come across two examples of a field of order 9 (that is, 3^2). Our task now is to show that fields of order p^r do exist for any prime p and any $r \geq 1$.

Exercises 23.2

1 Tables 23.2.1(a, b) define + and × operations on the set $\{w, y, z, t\}$, and the resulting structure is a field F_4.

Table 23.2.1(a)

+	w	y	z	t
w	w	y	z	t
y	y	w	t	z
z	z	t	w	y
t	t	z	y	w

Table 23.2.1(b)

×	w	y	z	t
w	w	w	w	w
y	w	y	z	t
z	w	z	t	y
t	w	t	y	z

(i) Identify the elements 0 and 1 of F_4.
(ii) Show that the additive and multiplicative groups of F_4 are isomorphic to $C_2 \times C_2$ and C_3, respectively.
(iii) What is the characteristic of F_4?

2 Prove that the subset of a finite field F consisting of all the elements of the form $1 + 1 + \cdots + 1$ is itself a field F_0. (F_0 is called the **prime field** of F.)

3 Let F be a field of characteristic 3. Establish the following identities in F:

(i) $x^3 + y^3 = (x + y)^3$,
(ii) $(x + y)^4 + x^4 + (x - y)^4 + y^4 = 0$.

4 Show that in any field of characteristic p

$$(x + y)^p = x^p + y^p.$$

[Hint: Ex. 11.3.5.]

23.3 Construction of finite fields

The field of order 9 constructed in Section 23.1 can be viewed in a slightly more abstract way. The relation $\sim$ on $\mathbb{Z}_3[x]$ defined by

$$a(x) \sim b(x) \quad \Leftrightarrow \quad a(x) - b(x) \text{ is divisible by } x^2 + 1$$

is an equivalence relation. In fact, the polynomials

$$0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2$$

form a complete set of representatives for the equivalence classes, and we can take the classes, rather than their representatives, as the elements of F_9. Denoting the equivalence class of $a(x)$ by $[a(x)]$, we can define the addition and multiplication of equivalence classes in the obvious way as

$$[a(x)] + [b(x)] = [a(x) + b(x)], \qquad [a(x)][b(x)] = [a(x)b(x)],$$

and clearly these definitions correspond exactly to the naive calculations in Section 23.1.

This more general viewpoint opens the way for a more general construction of finite fields. The critical point is that the polynomial used to define the equivalence classes must be *irreducible*.

Theorem 23.3 Let $k(x)$ be an irreducible polynomial of degree r in $\mathbb{Z}_p[x]$, and let $\sim$ be the equivalence relation on $\mathbb{Z}_p[x]$ defined by

$$a(x) \sim b(x) \quad \Leftrightarrow \quad a(x) - b(x) \text{ is divisible by } k(x).$$

Then the set of equivalence classes of $\sim$ in $\mathbb{Z}_p[x]$ is a field of order p^r.

Proof It is clear that the polynomials of degree $0, 1, \ldots, r-1$ form a complete set of representatives for the classes, so there are p^r classes in all. Furthermore, it is entirely a matter of routine checking to verify that the classes (like the polynomials themselves) form a ring, and that multiplication is commutative.

The important thing is to show that every class except $[0]$ has a multiplicative inverse, and this is where the irreducibility of $k(x)$ is vital. Given any polynomial $a(x)$ in $\mathbb{Z}_p[x]$, the fact that $k(x)$ is irreducible means that the monic gcd of $a(x)$ and $k(x)$ is 1. So by Theorem 22.6 there are polynomials $f(x)$ and $g(x)$ in $\mathbb{Z}_p[x]$ such that

$$a(x)f(x) + k(x)g(x) = 1.$$

Taking equivalence classes, and noting that $[k(x)] = [0]$, we obtain

$$[a(x)][f(x)] = [1].$$

In other words, $[a(x)]$ has the inverse $[f(x)]$. □

The theorem tells us that in order to construct a field of order p^r it is only necessary to find an irreducible polynomial of degree r in $\mathbb{Z}_p[x]$. That sounds easy. Indeed, in a very down-to-earth sense it is easy, since there are tables of irreducible polynomials covering any values of p and r which are ever likely to arise in practice. But in mathematics we wish to prove such things, and unfortunately the general proof that there is at least one irreducible polynomial for *every* value of p and r is rather difficult. For that reason we shall proceed to derive some general properties of finite fields and indicate some of their applications, deferring the proof of their existence in all cases until Section 23.9.

Exercises 23.3

1 Prove that $x^3 + x^2 + 1$ is irreducible in $\mathbb{Z}_2[x]$, and hence construct a field of order 8. What is the order of its multiplicative group? Describe the group explicitly.

2 Prove that the field of order 4 constructed by using the irreducible polynomial $x^2 + x + 1$ in $\mathbb{Z}_2[x]$ is essentially the same as the field F_4 constructed in Ex. 23.2.1.

3 For which of the following primes p can we construct a field of order p^2 by using the polynomial $x^2 + 1$?

$$p = 3, 5, 7, 11, 13, 19, 23.$$

Describe the multiplicative group for the first two cases in which the field can be constructed.

4 Show that for every prime p there are fields of order p^2 and p^3. [Hint: see Section 22.8.]

23.4 The primitive element theorem

In Section 23.2 we showed that the *additive* group of a finite field of order $q = p^r$ is isomorphic to $(C_p)^r$, the direct product of r cyclic groups C_p. The *multiplicative* group of the field is a group of order $q - 1$ (since 0 is excluded), and its structure is surprisingly straightforward.

$$\partial(\mathbf{z}, \mathbf{c}') \geq e + 1.$$

Thus $\mathbf{c}$ is the only codeword within distance e of $\mathbf{z}$, and the nearest-neighbour principle will yield the correct answer. □

Exercises 24.1

1 Find the minimum distance δ for each of the following codes.

(i) $\{0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111\}$ in V^4;

(ii) $\{10000, 01010, 00001\}$ in V^5;

(iii) $\{000000, 101010, 010101\}$ in V^6.

In each case, state the number of errors which can be detected and corrected.

2 Which of the codes in Ex. 1 can be extended by the inclusion of an extra codeword without altering δ?

3 Construct a code C in V^6 which will encode five messages and correct one error.

4 Prove the 'triangle inequality'

$$\partial(\mathbf{x}, \mathbf{y}) \leq \partial(\mathbf{x}, \mathbf{z}) + \partial(\mathbf{z}, \mathbf{y}),$$

where $\mathbf{x}, \mathbf{y}, \mathbf{z}$ are any words in V^n.

24.2 Linear codes

The set V^n of all binary words of length n can be made into a group by defining $\mathbf{x}+\mathbf{y}$ to be the word obtained by adding the corresponding bits of $\mathbf{x}$ and $\mathbf{y}$ modulo 2. For example

$$1011001 + 1000111 = 0011110.$$

It is easy to verify that with this definition of the operation $+$, V^n becomes a group. As a group it is simply $(\mathbb{Z}_2)^n$, the direct product of n copies of $\mathbb{Z}_2$.

Definition A code C in V^n is **linear** if, whenever $\mathbf{a}$ and $\mathbf{b}$ are in C, then $\mathbf{a} + \mathbf{b}$ is in C. Equivalently, C is linear if and only if it is a subgroup of V^n.

The codes C_1 and C_2 discussed in the previous section are linear, but the code C_3 is not linear, since 111000 and 110011 belong to C_3 and

$$111000 + 110011 = 001011,$$

where 001011 is not in C_3.

It follows from Lagrange's theorem that, since a linear code is a subgroup of V^n, its size $|C|$ is a divisor of $|V^n| = 2^n$. Hence $|C|$ is an integer of the form 2^k, $0 \leq k \leq n$, and k is called the **dimension** of C.

We have now defined the three parameters (see Table 24.2.1) which determine the practical usefulness of a linear code.

Table 24.2.1

Name	Symbol	Significance
Length	n	Each codeword requires n bits.
Dimension	k	2^k different codewords are available.
Minimum distance	δ	Up to e errors can be corrected, provided $\delta \geq 2e + 1$.