Clearly the prototype of a ring is the set $\mathbb{Z}$ of integers with the usual addition and multiplication. The integers also have two extra algebraic properties, not included in the general definition of a ring: the multiplication is commutative and we can cancel a non-zero integer from both sides of an equation (Theorem 7.5.2).

Another familiar example of a ring is the set $\mathbb{Z}_m$ of integers modulo m, with the operations defined in Section 13.2. The ring $\mathbb{Z}_m$ has a commutative multiplication, but the cancellation rule does not hold, since in $\mathbb{Z}_6$ (for example) we have $3 \times 1 = 3 \times 5$ but we cannot conclude that $1 = 5$.

As an example of a ring in which the commutative law for multiplication does not hold we can take the set of 2×2 matrices with integer entries, and the usual operations of matrix addition and multiplication. It is easy to verify that axioms **R1**, **R2**, and **R3** hold, but multiplication is not commutative. For example, if

$$A = \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}, \qquad B = \begin{bmatrix} 1 & 0 \\ 2 & 2 \end{bmatrix},$$

then

$$AB = \begin{bmatrix} 4 & 2 \\ 2 & 2 \end{bmatrix}, \qquad BA = \begin{bmatrix} 2 & 1 \\ 4 & 4 \end{bmatrix}.$$

Exercises 22.1

1 If R is a ring then the set $M_2(R)$ of 2×2 matrices over R is also a ring. (You need not verify this.)

(i) What is the additive identity in $M_2(R)$?
(ii) What is the additive inverse $-A$ of a matrix A in $M_2(R)$?
(iii) What is the multiplicative identity in $M_2(R)$?
(iv) What is the cardinality of $M_2(\mathbb{Z}_m)$?
(v) Show that multiplication is not commutative in $M_2(\mathbb{Z}_2)$.
(vi) Which elements of $M_2(\mathbb{Z}_2)$ have a multiplicative inverse?

2 By using Theorem 7.5.2, prove that if x and y are integers such that $xy = 0$, then $x = 0$ or $y = 0$. Show by examples that the corresponding result does not hold when $\mathbb{Z}$ is replaced by $\mathbb{Z}_6$ or by $M_2(\mathbb{Z})$.

3 Show that if x and y are members of a ring R then $(-x)y = -xy$ and $(-x)(-y) = xy$. (At each stage of the proof, explain which property of R you are using.)

22.2 Invertible elements of a ring

An element x of a ring R is said to be **invertible** if x has a multiplicative inverse in R, that is, if there is an element u in R such that

$$ux = xu = 1.$$

A simple argument (Ex. 22.2.2) shows that if x is invertible then the element u is unique, and so we can use symbol x^{-1} for u without ambiguity. The element x^{-1} is the **inverse** of x, and the set of invertible elements of R is denoted by $U(R)$.

Exercises 22.2

1 Find the orders of the groups $U(\mathbb{Z}_{10})$, $U(\mathbb{Z}_{11})$, and $U(\mathbb{Z}_{12})$, and describe their structure.

2 Show that if x is an element of a ring R and u, v are elements of R such that

$$ux = xu = 1, \qquad vx = xv = 1,$$

then $u = v$.

3 A complex number of the form $m + ni$, where m and n are integers, is known as a **Gaussian integer**. Verify that the set Γ of Gaussian integers is a ring with respect to the usual addition and multiplication of complex numbers. (You need not verify explicitly the standard properties of complex numbers.) Find the invertible elements of Γ and describe the group structure of $U(\Gamma)$.

22.3 Fields

A **field** is a ring in which the multiplication is commutative and every element except 0 has a multiplicative inverse. Thus, in a field F we have

$$U(F) = F\backslash\{0\}.$$

In order to avoid difficulties about trivial cases, we insist that a field has at least two elements.

We can reorganize the definition, and make it more explicit, by saying that a set F is a field with respect to the operations $+$ and $\times$ if

(i) F is a commutative group with respect to $+$,
(ii) $F\backslash\{0\}$ is a commutative group with respect to $\times$,
(iii) the distributive laws (**R3**) hold.

The groups in (i) and (ii) are usually referred to as the **additive group** and the **multiplicative group** of the field, respectively.

Certainly, $\mathbb{Z}$ is *not* a field since only 1 and -1 have inverses in $\mathbb{Z}$. Similarly, the ring $\mathbb{Z}_m$ is not generally a field, but it follows from Theorem 13.3.1 that

when p is a prime $\mathbb{Z}_p$ is a field.

Of course, the most familiar field is the field $\mathbb{R}$ of real numbers. But, as explained in Chapter 9, its definition and properties are far from being elementary. Fortunately, in Discrete Mathematics the more amenable finite fields such as $\mathbb{Z}_p$ are just as important as is the field $\mathbb{R}$ in Calculus.

In fact there are other finite fields besides the fields $\mathbb{Z}_p$ (p prime), and we shall study their construction and properties in the next chapter. The following *Example* contains a construction of one such field.

Example Let F be a field and let $S_2(F)$ denote the set of 2×2 matrices over F of the form

$$M = \begin{bmatrix} x & y \\ -y & x \end{bmatrix}, \qquad (x, y \in F).$$

do not require an inverse matrix. We have to ask as to whether it is possible that $x^2 + y^2 = 0$ in F when x and y are not both zero.

In $\mathbb{Z}_3$ we can verify explicitly that $x^2 + y^2 \neq 0$ when $(x, y) \neq (0, 0)$:

x	0	0	1	1	1	2	2	2
y	1	2	0	1	2	0	1	2
$x^2 + y^2$	1	1	1	2	2	1	2	2.

We conclude that every non-zero matrix in $S_2(\mathbb{Z}_3)$ has an inverse, and so $S_2(\mathbb{Z}_3)$ is a field.

On the other hand, in $\mathbb{Z}_5$

$$1^2 + 2^2 = 0,$$

and so the matrix with $x = 1$, $y = 2$ has no inverse in $S_2(\mathbb{Z}_5)$, and we do not have a field.

□

Exercises 22.3

1 In the *Example* we showed that $S_2(\mathbb{Z}_3)$ is a field. It has nine elements.

(i) Denote the elements of $S_2(\mathbb{Z}_3)$ by O, I, A_1, $A_2, \ldots$, A_7, where O, I denote the additive and multiplicative identities, and A_1, $A_2, \ldots, A_7$ are the remaining elements in some order.

(ii) Write out the group table for the additive group.

(iii) Show that the additive group is not cyclic.

(iv) Write out the group table for the multiplicative group.

(v) Show that the multiplicative group is cyclic.

2 By finding a suitable generator, show that the multiplicative group of the field $\mathbb{Z}_{23}$ is cyclic.

3 Suppose x and y are elements of a field such that $xy = 0$. Prove that $x = 0$ or $y = 0$.

22.4 Polynomials

In elementary algebra the word *polynomial* is used to describe expressions such as

$$x^2 + 4x + 3, \quad 7x^4 + 2x^2 + 3x + 1.$$

We do not usually trouble ourselves about the meaning of the symbol x, since the context signifies what is intended. For instance, if we are asked to solve the *equation*

$$x^2 + 4x + 3 = 0,$$

then it is understood that x is to be replaced by a suitable number so that the statement becomes a valid equality between numbers.

When we compute with polynomials it becomes clear that the symbols x, x^2, $x^3, \ldots$ can be regarded simply as labels for the positions of the coefficients. In order to compute the sum of two polynomials, we add the corresponding coefficients of each x^i. In order to find the coefficient of x^i in the product of two polynomials, we find the product of the coefficient of x^j in the first one and the coefficient

$$\begin{aligned} a(x)+b(x) &= (1+2)+(2+1)x+(2+0)x^2 \\ &= 2x^2; \\ a(x)b(x) &= (1\times 2)+(1\times 1+2\times 2)x+(2\times 2+2\times 1)x^2+(2\times 1)x^3 \\ &= 2+2x+2x^3. \end{aligned}$$

In general, $R[x]$ is closed under addition and multiplication. With a lot of tedious checking, one can prove that $R[x]$ is in fact a ring with commutative multiplication, provided that R is a ring with commutative multiplication. We shall accept this fact without explicit justification.

We shall also use the standard notational conventions for dealing with polynomials. Thus the coefficient 1 is usually suppressed: for example, we write $2+x$ instead of $2+1x$ for the polynomial $b(x)$ considered above. When a coefficient is zero, we suppress both it and the corresponding power of x (as for example, with the coefficient of x^2 in $a(x)b(x)$ above). Finally, we often write a polynomial with its **leading coefficient** first, that is, in the form

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_n \neq 0$. When $a_n = 1$ we say that the polynomial is **monic**.

Exercises 22.4

1 Compute the sum and product of the following polynomials in $\mathbb{Z}_5[x]$:

(i) x^3+3x^2+2x+1 and x^2+4x+2;
(ii) x^4+x^2+2 and x^3+4x+1.

2 Show that the number of multiplications required to compute the product of the polynomials

$$a_n x^n + \cdots + a_0,$$

and

$$b_n x^n + \cdots + b_0,$$

by direct use of the definition, is $O(n^2)$. (Remarkably this is *not* the most efficient method.)

3 Suppose

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

and

$$b(x) = b_0 + \cdots + b_m x^m$$

are polynomials in $\mathbb{Z}[x]$. Write a program to compute the coefficients c_i $(0 \leq i \leq n+m)$ in the product $a(x)b(x)$.

4 Show that, in $\mathbb{Z}_7[x]$,

$$(x+1)^7 = x^7 + 1.$$

For which values of m is it true that $(x+1)^m = x^m + 1$ in $\mathbb{Z}_m[x]$?

5 Let

$$f(x) = f_0 + f_1 x + \cdots + f_k x^k$$

be an element of the ring $\mathbb{Z}_p[x]$, where p is a prime. Denote the product of n factors $f(x)$ by $f(x)^n$ and the result of replacing x by x^n in $f(x)$ by $f(x^n)$. Show that

(i) $f(x)^p = f(x^p)$,
(ii) $f(x)^{p^r} = f(x^{p^r})$ for all $r \geq 1$.

[Hint: for part (i) use the multinomial theorem and Ex. 12.3.6; for part (ii) use the principle of induction.]

In order to show that $q(x)$ and $r(x)$ are unique, suppose that

$$a(x) = b(x)q_1(x) + r_1(x) = b(x)q_2(x) + r_2(x),$$

where either $\deg r_1(x) < \deg b(x)$ or $r_1(x) = 0$, and either $\deg r_2(x) < \deg b(x)$ or $r_2(x) = 0$. Then

$$b(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x).$$

The left-hand side is zero if $q_1(x) = q_2(x)$; otherwise its degree is at least equal to that of $b(x)$. On the other hand, if the right-hand side is not zero then its degree is strictly less than that of $b(x)$. Hence both sides must be zero and $q_1(x) = q_2(x)$ and $r_1(x) = r_2(x)$. □

It is worth remarking that the construction of $\bar{a}(x)$ in the proof is precisely how we proceed in practical 'long division'. In the example at the beginning of the section, we begin with

$$a(x) = x^4 + 4x^3 + x^2 + 3x + 4, \qquad b(x) = x^2 + 3x + 2$$

and at the first step obtain

$$\bar{a}(x) = x^3 - x^2 + (3x + 4).$$

Of course when the calculation is set out in the usual style, we do not 'bring down' the terms $3x$ and 4 until they are required in the working.

Exercises 22.5

1 Find the quotient and remainder when $x^3 + x^2 + 1$ is divided by $x^2 + x + 1$ in $\mathbb{Z}_2[x]$.

2 Find the quotient and remainder when $x^2 + 2x + 3$ is divided into $x^5 + x^4 + 2x^3 + x^2 + 4x + 2$ in $\mathbb{Z}_5[x]$.

3 Repeat Ex. 2 when the polynomials are regarded as members of $\mathbb{Z}[x]$ and comment on the relationship between the two results.

4 Without carrying out any further long division, write down the quotient and remainder when $x^2 + 2x + 3$ is divided into $x^5 + x^4 + 2x^3 + x^2 + 4x + 2$ in $\mathbb{Z}_7[x]$; and in $\mathbb{Z}_{73}[x]$.

5 Let F be a field. Show that the polynomial $p(x)$ has an inverse in the ring $F[x]$ if and only if $p(x)$ is a non-zero constant polynomial.

22.6 The Euclidean algorithm for polynomials

Now that we have a division algorithm for $F[x]$, analogous to the familiar one for $\mathbb{Z}$, we can proceed with some definitions and theorems about divisibility and factorization of polynomials.

We say that $g(x)$ is a **divisor** (or **factor**) of $f(x)$ in $F[x]$ if there is a polynomial $h(x)$ in $F[x]$ such that $f(x) = g(x)h(x)$. Given any two polynomials $a(x)$ and $b(x)$ in $F[x]$, we say that $d(x)$ is a **greatest common divisor** (**gcd**) of $a(x)$ and $b(x)$ if

(i) $d(x)$ is a divisor of $a(x)$ and $b(x)$, and
(ii) any divisor of $a(x)$ and $b(x)$ is also a divisor of $d(x)$.