3.17** (R. A. Dean***) Define $\mathbb{F}_4$ to be the set of all 2×2 matrices

$$\mathbb{F}_4 = \left\{ \begin{bmatrix} a & b \\ b & a+b \end{bmatrix} : a, b \in \mathbb{F}_2 \right\}.$$

- **(i)** Prove that $\mathbb{F}_4$ is a commutative ring whose operations are matrix addition and matrix multiplication.
- **(ii)** Prove that $\mathbb{F}_4$ is a field having exactly 4 elements.
- **(iii)** Show that $\mathbb{I}_4$ is not a field.

3.18 Prove that every domain R with a finite number of elements must be a field. Using Proposition 3.12, this gives a new proof of sufficiency in Proposition 3.19.

***3.19** Find all the units in the ring $\mathbb{Z}[i]$ of Gaussian integers.

3.20 Show that $F = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a field.

***3.21**
- **(i)** Show that $F = \{a + bi : a, b \in \mathbb{Q}\}$ is a field.
- **(ii)** Show that every $u \in F$ has a factorization $u = \alpha\beta^{-1}$, where $\alpha, \beta \in \mathbb{Z}[i]$. (see Exercise 3.49(ii) on page 249.)

***3.22** If R is a commutative ring, define a relation $\equiv$ on R by $a \equiv b$ if there is a unit $u \in R$ with $b = ua$.
- **(i)** Prove that $\equiv$ is an equivalence relation.
- **(ii)** If $a \equiv b$, prove that $(a) = (b)$, where $(a) = \{ra : r \in R\}$. Conversely, prove that if R is a domain, then $(a) = (b)$ implies $a \equiv b$.

3.23 If R is a domain, prove that there is no subfield K of $\mathrm{Frac}(R)$ such that

$$R \subseteq K \subsetneq \mathrm{Frac}(R).$$

***3.24** Let k be a field with one ε, and let R be the subring

$$R = \{n\varepsilon : n \in \mathbb{Z}\}.$$

- **(i)** If F is a subfield of k, prove that $R \subseteq F$.
- **(ii)** Prove that a subfield F of k is the prime field of k if and only if it is the *smallest* subfield of k containing R; that is, there is no subfield F' with $R \subseteq F' \subsetneq F$.
- **(iii)** If R is a subfield of k, prove that R is the prime field of k.

3.25
- **(i)** Show that every subfield of $\mathbb{C}$ contains $\mathbb{Q}$.
- **(ii)** Show that the prime field of $\mathbb{R}$ is $\mathbb{Q}$.
- **(iii)** Show that the prime field of $\mathbb{C}$ is $\mathbb{Q}$.

***3.26**
- **(i)** For any field F, prove that $\Sigma(2, F) \cong \mathrm{Aff}(1, F)$, where $\Sigma(2, F)$ denotes the stochastic group (defined in Exercise 2.42 on page 144).
- **(ii)** If F is a finite field with q elements, prove that $|\Sigma(2, F)| = q(q-1)$.
- **(iii)** Prove that $\Sigma(2, \mathbb{F}_3) \cong S_3$.

3.3 POLYNOMIALS

Even though the reader is familiar with polynomials, we now introduce them carefully. One modest consequence is that the mystery surrounding the "unknown" x will vanish.

Informally, a polynomial is an "expression" $s_0 + s_1x + s_2x^2 + \cdots + s_nx^n$. The key observation is that one should pay attention to where the coefficients of polynomials live.

Definition. If R is a commutative ring, then a *sequence*[8] in R is a function $\sigma : \mathbb{N} \to R$.

Informally, the expression $s_0 + s_1x + s_2x^2 + \cdots + s_nx^n$ corresponds to the sequence $(s_0, s_1, s_2, \ldots, s_n, 0, 0, \ldots)$ of its coefficients.

As any function, a sequence σ is determined by its values; for each $i \in \mathbb{N}$, write $\sigma(i) = s_i \in R$, so that

$$\sigma = (s_0, s_1, s_2, \ldots, s_i \ \ldots).$$

The entries $s_i \in R$ are called the *coefficients* of the sequence. The term *coefficient* means "acting together to some single end." Here, coefficients combine with powers of x to give the terms of a sequence.

By Proposition 2.2, two sequences σ and τ in R are equal if and only if $\sigma(i) = \tau(i)$ for all $i \geq 0$; that is, $\sigma = \tau$ if and only if they have the same coefficients.

Definition. A sequence $\sigma = (s_0, s_1, \ldots, s_i, \ldots)$ in a commutative ring R is called a *polynomial* if there is some integer $n \geq 0$ with $s_i = 0$ for all $i > n$; that is,

$$\sigma = (s_0, s_1, \ldots, s_n, 0, 0, \ldots).$$

A polynomial has only finitely many nonzero coefficients.

The sequence $\sigma = (0, 0, 0, \ldots)$ is a polynomial, called the *zero polynomial*; it is denoted by $\sigma = 0$.

Definition. If $\sigma \neq 0$ is a polynomial, then there is a natural number n with $s_n \neq 0$ and $s_i = 0$ for all $i > n$. One calls s_n the *leading coefficient* of σ, one calls n the *degree*[9] of σ, and one denotes it by $\deg(\sigma)$.

The zero polynomial 0 does not have a degree because it has no nonzero coefficients; every other polynomial does have a degree.

Notation. If R is a commutative ring, then the set of all polynomials with coefficients in R is denoted by $R[x]$.

[8]Sequences in R are also called *formal power series* (see Exercise 3.36 on page 240).

[9]The word *degree* comes from the Latin word meaning "step."

We will soon prove that a polynomial $(s_0, s_1, \dots, s_n, 0, 0, \dots)$ of degree n can be written as $s_0 + s_1x + s_2x^2 + \cdots + s_nx^n$, but, until then, we proceed formally. Equip $R[x]$ with the following operations. Define

$$\sigma + \tau = (s_0 + t_0, s_1 + t_1, \dots, s_i + t_i, \dots)$$

and

$$\sigma\tau = (a_0, a_1, \dots, a_k, \dots),$$

where $a_k = \sum_{i+j=k} s_i t_j = \sum_{i=0}^{k} s_i t_{k-i}$; thus,

$$\sigma\tau = (s_0t_0, s_0t_1 + s_1t_0, s_0t_2 + s_1t_1 + s_2t_0, \dots).$$

We will soon prove that $R[x]$ is a commutative ring. The next proposition shows where the formula for multiplication comes from.

Proposition 3.23. *If R is a commutative ring and $r, s_i, t_j \in R$ for $i \geq 0$ and $j \geq 0$, then*

$$(s_0 + s_1r + \cdots)(t_0 + t_1r + \cdots) = a_0 + a_1r + \cdots + a_kr^k + \cdots,$$

where $a_k = \sum_{i+j=k} s_i t_j$ for all $k \geq 0$.

Remark. This proof should be an induction on $k \geq 0$, but we give an informal proof instead. ◀

Proof. Write $\sum_i s_i r^i = f(r)$ and $\sum_j t_j r^j = g(r)$. Then

$$\begin{aligned} f(r)g(r) &= (s_0 + s_1r + s_2r^2 + \cdots)g(r) \\ &= s_0g(r) + s_1rg(r) + s_2r^2g(r) + \cdots \\ &= s_0(t_0 + t_1r + \cdots) + s_1r(t_0 + t_1r + \cdots) \\ &\qquad + s_2r^2(t_0 + t_1r + \cdots) + \cdots \\ &= s_0t_0 + (s_1t_0 + s_0t_1)r + (s_2t_0 + s_1t_1 + s_0t_2)r^2 + \\ &\qquad (s_0t_3 + s_1t_2 + s_2t_1 + s_3t_0)r^3 + \cdots. \end{aligned}$$ •

Lemma 3.24. *Let R be a commutative ring and let $\sigma, \tau \in R[x]$ be nonzero polynomials.*

(i) *Either $\sigma\tau = 0$ or $\deg(\sigma\tau) \leq \deg(\sigma) + \deg(\tau)$.*

(ii) *If R is a domain, then $\sigma\tau \neq 0$ and*

$$\deg(\sigma\tau) = \deg(\sigma) + \deg(\tau).$$

Proof.
(i) Let $\sigma = (s_0, s_1, \dots)$ have degree m, let $\tau = (t_0, t_1, \dots)$ have degree n, and let $\sigma\tau = (a_0, a_1, \dots)$. It suffices to prove that $a_k = 0$ for all $k > m + n$. By definition,

$$a_k = \sum_{i+j=k} s_i t_j.$$

If $i \le m$, then $j = k - i \ge k - m > n$ (because $k > m + n$), and so $t_j = 0$ (because τ has degree n); if $i > m$, then $s_i = 0$ because σ has degree m. In either case, each term $s_i t_j = 0$, and so $a_k = \sum_{i+j=k} s_i t_j = 0$.
(ii) Now let $k = m + n$. With the possible exception of $s_m t_n$ (the product of the leading coefficients of σ and τ), the same calculation as in part (i) shows that each term $s_i t_j$ in

$$a_{m+n} = s_0 t_{m+n} + \cdots + s_{n-1} t_{m+1} + s_n t_m + s_{n+1} t_{m-1} + \cdots + s_{m+n} t_0$$

is 0. If $i < m$, then $m - i > 0$, hence $j = m - i + n > n$, and so $t_j = 0$; if $i > m$, then $s_i = 0$. Hence

$$a_{m+n} = s_m t_n.$$

Since R is a domain, $s_m \neq 0$ and $t_n \neq 0$ imply $s_m t_n \neq 0$; hence, $\sigma\tau \neq 0$ and $\deg(\sigma\tau) = m + n = \deg(\sigma) + \deg(\tau)$. •

Proposition 3.25.

(i) *If R is a commutative ring, then $R[x]$ is a commutative ring that contains R as a subring.*

(ii) *If R is a domain, then $R[x]$ is a domain.*

Proof.
(i) Addition and multiplication are operations on $R[x]$: the sum of two polynomials σ and τ is a sequence which is also a polynomial (indeed, either $\sigma + \tau = 0$ or $\deg(\sigma + \tau) \le \max\{\deg(\sigma), \deg(\tau)\}$), while the lemma shows that the sequence which is the product of two polynomials is a polynomial as well. Verifications of the axioms for a commutative ring are again routine, and they are left to the reader. Note that the zero is the zero polynomial, the one is the polynomial $(1, 0, 0, \dots)$, and the negative of $(s_0, s_1, \dots, s_i, \dots)$ is $(-s_0, -s_1, \dots, -s_i, \dots)$. The only possible problem is proving associativity of multiplication; we give the hint that if $\rho = (r_0, r_1, \dots, r_i, \dots)$, then the ℓth coordinate of the polynomial $\rho(\sigma\tau)$ turns out to be $\sum_{i+j+k=\ell} r_i(s_j t_k)$, while the ℓth coordinate of the polynomial $(\rho\sigma)\tau$ turns out to be $\sum_{i+j+k=\ell}(r_i s_j)t_k$; these are equal because of associativity of the multiplication in R.

It is easy to check that $R' = \{(r, 0, 0, \dots) : r \in R\}$ is a subring of $R[x]$, and we identify R' with R by identifying $r \in R$ with $(r, 0, 0, \dots)$.

(ii) If R is a domain and if σ and τ are nonzero polynomials, then Lemma 3.24 shows that $\sigma\tau \neq 0$. Therefore, $R[x]$ is a domain. •

Just as our assertion (in Theorem 3.21) that a domain is a subring of its fraction field was not quite true, so, too, our assertion here that a commutative ring R is a subring of $R[x]$ is not quite correct. There is a subring of $R[x]$, namely $R' = \{(r, 0, 0, \ldots) : r \in R\}$, which strongly resembles R, and the statement of Proposition 3.25 will be made precise once the notion of *isomorphism* is introduced (see Example 3.31).

We can now recapture the usual notation.

Definition. Define the *indeterminate* to be the element

$$x = (0, 1, 0, 0, \ldots) \in R[x].$$

Even though x is neither "the unknown" nor a variable, we call it the *indeterminate* to recall one's first encounter with it in high school (see the discussion on page 238). However, the indeterminate x is a specific element in the ring $R[x]$, namely, the polynomial $(t_0, t_1, t_2, \ldots)$ with $t_1 = 1$ and all other $t_i = 0$. One reason we insist that commutative rings have ones is to enable us to make this definition; if the set E of even integers were a commutative ring, then $E[x]$ would not contain x (it would contain $2x$, however). Note that if R is the zero ring, then $R[x]$ is also the zero ring.

Lemma 3.26.

(i) *If* $\sigma = (s_0, s_1, \ldots, s_j, \ldots)$, *then*

$$x\sigma = (0, s_0, s_1, \ldots, s_j, \ldots);$$

that is, multiplying by x *shifts each coefficient one step to the right.*

(ii) *If* $n \geq 1$, *then* x^n *is the polynomial having* 0 *everywhere except for* 1 *in the* n*th coordinate.*

(iii) *If* $r \in R$, *then*

$$(r, 0, 0, \ldots)(s_0, s_1, \ldots, s_j, \ldots) = (rs_0, rs_1, \ldots, rs_j, \ldots).$$

Proof.
(i) Write $x = (t_0, t_1, \ldots, t_i, \ldots)$, where $t_1 = 1$ and all other $t_i = 0$, and let $x\sigma = (a_0, a_1, \ldots, a_k, \ldots)$. Now $a_0 = t_0 s_0 = 0$ because $t_0 = 0$. If $k \geq 1$, then the only nonzero term in the sum $a_k = \sum_{i+j=k} s_i t_j$ is $s_{k-1}t_1 = s_{k-1}$, because $t_1 = 1$ and $t_i = 0$ for $i \neq 1$; thus, for $k \geq 1$, the kth coordinate a_k of $x\sigma$ is s_{k-1}, and $x\sigma = (0, s_0, s_1, \ldots, s_i, \ldots)$.
(ii) An easy induction, using (i).
(iii) This follows easily from the definition of multiplication. •

If we identify $(r, 0, 0, \dots)$ with r, then Lemma 3.26(iii) reads

$$r(s_0, s_1, \dots, s_i, \dots) = (rs_0, rs_1, \dots, rs_i, \dots).$$

We can now recapture the usual notation.

Proposition 3.27. *If* $\sigma = (s_0, s_1, \dots, s_n, 0, 0, \dots)$, *then*

$$\sigma = s_0 + s_1x + s_2x^2 + \cdots + s_nx^n,$$

where each element $s \in R$ *is identified with the polynomial* $(s, 0, 0, \dots)$.

Proof.

$$\begin{aligned}\sigma &= (s_0, s_1, \dots, s_n, 0, 0, \dots)\\ &= (s_0, 0, 0, \dots) + (0, s_1, 0, \dots) + \cdots + (0, 0, \dots, s_n, 0, \dots)\\ &= s_0(1, 0, 0, \dots) + s_1(0, 1, 0, \dots) + \cdots + s_n(0, 0, \dots, 1, 0, \dots)\\ &= s_0 + s_1x + s_2x^2 + \cdots + s_nx^n. \quad \bullet\end{aligned}$$

We shall use this familiar (and standard) notation from now on. As is customary, we shall write

$$f(x) = s_0 + s_1x + s_2x^2 + \cdots + s_nx^n$$

instead of $\sigma = (s_0, s_1, \dots, s_n, 0, 0, \dots)$.

Definition. If R is a commutative ring, then $R[x]$ is called the *ring of polynomials over* R.

Here is some standard vocabulary associated with polynomials. If $f(x) = s_0 + s_1x + s_2x^2 + \cdots + s_nx^n$, where $s_n \neq 0$, then s_0 is called its *constant term* and, as we have already said, s_n is called its *leading coefficient*. If its leading coefficient $s_n = 1$, then $f(x)$ is called *monic*. Every polynomial other than the zero polynomial 0 (having all coefficients 0) has a degree. A *constant polynomial* is either the zero polynomial or a polynomial of degree 0. Polynomials of degree 1, namely, $a + bx$ with $b \neq 0$, are called *linear*, polynomials of degree 2 are *quadratic*,[10] degree 3's are *cubic*, then *quartic*, *quintic*, etc.

[10]Quadratic polynomials are so called because the particular quadratic x^2 gives the area of a square (*quadratic* comes from the Latin word meaning "four," which is to remind one of the 4-sided figure); similarly, *cubic* polynomials are so called because x^3 gives the volume of a cube. *Linear* polynomials are so called because the graph of a linear polynomial in $\mathbb{R}[x]$ is a line.

Corollary 3.28. *Polynomials* $f(x) = s_0 + s_1x + s_2x^2 + \cdots + s_nx^n$ *and* $g(x) = t_0 + t_1x + t_2x^2 + \cdots + t_mx^m$ *are equal if and only if* $s_i = t_i$ *for all* $i \in \mathbb{N}$.

Proof. We have merely restated the definition of equality of polynomials in terms of the familiar notation. •

We can now describe the usual role of the indeterminate x as a variable. If R is a commutative ring, each polynomial $f(x) = s_0 + s_1x + s_2x^2 + \cdots + s_nx^n \in R[x]$ defines a *polynomial function* $f^\flat\colon R \to R$ by evaluation: if $r \in R$, define $f^\flat(r) = s_0 + s_1r + s_2r^2 + \cdots + s_nr^n \in R$ [usually, one is not so fussy, and one writes $f(r)$ instead of $f^\flat(r)$]. The reader should realize that polynomials and polynomial functions are distinct objects. For example, if R is a finite ring, e.g., $\mathbb{I}_m$, then there are only finitely many functions from R to itself; a fortiori, there are only finitely many polynomial functions. On the other hand, if R is not the zero ring, there are infinitely many polynomials. For example, all the powers $1, x, x^2, \ldots, x^n, \ldots$ are distinct, by Corollary 3.28.

Definition. Let F be a field. The fraction field of $F[x]$, denoted by $F(x)$, is called the *field of rational functions* over F.

Proposition 3.29. *The elements of* $F(x)$ *have the form* $f(x)/g(x)$, *where* $f(x)$, $g(x) \in F[x]$ *and* $g(x) \neq 0$.

Proof. By Theorem 3.21, every element in the fraction field $F(x)$ has the form $f(x)g(x)^{-1}$. •

Proposition 3.30. *If* p *is a prime, then the field of rational functions* $\mathbb{F}_p(x)$ *is an infinite field whose prime field is* $\mathbb{F}_p$.

Proof. By Proposition 3.25, $\mathbb{F}_p[x]$ is a domain. Its fraction field $\mathbb{F}_p(x)$ is a field containing $\mathbb{F}_p[x]$ as a subring, while $\mathbb{F}_p[x]$ contains $\mathbb{F}_p$ as a subring, by Proposition 3.25. That $\mathbb{F}_p$ is the prime field follows from Exercise 3.24 on page 232. •

In spite of the difference between polynomials and polynomial functions (we shall see, in Corollary 3.52, that these objects coincide when the coefficient ring R is an infinite field), one often calls $R[x]$ the ring of all *polynomials over* R *in one variable* (or *polynomials over* R *in one indeterminate*). If we write $A = R[x]$, then the polynomial ring $A[y]$ is called the ring of all *polynomials over* R *in two variables* x *and* y (or *indeterminates*), and it is denoted by $R[x, y]$. For example, the quadratic polynomial $ax^2 + bxy + cy^2 + dx + ey + f$ can be written $cy^2 + (bx + e)y + (ax^2 + dx + f)$, a polynomial in y with coefficients in $R[x]$. By induction, one can form the commutative ring $R[x_1, x_2, \ldots, x_n]$ of all *polynomials in* n *variables* (or *indeterminates*) with coefficients in R.