product $\prod_{i \in I} R_i$ is a ring under componentwise addition and multiplication.

20. Let R be the collection of sequences $(a_1, a_2, a_3, \ldots)$ of integers $a_1, a_2, a_3, \ldots$ where all but finitely many of the a_i are 0 (called the *direct sum* of infinitely many copies of $\mathbb{Z}$). Prove that R is a ring under componentwise addition and multiplication which does not have an identity.

21. Let X be any nonempty set and let $\mathcal{P}(X)$ be the set of all subsets of X (the *power set* of X). Define addition and multiplication on $\mathcal{P}(X)$ by

$$A + B = (A - B) \cup (B - A) \qquad \text{and} \qquad A \times B = A \cap B$$

i.e., addition is symmetric difference and multiplication is intersection.

(a) Prove that $\mathcal{P}(X)$ is a ring under these operations ($\mathcal{P}(X)$ and its subrings are often referred to as *rings of sets*).

(b) Prove that this ring is commutative, has an identity and is a Boolean ring.

22. Give an example of an infinite Boolean ring.

23. Let D be a squarefree integer, and let $\mathcal{O}$ be the ring of integers in the quadratic field $\mathbb{Q}(\sqrt{D})$. For any positive integer f prove that the set $\mathcal{O}_f = \mathbb{Z}[f\omega] = \{a + bf\omega \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathcal{O}$ containing the identity. Prove that $[\mathcal{O} : \mathcal{O}_f] = f$ (index as additive abelian groups). Prove conversely that a subring of $\mathcal{O}$ containing the identity and having finite index f in $\mathcal{O}$ (as additive abelian group) is equal to $\mathcal{O}_f$. (The ring $\mathcal{O}_f$ is called the *order of conductor* f in the field $\mathbb{Q}(\sqrt{D})$. The ring of integers $\mathcal{O}$ is called the *maximal order* in $\mathbb{Q}(\sqrt{D})$.)

24. Show for $D = 3, 5, 6$, and 7 that the group of units $\mathcal{O}^\times$ of the quadratic integer ring $\mathcal{O}$ is infinite by exhibiting an explicit unit of infinite (multiplicative) order in each ring.

25. Let I be the ring of integral Hamilton Quaternions and define

$$N : I \to \mathbb{Z} \qquad \text{by} \qquad N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$$

(the map N is called a *norm*).

(a) Prove that $N(\alpha) = \alpha\overline{\alpha}$ for all $\alpha \in I$, where if $\alpha = a + bi + cj + dk$ then $\overline{\alpha} = a - bi - cj - dk$.

(b) Prove that $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in I$.

(c) Prove that an element of I is a unit if and only if it has norm $+1$. Show that $I^\times$ is isomorphic to the quaternion group of order 8. [The inverse in the ring of rational quaternions of a nonzero element α is $\dfrac{\overline{\alpha}}{N(\alpha)}$.]

26. Let K be a field. A *discrete valuation* on K is a function $v : K^\times \to \mathbb{Z}$ satisfying

(i) $v(ab) = v(a) + v(b)$ (i.e., v is a homomorphism from the multiplicative group of nonzero elements of K to $\mathbb{Z}$),

(ii) v is surjective, and

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K^\times$ with $x + y \neq 0$.

The set $R = \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}$ is called the *valuation ring* of v.

(a) Prove that R is a subring of K which contains the identity. (In general, a ring R is called a *discrete valuation ring* if there is some field K and some discrete valuation v on K such that R is the valuation ring of v.)

(b) Prove that for each nonzero element $x \in K$ either x or x^{-1} is in R.

(c) Prove that an element x is a unit of R if and only if $v(x) = 0$.

27. A specific example of a discrete valuation ring (cf. the preceding exercise) is obtained

when p is a prime, $K = \mathbb{Q}$ and

$$v_p : \mathbb{Q}^\times \to \mathbb{Z} \qquad \text{by} \qquad v_p(\frac{a}{b}) = \alpha \quad \text{where } \frac{a}{b} = p^\alpha \frac{c}{d}, \quad p \nmid c \text{ and } p \nmid d.$$

Prove that the corresponding valuation ring R is the ring of all rational numbers whose denominators are relatively prime to p. Describe the units of this valuation ring.

28. Let R be a ring with $1 \neq 0$. A nonzero element a is called a *left zero divisor* in R if there is a nonzero element $x \in R$ such that $ax = 0$. Symmetrically, $b \neq 0$ is a *right zero divisor* if there is a nonzero $y \in R$ such that $yb = 0$ (so a zero divisor is an element which is either a left or a right zero divisor). An element $u \in R$ has a *left inverse* in R if there is some $s \in R$ such that $su = 1$. Symmetrically, v has a *right inverse* if $vt = 1$ for some $t \in R$.

(a) Prove that u is a unit if and only if it has both a right and a left inverse (i.e., u must have a two-sided inverse).

(b) Prove that if u has a right inverse then u is not a right zero divisor.

(c) Prove that if u has more than one right inverse then u is a left zero divisor.

(d) Prove that if R is a finite ring then every element that has a right inverse is a unit (i.e., has a two-sided inverse).

29. Let A be any commutative ring with identity $1 \neq 0$. Let R be the set of all group homomorphisms of the additive group A to itself with addition defined as pointwise addition of functions and multiplication defined as function composition. Prove that these operations make R into a ring with identity. Prove that the units of R are the group automorphisms of A (cf. Exercise 20, Section 1.6).

30. Let $A = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \cdots$ be the direct product of copies of $\mathbb{Z}$ indexed by the positive integers (so A is a ring under componentwise addition and multiplication) and let R be the ring of all group homomorphisms from A to itself as described in the preceding exercise. Let φ be the element of R defined by $\varphi(a_1, a_2, a_3, \dots) = (a_2, a_3, \dots)$. Let ψ be the element of R defined by $\psi(a_1, a_2, a_3, \dots) = (0, a_1, a_2, a_3, \dots)$.

(a) Prove that $\varphi\psi$ is the identity of R but $\psi\varphi$ is not the identity of R (i.e., ψ is a *right inverse* for φ but not a left inverse).

(b) Exhibit infinitely many right inverses for φ.

(c) Find a nonzero element π in R such that $\varphi\pi = 0$ but $\pi\varphi \neq 0$.

(d) Prove that there is no nonzero element $\lambda \in R$ such that $\lambda\varphi = 0$ (i.e., φ is a left zero divisor but not a right zero divisor).

7.2 EXAMPLES: POLYNOMIAL RINGS, MATRIX RINGS, AND GROUP RINGS

We introduce here three important types of rings: polynomial rings, matrix rings, and group rings. We shall see in the course of the text that these three classes of rings are often related. For example, we shall see in Part VI that the group ring of a group G over the complex numbers $\mathbb{C}$ is a direct product of matrix rings over $\mathbb{C}$.

These rings also have many important applications, in addition to being interesting in their own right. In Part III we shall use polynomial rings to prove some classification theorems for matrices which, in particular, determine when a matrix is similar to a diagonal matrix. In Part VI we shall use group rings to study group actions and to prove some additional important classification theorems.

Polynomial Rings

Fix a commutative ring R with identity. We define the ring of polynomials in a form which may already be familiar, at least for polynomials with real coefficients. A definition in terms of Cartesian products is given in Appendix I. Let x be an indeterminate. The formal sum

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

with $n \geq 0$ and each $a_i \in R$ is called a *polynomial* in x with coefficients a_i in R. If $a_n \neq 0$, then the polynomial is said to be of *degree* n, $a_n x^n$ is called the *leading term*, and a_n is called the *leading coefficient* (where the leading coefficient of the zero polynomial is taken to be 0). The polynomial is *monic* if $a_n = 1$. The set of all such polynomials is called the ring of *polynomials in the variable x with coefficients in R* and will be denoted $R[x]$.

The operations of addition and multiplication which make $R[x]$ into a ring are the same operations familiar from elementary algebra: addition is "componentwise"

$$\begin{aligned}(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) + (b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0)\\ = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0)\end{aligned}$$

(here a_n or b_n may be zero in order for addition of polynomials of different degrees to be defined). Multiplication is performed by first defining $(ax^i)(bx^j) = abx^{i+j}$ for polynomials with only one nonzero term and then extending to all polynomials by the distributive laws (usually referred to as "expanding out and collecting like terms"):

$$\begin{aligned}&(a_0 + a_1 x + a_2 x^2 + \ldots) \times (b_0 + b_1 x + b_2 x^2 + \ldots)\\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \ldots\end{aligned}$$

(in general, the coefficient of x^k in the product will be $\sum_{i=0}^{k} a_i b_{k-i}$). These operations make sense since R is a ring so the sums and products of the coefficients are defined. An easy verification proves that $R[x]$ is indeed a ring with these definitions of addition and multiplication.

The ring R appears in $R[x]$ as the *constant polynomials*. Note that by definition of the multiplication, $R[x]$ is a *commutative ring with identity* (the identity 1 from R).

The coefficient ring R above was assumed to be a commutative ring since that is the situation we shall be primarily interested in, but note that the definition of the addition and multiplication in $R[x]$ above would be valid even if R were not commutative or did not have an identity. If the coefficient ring R is the integers $\mathbb{Z}$ (respectively, the rationals $\mathbb{Q}$) the polynomial ring $\mathbb{Z}[x]$ (respectively, $\mathbb{Q}[x]$) is the ring of polynomials with integer (rational) coefficients familiar from elementary algebra.

Another example is the polynomial ring $\mathbb{Z}/3\mathbb{Z}[x]$ of polynomials in x with coefficients in $\mathbb{Z}/3\mathbb{Z}$. This ring consists of nonnegative powers of x with coefficients 0, 1, and 2 with calculations on the coefficients performed modulo 3. For example, if

$$p(x) = x^2 + 2x + 1 \qquad \text{and} \qquad q(x) = x^3 + x + 2$$

then

$$p(x) + q(x) = x^3 + x^2$$