and

$$p(x)q(x) = x^5 + 2x^4 + 2x^3 + x^2 + 2x + 2.$$

The ring in which the coefficients are taken makes a substantial difference in the behavior of polynomials. For example, the polynomial $x^2 + 1$ is not a perfect square in the polynomial ring $\mathbb{Z}[x]$, but *is* a perfect square in the polynomial ring $\mathbb{Z}/2\mathbb{Z}[x]$, since $(x + 1)^2 = x^2 + 2x + 1 = x^2 + 1$ in this ring.

Proposition 4. Let R be an integral domain and let $p(x), q(x)$ be nonzero elements of $R[x]$. Then

(1) degree $p(x)q(x)$ = degree $p(x)$ + degree $q(x)$,
(2) the units of $R[x]$ are just the units of R,
(3) $R[x]$ is an integral domain.

Proof: If R has no zero divisors then neither does $R[x]$; if $p(x)$ and $q(x)$ are polynomials with leading terms $a_n x^n$ and $b_m x^m$, respectively, then the leading term of $p(x)q(x)$ is $a_n b_m x^{n+m}$, and $a_n b_m \neq 0$. This proves (3) and also verifies (1). If $p(x)$ is a unit, say $p(x)q(x) = 1$ in $R[x]$, then degree $p(x)$ + degree $q(x) = 0$, so both $p(x)$ and $q(x)$ are elements of R, hence are units in R since their product is 1. This proves (2).

If the ring R has zero divisors then so does $R[x]$, because $R \subset R[x]$. Also, if $f(x)$ is a zero divisor in $R[x]$ (i.e., $f(x)g(x) = 0$ for some nonzero $g(x) \in R[x]$) then in fact $cf(x) = 0$ for some nonzero $c \in R$ (cf. Exercise 2).

If S is a subring of R then $S[x]$ is a subring of $R[x]$. For instance, $\mathbb{Z}[x]$ is a subring of $\mathbb{Q}[x]$. Some other examples of subrings of $R[x]$ are the set of all polynomials in x^2 (i.e., in which only even powers of x appear) and the set of all polynomials with zero constant term (the latter subring does not have an identity).

Polynomial rings, particularly those over fields, will be studied extensively in Chapter 9.

Matrix Rings

Fix an arbitrary ring R and let n be a positive integer. Let $M_n(R)$ be the set of all $n \times n$ *matrices with entries from* R. The element (a_{ij}) of $M_n(R)$ is an $n \times n$ square array of elements of R whose entry in row i and column j is $a_{ij} \in R$. The set of matrices becomes a ring under the usual rules by which matrices of real numbers are added and multiplied. Addition is componentwise: the i, j entry of the matrix $(a_{ij}) + (b_{ij})$ is $a_{ij} + b_{ij}$. The i, j entry of the matrix product $(a_{ij}) \times (b_{ij})$ is $\sum_{k=1}^{n} a_{ik} b_{kj}$ (note that these matrices need to be square in order that multiplication of any two elements be defined). It is a straightforward calculation to check that these operations make $M_n(R)$ into a ring. When R is a field we shall prove that $M_n(R)$ is a ring by less computational means in Part III.

Note that if R is any nontrivial ring (even a commutative one) and $n \geq 2$ then $M_n(R)$ is *not commutative*: if $ab \neq 0$ in R let A be the matrix with a in position 1,1 and zeros elsewhere and let B be the matrix with b in position 1,2 and zeros elsewhere; then ab is the (nonzero) entry in position 1,2 of AB whereas BA is the zero matrix.

These two matrices also show that $M_n(R)$ has zero divisors for all nonzero rings R whenever $n \geq 2$.

An element (a_{ij}) of $M_n(R)$ is called a *scalar matrix* if for some $a \in R$, $a_{ii} = a$ for all $i \in \{1, \ldots, n\}$ and $a_{ij} = 0$ for all $i \neq j$ (i.e., all diagonal entries equal a and all off-diagonal entries are 0). The set of scalar matrices is a subring of $M_n(R)$. This subring is a copy of R (i.e., is "isomorphic" to R): if the matrix A has the element a along the main diagonal and the matrix B has the element b along the main diagonal then the matrix $A + B$ has $a + b$ along the diagonal and AB has ab along the diagonal (and all other entries 0). If R is commutative, the scalar matrices commute with all elements of $M_n(R)$. If R has a 1, then the scalar matrix with 1's down the diagonal (the *$n \times n$ identity matrix*) is the 1 of $M_n(R)$. In this case the units in $M_n(R)$ are the invertible $n \times n$ matrices and the group of units is denoted $GL_n(R)$, the *general linear group* of degree n over R.

If S is a subring of R then $M_n(S)$ is a subring of $M_n(R)$. For instance $M_n(\mathbb{Z})$ is a subring of $M_n(\mathbb{Q})$ and $M_n(2\mathbb{Z})$ is a subring of both of these. Another example of a subring of $M_n(R)$ is the set of *upper triangular* matrices: $\{(a_{ij}) \mid a_{pq} = 0 \text{ whenever } p > q\}$ (the set of matrices all of whose entries below the main diagonal are zero) — one easily checks that the sum and product of upper triangular matrices is upper triangular.

Group Rings

Fix a commutative ring R with identity $1 \neq 0$ and let $G = \{g_1, g_2, \ldots, g_n\}$ be any finite group with group operation written multiplicatively. Define the *group ring*, RG, of G with coefficients in R to be the set of all formal sums

$$a_1g_1 + a_2g_2 + \cdots + a_ng_n \qquad a_i \in R, \quad 1 \leq i \leq n.$$

If g_1 is the identity of G we shall write a_1g_1 simply as a_1. Similarly, we shall write the element $1g$ for $g \in G$ simply as g.

Addition is defined "componentwise"

$$\begin{aligned}(a_1g_1 + a_2g_2 + \cdots + a_ng_n) &+ (b_1g_1 + b_2g_2 + \cdots + b_ng_n) \\ &= (a_1 + b_1)g_1 + (a_2 + b_2)g_2 + \cdots + (a_n + b_n)g_n.\end{aligned}$$

Multiplication is performed by first defining $(ag_i)(bg_j) = (ab)g_k$, where the product ab is taken in R and $g_ig_j = g_k$ is the product in the group G. This product is then extended to all formal sums by the distributive laws so that the coefficient of g_k in the product $(a_1g_1 + \cdots + a_ng_n) \times (b_1g_1 + \cdots + b_ng_n)$ is $\sum_{g_ig_j = g_k} a_ib_j$. It is straightforward to check that these operations make RG into a ring (again, commutativity of R is not needed). The associativity of multiplication follows from the associativity of the group operation in G. The ring RG is commutative if and only if G is a commutative group.

Example

Let $G = D_8$ be the dihedral group of order 8 with the usual generators r, s ($r^4 = s^2 = 1$ and $rs = sr^{-1}$) and let $R = \mathbb{Z}$. The elements $\alpha = r + r^2 - 2s$ and $\beta = -3r^2 + rs$ are typical members of $\mathbb{Z}D_8$. Their sum and product are then

$$\begin{aligned}\alpha+\beta &= r-2r^2-2s+rs\\ \alpha\beta &= (r+r^2-2s)(-3r^2+rs)\\ &= r(-3r^2+rs)+r^2(-3r^2+rs)-2s(-3r^2+rs)\\ &= -3r^3+r^2s-3+r^3s+6r^2s-2r^3\\ &= -3-5r^3+7r^2s+r^3s.\end{aligned}$$

The ring R appears in RG as the "constant" formal sums i.e., the R-multiples of the identity of G (note that the definition of the addition and multiplication in RG restricted to these elements is just the addition and multiplication in R). These elements of R commute with all elements of RG. The identity of R is the identity of RG.

The group G also appears in RG (the element g_i appears as $1g_i$ — for example, $r, s \in D_8$ are also elements of the group ring $\mathbb{Z}D_8$ above) — multiplication in the ring RG restricted to G is just the group operation. In particular, each element of G has a multiplicative inverse in the ring RG (namely, its inverse in G). This says that G is a *subgroup of the group of units of RG*.

If $|G| > 1$ then RG always has zero divisors. For example, let g be any element of G of order $m > 1$. Then

$$(1-g)(1+g+\cdots+g^{m-1}) = 1-g^m = 1-1 = 0$$

so $1-g$ is a zero divisor (note that by definition of RG neither of the formal sums in the above product is zero).

If S is a subring of R then SG is a subring of RG. For instance, $\mathbb{Z}G$ (called the *integral group ring* of G) is a subring of $\mathbb{Q}G$ (the *rational group ring* of G). Furthermore, if H is a subgroup of G then RH is a subring of RG. The set of all elements of RG whose coefficients sum to zero is a subring (without identity). If $|G| > 1$, the set of elements with zero "constant term" (i.e., the coefficient of the identity of G is zero) is *not* a subring (it is not closed under multiplication).

Note that the group ring $\mathbb{R}Q_8$ is *not* the same ring as the Hamilton Quaternions $\mathbb{H}$ even though the latter contains a copy of the quaternion group Q_8 (under multiplication). One difference is that the unique element of order 2 in Q_8 (usually denoted by -1) is not the additive inverse of 1 in $\mathbb{R}Q_8$. In other words, if we temporarily denote the identity of the group Q_8 by g_1 and the unique element of order 2 by g_2, then g_1+g_2 is not zero in $\mathbb{R}Q_8$, whereas $1+(-1)$ is zero in $\mathbb{H}$. Furthermore, as noted above, the group ring $\mathbb{R}Q_8$ contains zero divisors hence is not a division ring.

Group rings over fields will be studied extensively in Chapter 18.

EXERCISES

Let R be a commutative ring with 1.

1. Let $p(x) = 2x^3-3x^2+4x-5$ and let $q(x) = 7x^3+33x-4$. In each of parts (a), (b) and (c) compute $p(x)+q(x)$ and $p(x)q(x)$ under the assumption that the coefficients of the two given polynomials are taken from the specified ring (where the integer coefficients are taken mod n in parts (b) and (c)):
(a) $R=\mathbb{Z}$, **(b)** $R=\mathbb{Z}/2\mathbb{Z}$, **(c)** $R=\mathbb{Z}/3\mathbb{Z}$.