CHAPTER 9

Polynomial Rings

We begin this chapter on polynomial rings with a summary of facts from the preceding two chapters (with references where needed). The basic definitions were given in slightly greater detail in Section 7.2. For convenience, the ring R will always be a commutative ring with identity $1 \neq 0$.

9.1 DEFINITIONS AND BASIC PROPERTIES

The polynomial ring $R[x]$ in the indeterminate x with coefficients from R is the set of all formal sums $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $n \geq 0$ and each $a_i \in R$. If $a_n \neq 0$ then the polynomial is of degree n, $a_n x^n$ is the leading term, and a_n is the leading coefficient (where the leading coefficient of the zero polynomial is defined to be 0). The polynomial is monic if $a_n = 1$. Addition of polynomials is "componentwise":

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i$$

(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 $(ax^i)(bx^j) = abx^{i+j}$ and then extending to all polynomials by the distributive laws so that in general

$$\left(\sum_{i=0}^{n} a_i x^i\right) \times \left(\sum_{i=0}^{m} b_i x^i\right) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k.$$

In this way $R[x]$ is a commutative ring with identity (the identity 1 from R) in which we identify R with the subring of constant polynomials.

We have already noted that if R is an integral domain then the leading term of a product of polynomials is the product of the leading terms of the factors. The following is Proposition 4 of Section 7.2 which we record here for completeness.

Proposition 1. Let R be an integral domain. Then

(1) degree $p(x)q(x)$ = degree $p(x)$ + degree $q(x)$ if $p(x), q(x)$ are nonzero

(2) the units of $R[x]$ are just the units of R

(3) $R[x]$ is an integral domain.

Recall also that if R is an integral domain, the quotient field of $R[x]$ consists of all quotients $\dfrac{p(x)}{q(x)}$ where $q(x)$ is not the zero polynomial (and is called the field of rational functions in x with coefficients in R).

The next result describes a relation between the ideals of R and those of $R[x]$.

Proposition 2. Let I be an ideal of the ring R and let $(I) = I[x]$ denote the ideal of $R[x]$ generated by I (the set of polynomials with coefficients in I). Then

$$R[x]/(I) \cong (R/I)[x].$$

In particular, if I is a prime ideal of R then (I) is a prime ideal of $R[x]$.

Proof: There is a natural map $\varphi : R[x] \to (R/I)[x]$ given by reducing each of the coefficients of a polynomial modulo I. The definition of addition and multiplication in these two rings shows that φ is a ring homomorphism. The kernel is precisely the set of polynomials each of whose coefficients is an element of I, which is to say that $\ker\varphi = I[x] = (I)$, proving the first part of the proposition. The last statement follows from Proposition 1, since if I is a prime ideal in R, then R/I is an integral domain, hence also $(R/I)[x]$ is an integral domain. This shows if I is a prime ideal of R, then (I) is a prime ideal of $R[x]$.

Note that it is not true that if I is a maximal ideal of R then (I) is a maximal ideal of $R[x]$. However, if I is maximal in R then the ideal of $R[x]$ generated by I and x is maximal in $R[x]$.

We now give an example of the "reduction homomorphism" of Proposition 2 which will be useful on a number of occasions later ("reduction homomorphisms" were also discussed at the end of Section 7.3 with reference to reducing the integers mod n).

Example

Let $R = \mathbb{Z}$ and consider the ideal $n\mathbb{Z}$ of $\mathbb{Z}$. Then the isomorphism above can be written

$$\mathbb{Z}[x]/n\mathbb{Z}[x] \cong \mathbb{Z}/n\mathbb{Z}[x]$$

and the natural projection map of $\mathbb{Z}[x]$ to $\mathbb{Z}/n\mathbb{Z}[x]$ by reducing the coefficients modulo n is a ring homomorphism. If n is composite, then the quotient ring is not an integral domain. If, however, n is a prime p, then $\mathbb{Z}/p\mathbb{Z}$ is a field and so $\mathbb{Z}/p\mathbb{Z}[x]$ is an integral domain (in fact, a Euclidean Domain, as we shall see shortly). We also see that the set of polynomials whose coefficients are divisible by p is a prime ideal in $\mathbb{Z}[x]$.

We close this section with a description of the natural extension to polynomial rings in *several* variables.

Definition. The *polynomial ring in the variables $x_1, x_2, \ldots, x_n$ with coefficients in R*, denoted $R[x_1. x_2, \ldots, x_n]$, is defined inductively by

$$R[x_1, x_2, \ldots, x_n] = R[x_1, x_2, \ldots, x_{n-1}][x_n]$$

This definition means that we can consider polynomials in n variables with coefficients in R simply as polynomials in *one* variable (say x_n) but now with coefficients that are themselves *polynomials in $n-1$ variables*. In a slightly more concrete formulation, a nonzero polynomial in $x_1, x_2, \ldots, x_n$ with coefficients in R is a finite sum of nonzero *monomial terms*, i.e., a finite sum of elements of the form

$$ax_1^{d_1}x_2^{d_2}\ldots x_n^{d_n}$$

where $a \in R$ (the *coefficient* of the term) and the d_i are nonnegative integers. A monic term $x_1^{d_1}x_2^{d_2}\ldots x_n^{d_n}$ is called simply a *monomial* and is the *monomial part* of the term $ax_1^{d_1}x_2^{d_2}\ldots x_n^{d_n}$. The exponent d_i is called the *degree in x_i* of the term and the sum

$$d = d_1 + d_2 + \cdots + d_n$$

is called the *degree* of the term. The ordered n-tuple $(d_1, d_2, \ldots, d_n)$ is the *multidegree* of the term. The *degree* of a nonzero polynomial is the largest degree of any of its monomial terms. A polynomial is called *homogeneous* or a *form* if all its terms have the same degree. If f is a nonzero polynomial in n variables, the sum of all the monomial terms in f of degree k is called the *homogeneous component of f of degree k*. If f has degree d then f may be written uniquely as the sum $f_0 + f_1 + \cdots + f_d$ where f_k is the homogeneous component of f of degree k, for $0 \leq k \leq d$ (where some f_k may be zero).

Finally, to define a polynomial ring in an *arbitrary* number of variables with coefficients in R we take finite sums of monomial terms of the type above (but where the variables are not restricted to just $x_1, \ldots, x_n$), with the natural addition and multiplication. Alternatively, we could define this ring as the *union* of *all* the polynomial rings in a *finite* number of the variables being considered.

Example

The polynomial ring $\mathbb{Z}[x, y]$ in two variables x and y with integer coefficients consists of all finite sums of monomial terms of the form ax^iy^j (of degree $i+j$). For example,

$$p(x, y) = 2x^3 + xy - y^2$$

and

$$q(x, y) = -3xy + 2y^2 + x^2y^3$$

are both elements of $\mathbb{Z}[x, y]$, of degrees 3 and 5, respectively. We have

$$p(x, y) + q(x, y) = 2x^3 - 2xy + y^2 + x^2y^3$$

and

$$p(x, y)q(x, y) = -6x^4y + 4x^3y^2 + 2x^5y^3 - 3x^2y^2 + 5xy^3 + x^3y^4 - 2y^4 - x^2y^5,$$

a polynomial of degree 8. To view this last polynomial, say, as a polynomial in y with coefficients in $\mathbb{Z}[x]$ as in the definition of several variable polynomial rings above, we would write the polynomial in the form

$$(-6x^4)y + (4x^3 - 3x^2)y^2 + (2x^5 + 5x)y^3 + (x^3 - 2)y^4 - (x^2)y^5.$$

The nonzero homogeneous components of $f = f(x, y) = p(x, y)q(x, y)$ are the polynomials $f_4 = -3x^2y^2 + 5xy^3 - 2y^4$ (degree 4), $f_5 = -6x^4y + 4x^3y^2$ (degree 5), $f_7 = x^3y^4 - x^2y^5$ (degree 7), and $f_8 = 2x^5y^3$ (degree 8).

Each of the statements in Proposition 1 is true for polynomial rings with an arbitrary number of variables. This follows by induction for finitely many variables and from the definition in terms of unions in the case of polynomial rings in arbitrarily many variables.

EXERCISES

1. Let $p(x, y, z) = 2x^2y - 3xy^3z + 4y^2z^5$ and $q(x, y, z) = 7x^2 + 5x^2y^3z^4 - 3x^2z^3$ be polynomials in $\mathbb{Z}[x, y, z]$.
   (a) Write each of p and q as a polynomial in x with coefficients in $\mathbb{Z}[y, z]$.
   (b) Find the degree of each of p and q.
   (c) Find the degree of p and q in each of the three variables x, y and z.
   (d) Compute pq and find the degree of pq in each of the three variables x, y and z.
   (e) Write pq as a polynomial in the variable z with coefficients in $\mathbb{Z}[x, y]$.
2. Repeat the preceding exercise under the assumption that the coefficients of p and q are in $\mathbb{Z}/3\mathbb{Z}$.
3. If R is a commutative ring and $x_1, x_2, \dots, x_n$ are independent variables over R, prove that $R[x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(n)}]$ is isomorphic to $R[x_1, x_2, \dots, x_n]$ for any permutation π of $\{1, 2, \dots, n\}$.
4. Prove that the ideals (x) and (x, y) are prime ideals in $\mathbb{Q}[x, y]$ but only the latter ideal is a maximal ideal.
5. Prove that (x, y) and $(2, x, y)$ are prime ideals in $\mathbb{Z}[x, y]$ but only the latter ideal is a maximal ideal.
6. Prove that (x, y) is not a principal ideal in $\mathbb{Q}[x, y]$.
7. Let R be a commutative ring with 1. Prove that a polynomial ring in more than one variable over R is not a Principal Ideal Domain.
8. Let F be a field and let $R = F[x, x^2y, x^3y^2, \dots, x^ny^{n-1}, \dots]$ be a subring of the polynomial ring $F[x, y]$.
   (a) Prove that the fields of fractions of R and $F[x, y]$ are the same.
   (b) Prove that R contains an ideal that is not finitely generated.
9. Prove that a polynomial ring in infinitely many variables with coefficients in any commutative ring contains ideals that are not finitely generated.
10. Prove that the ring $\mathbb{Z}[x_1, x_2, x_3, \dots]/(x_1x_2, x_3x_4, x_5x_6, \dots)$ contains infinitely many minimal prime ideals (cf. Exercise 36 of Section 7.4).
11. Show that the radical of the ideal $I = (x, y^2)$ in $\mathbb{Q}[x, y]$ is (x, y) (cf. Exercise 30, Section 7.4). Deduce that I is a primary ideal that is not a power of a prime ideal (cf. Exercise 41, Section 7.4).
12. Let $R = \mathbb{Q}[x, y, z]$ and let bars denote passage to $\mathbb{Q}[x, y, z]/(xy - z^2)$. Prove that $\overline{P} = (\overline{x}, \overline{z})$ is a prime ideal. Show that $\overline{xy} \in \overline{P}^2$ but that no power of $\overline{y}$ lies in $\overline{P}^2$. (This shows $\overline{P}$ is a prime ideal whose square is *not* a primary ideal — cf. Exercise 41, Section 7.4).
13. Prove that the rings $F[x, y]/(y^2 - x)$ and $F[x, y]/(y^2 - x^2)$ are not isomorphic for any field F.
14. Let R be an integral domain and let i, j be relatively prime integers. Prove that the ideal $(x^i - y^j)$ is a prime ideal in $R[x, y]$. [Consider the ring homomorphism φ from $R[x, y]$ to $R[t]$ defined by mapping x to t^j and mapping y to t^i. Show that an element of $R[x, y]$