differs from an element in $(x^i - y^j)$ by a polynomial $f(x)$ of degree at most $j-1$ in y and observe that the exponents of $\varphi(x^r y^s)$ are distinct for $0 \le s < j$.]

15. Let $p(x_1, x_2, \dots, x_n)$ be a homogeneous polynomial of degree k in $R[x_1, \dots, x_n]$. Prove that for all $\lambda \in R$ we have $p(\lambda x_1, \lambda x_2, \dots, \lambda x_n) = \lambda^k p(x_1, x_2, \dots, x_n)$.

16. Prove that the product of two homogeneous polynomials is again homogeneous.

17. An ideal I in $R[x_1, \dots, x_n]$ is called a *homogeneous ideal* if whenever $p \in I$ then each homogeneous component of p is also in I. Prove that an ideal is a homogeneous ideal if and only if it may be generated by homogeneous polynomials. [Use induction on degrees to show the "if" implication.]

The following exercise shows that some care must be taken when working with polynomials over noncommutative rings R (the ring operations in $R[x]$ are defined in the same way as for commutative rings R), in particular when considering polynomials as functions.

18. Let R be an arbitrary ring and let $\text{Func}(R)$ be the ring of all functions from R to itself. If $p(x) \in R[x]$ is a polynomial, let $f_p \in \text{Func}(R)$ be the function on R defined by $f_p(r) = p(r)$ (the usual way of viewing a polynomial in $R[x]$ as defining a function on R by "evaluating at r").
   (a) For fixed $a \in R$, prove that "evaluation at a" is a ring homomorphism from $\text{Func}(R)$ to R (cf. Example 4 following Theorem 7 in Section 7.3).
   (b) Prove that the map $\varphi : R[x] \to \text{Func}(R)$ defined by $\varphi(p(x)) = f_p$ is not a ring homomorphism in general. Deduce that polynomial identities need not give corresponding identities when the polynomials are viewed as functions. [If $R = \mathbb{H}$ is the ring of real Hamilton Quaternions show that $p(x) = x^2 + 1$ factors as $(x+i)(x-i)$, but that $p(j) = 0$ while $(j+i)(j-i) \neq 0$.]
   (c) For fixed $a \in R$, prove that the composite "evaluation at a" of the maps in (a) and (b) mapping $R[x]$ to R is a ring homomorphism if and only if a is in the center of R.

9.2 POLYNOMIAL RINGS OVER FIELDS I

We now consider more carefully the situation where the coefficient ring is a *field* F. We can define a *norm* on $F[x]$ by defining $N(p(x))$ = degree of $p(x)$ (where we set $N(0) = 0$). From elementary algebra we know that we can divide one polynomial with, say, rational coefficients by another (nonzero) polynomial with rational coefficients to obtain a quotient and remainder. The same is true over any field.

Theorem 3. Let F be a field. The polynomial ring $F[x]$ is a Euclidean Domain. Specifically, if $a(x)$ and $b(x)$ are two polynomials in $F[x]$ with $b(x)$ nonzero, then there are *unique* $q(x)$ and $r(x)$ in $F[x]$ such that

$$a(x) = q(x)b(x) + r(x) \qquad \text{with } r(x) = 0 \text{ or degree } r(x) < \text{degree } b(x)\,.$$

Proof: If $a(x)$ is the zero polynomial then take $q(x) = r(x) = 0$. We may therefore assume $a(x) \neq 0$ and prove the existence of $q(x)$ and $r(x)$ by induction on n = degree $a(x)$. Let $b(x)$ have degree m. If $n < m$ take $q(x) = 0$ and $r(x) = a(x)$. Otherwise $n \ge m$. Write

$$a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

and

$$b(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0.$$

Then the polynomial $a'(x) = a(x) - \dfrac{a_n}{b_m}x^{n-m}b(x)$ is of degree less than n (we have arranged to subtract the leading term from $a(x)$). Note that this polynomial is well defined because the coefficients are taken from a *field* and $b_m \neq 0$. By induction then, there exist polynomials $q'(x)$ and $r(x)$ with

$$a'(x) = q'(x)b(x) + r(x) \qquad \text{with } r(x) = 0 \text{ or degree } r(x) < \text{degree } b(x).$$

Then, letting $q(x) = q'(x) + \dfrac{a_n}{b_m}x^{n-m}$ we have

$$a(x) = q(x)b(x) + r(x) \qquad \text{with } r(x) = 0 \text{ or degree } r(x) < \text{degree } b(x)$$

completing the induction step.

As for the uniqueness, suppose $q_1(x)$ and $r_1(x)$ also satisfied the conditions of the theorem. Then both $a(x) - q(x)b(x)$ and $a(x) - q_1(x)b(x)$ are of degree less than $m =$ degree $b(x)$. The difference of these two polynomials, i.e., $b(x)(q(x) - q_1(x))$ is also of degree less than m. But the degree of the product of two nonzero polynomials is the sum of their degrees (since F is an integral domain), hence $q(x) - q_1(x)$ must be 0, that is, $q(x) = q_1(x)$. This implies $r(x) = r_1(x)$, completing the proof.

Corollary 4. If F is a field, then $F[x]$ is a Principal Ideal Domain and a Unique Factorization Domain.

Proof: This is immediate from the results of the last chapter.

Recall also from Corollary 8 in Section 8.2 that if R is any commutative ring such that $R[x]$ is a Principal Ideal Domain (or Euclidean Domain) then R must be a field. We shall see in the next section, however, that $R[x]$ is a Unique Factorization Domain whenever R itself is a Unique Factorization Domain.

Examples

(1) By the above remarks the ring $\mathbb{Z}[x]$ is not a Principal Ideal Domain. As we have already seen (Example 3 beginning of Section 7.4) the ideal $(2, x)$ is not principal in this ring.

(2) $\mathbb{Q}[x]$ is a Principal Ideal Domain since the coefficients lie in the field $\mathbb{Q}$. The ideal generated in $\mathbb{Z}[x]$ by 2 and x is not principal in the subring $\mathbb{Z}[x]$ of $\mathbb{Q}[x]$. However, the ideal generated in $\mathbb{Q}[x]$ is principal; in fact it is the entire ring (so has 1 as a generator) since 2 is a unit in $\mathbb{Q}[x]$.

(3) If p is a prime, the ring $\mathbb{Z}/p\mathbb{Z}[x]$ obtained by reducing $\mathbb{Z}[x]$ modulo the prime ideal (p) is a Principal Ideal Domain, since the coefficients lie in the field $\mathbb{Z}/p\mathbb{Z}$. This example shows that the quotient of a ring which is not a Principal Ideal Domain *may* be a Principal Ideal Domain. To follow the ideal $(2, x)$ above in this example, note that if $p = 2$, then the ideal $(2, x)$ reduces to the ideal (x) in the quotient $\mathbb{Z}/2\mathbb{Z}[x]$, which is a proper (maximal) ideal. If $p \neq 2$, then 2 is a unit in the quotient, so the ideal $(2, x)$ reduces to the entire ring $\mathbb{Z}/p\mathbb{Z}[x]$.

(4) $\mathbb{Q}[x, y]$, the ring of polynomials in two variables with rational coefficients, is *not* a Principal Ideal Domain since this ring is $\mathbb{Q}[x][y]$ and $\mathbb{Q}[x]$ is not a field (any element

of positive degree is not invertible). It is an exercise to see that the ideal (x, y) is not a principal ideal in this ring. We shall see shortly that $\mathbb{Q}[x, y]$ *is* a Unique Factorization Domain.

We note that the quotient and remainder in the Division Algorithm applied to $a(x), b(x) \in F[x]$ are *independent of field extensions* in the following sense. Suppose the field F is contained in the field E and $a(x) = Q(x)b(x) + R(x)$ for some $Q(x)$, $R(x)$ satisfying the conditions of Theorem 3 in $E[x]$. Write $a(x) = q(x)b(x)+r(x)$ for some $q(x), r(x) \in F[x]$ and apply the uniqueness condition of Theorem 3 in the ring $E[x]$ to deduce that $Q(x) = q(x)$ and $R(x) = r(x)$. In particular, $b(x)$ divides $a(x)$ in the ring $E[x]$ if and only if $b(x)$ divides $a(x)$ in $F[x]$. Also, the greatest common divisor of $a(x)$ and $b(x)$ (which can be obtained from the Euclidean Algorithm) is the same, once we make it unique by specifying it to be monic, whether these elements are viewed in $F[x]$ or in $E[x]$.

EXERCISES

Let F be a field and let x be an indeterminate over F.

1. Let $f(x) \in F[x]$ be a polynomial of degree $n \geq 1$ and let bars denote passage to the quotient $F[x]/(f(x))$. Prove that for each $\overline{g(x)}$ there is a unique polynomial $g_0(x)$ of degree $\leq n - 1$ such that $\overline{g(x)} = \overline{g_0(x)}$ (equivalently, the elements $\bar{1}, \bar{x}, \dots, \overline{x^{n-1}}$ are a *basis* of the vector space $F[x]/(f(x))$ over F — in particular, the dimension of this space is n). [Use the Division Algorithm.]

2. Let F be a finite field of order q and let $f(x)$ be a polynomial in $F[x]$ of degree $n \geq 1$. Prove that $F[x]/(f(x))$ has q^n elements. [Use the preceding exercise.]

3. Let $f(x)$ be a polynomial in $F[x]$. Prove that $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible. [Use Proposition 7, Section 8.2.]

4. Let F be a finite field. Prove that $F[x]$ contains infinitely many primes. (Note that over an infinite field the polynomials of degree 1 are an infinite set of primes in the ring of polynomials).

5. Exhibit *all* the ideals in the ring $F[x]/(p(x))$, where F is a field and $p(x)$ is a polynomial in $F[x]$ (describe them in terms of the factorization of $p(x)$).

6. Describe (briefly) the ring structure of the following rings:
(a) $\mathbb{Z}[x]/(2)$, (b) $\mathbb{Z}[x]/(x)$, (c) $\mathbb{Z}[x]/(x^2)$, (d) $\mathbb{Z}[x, y]/(x^2, y^2, 2)$.
Show that $\alpha^2 = 0$ or 1 for every α in the last ring and determine those elements with $\alpha^2 = 0$. Determine the characteristics of each of these rings (cf. Exercise 26, Section 7.3).

7. Determine all the ideals of the ring $\mathbb{Z}[x]/(2, x^3 + 1)$.

8. Determine the greatest common divisor of $a(x) = x^3 - 2$ and $b(x) = x + 1$ in $\mathbb{Q}[x]$ and write it as a linear combination (in $\mathbb{Q}[x]$) of $a(x)$ and $b(x)$.

9. Determine the greatest common divisor of $a(x) = x^5+2x^3+x^2+x+1$ and the polynomial $b(x) = x^5 + x^4 + 2x^3 + 2x^2 + 2x + 1$ in $\mathbb{Q}[x]$ and write it as a linear combination (in $\mathbb{Q}[x]$) of $a(x)$ and $b(x)$.

10. Determine the greatest common divisor of $a(x) = x^3+4x^2+x-6$ and $b(x) = x^5-6x+5$ in $\mathbb{Q}[x]$ and write it as a linear combination (in $\mathbb{Q}[x]$) of $a(x)$ and $b(x)$.

11. Suppose $f(x)$ and $g(x)$ are two nonzero polynomials in $\mathbb{Q}[x]$ with greatest common divisor $d(x)$.