CHAPTER 8

Polynomial Rings

8.1. Introduction and Elementary Properties

Suppose that R is a ring, not necessarily commutative. We write

$$R[X] = \{a_0 + a_1X + a_2X^2 + \ldots + a_nX^n : n \geqslant 0,\ a_0, a_1, \ldots, a_n \in R\};$$

in other words, $R[X]$ denotes the set of all polynomials with coefficients in the ring R. Furthermore, for any two polynomials $a(X), b(X) \in R[X]$, where

$$a(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n \quad \text{and} \quad b(X) = b_0 + b_1X + b_2X^2 + \ldots + b_mX^m,$$

we define *addition* and *multiplication* as follows: Adding zero coefficients if necessary, we may write

$$a(X) = a_0 + a_1X + a_2X^2 + \ldots + a_pX^p \quad \text{and} \quad b(X) = b_0 + b_1X + b_2X^2 + \ldots + b_pX^p,$$

where $p = \max\{n, m\}$. Then we let

$$a(X) + b(X) = (a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 + \ldots + (a_p + b_p)X^p.$$

On the other hand, we let

$$a(X)b(X) = c_0 + c_1X + c_2X^2 + \ldots + c_{n+m}X^{n+m}, \tag{8.1}$$

where for every $j = 0, 1, 2, \ldots, n + m$,

$$c_j = a_0b_j + a_1b_{j-1} + a_2b_{j-2} + \ldots + a_jb_0. \tag{8.2}$$

It is not difficult to prove the following result.

THEOREM 8.1. *Suppose that R is a ring. Then $R[X]$ is also a ring.*

The proofs of the next two results are almost trivial.

PROPOSITION 8.2. *Suppose that R is a commutative ring. Then $R[X]$ is also a commutative ring.*

PROPOSITION 8.3. *Suppose that the ring R has unity 1. Then $R[X]$ has unity 1.*

PROPOSITION 8.4. *Suppose that R is an integral domain. Then $R[X]$ is also an integral domain.*

PROOF. In view of Propositions 8.2 and 8.3, it remains to show that $R[X]$ has no zero divisors. Suppose that $a(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$ and $b(X) = b_0 + b_1X + b_2X^2 + \ldots + b_mX^m$, where $a_n \neq 0$ and $b_m \neq 0$. Then $a(X)b(X)$ satisfies (8.1) with $c_{n+m} = a_nb_m$. Since R is an integral domain, it follows that $a_nb_m \neq 0$, so that $a(X)b(X) \neq 0$. Hence $R[X]$ is an integral domain. ○

REMARK. Note that we have proved a result on the degree of the polynomial $a(X)b(X)$.

PROPOSITION 8.5. *For every ring R, the ring $R[X]$ is not a field.*

PROOF. If R has no unity, then $R[X]$ has no unity, and is therefore not a field. We may therefore assume that R has unity 1, so that $R[X]$ has unity 1. Then the polynomial X has no multiplicative inverse. To see this, note that for every $a(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n \in R[X]$, where $a_n \neq 0$, we have

$$Xa(X) = a_0X + a_1X^2 + a_2X^3 + \ldots + a_nX^{n+1}.$$

Since $a_n \neq 0$, the polynomial on the right hand side is non-constant, and so $Xa(X) \neq 1$. $\bigcirc$

EXAMPLES. (1) The rings $\mathbb{Q}[X]$ and $\mathbb{R}[X]$ are familiar.
(2) In $\mathbb{Z}_3[X]$, we have $(1 + 2X^2 + X^5)(X + X^4) = X + 2X^3 + X^4 + X^9$.
(3) In $\mathbb{Z}_6[X]$, we have $(2X^3 + 4X + 2)(3X^2 + 3) = 0$.

8.2. Factorization Properties

DEFINITION. Suppose that R is a field, and that $a(X) \in R[X]$ is a non-constant polynomial. Then $a(X)$ is said to be irreducible over R if the following condition holds: If $b(X), c(X) \in R[X]$ satisfy $a(X) = b(X)c(X)$, then $b(X)$ or $c(X)$ is constant.

EXAMPLE. The polynomial $X^2 - 3$ is irreducible over $\mathbb{Q}[X]$ but $X^2 - 3 = (X + \sqrt{3})(X - \sqrt{3})$ in $\mathbb{R}[X]$.

As in this example, we shall, for the remainder of this chapter, abuse notation by using $a(X) - b(X)$ to denote $a(X) + (-b(X))$.

As in factorization of integers, the first result is naturally the Division algorithm.

PROPOSITION 8.6. *Suppose that R is a field. Suppose further that $a(X), b(X) \in R[X]$, and that $a(X) \neq 0$. Then there exist unique polynomials $q(X), r(X) \in R[X]$ such that*
(i) *$b(X) = a(X)q(X) + r(X)$; and*
(ii) *either $r(X) = 0$ or $\deg r(X) < \deg a(X)$.*

PROOF. Consider all polynomials of the form $b(X) - a(X)Q(X)$, where $Q(X) \in R[X]$. If there exists $q(X) \in R[X]$ such that $b(X) - a(X)q(X) = 0$, then our proof is complete. Suppose now that $b(X) - a(X)Q(X) \neq 0$ for any $Q(X) \in R[X]$. Then

$$m = \min\{\deg(b(X) - a(X)Q(X)) : Q(X) \in R[X]\}$$

exists. Let $q(X) \in R[X]$ satisfy $\deg(b(X) - a(X)q(X)) = m$, and let $r(X) = b(X) - a(X)q(X)$. Then $\deg r(X) < \deg a(X)$, for otherwise, writing

$$a(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n \quad \text{and} \quad r(X) = r_0 + r_1X + r_2X^2 + \ldots + r_mX^m,$$

where $m \geqslant n$, we have

$$r(X) - (r_m a_n^{-1} X^{m-n})a(X) = b(X) - a(X)(q(X) + r_m a_n^{-1} X^{m-n}) \in R[X].$$

Clearly $\deg(r(X) - (r_m a_n^{-1} X^{m-n})a(X)) < \deg r(X)$, contradicting the minimality of m. On the other hand, suppose that $q_1(X), q_2(X) \in R[X]$ satisfy

$$\deg(b(X) - a(X)q_1(X)) = m \quad \text{and} \quad \deg(b(X) - a(X)q_2(X)) = m.$$

Let $r_1(X) = b(X) - a(X)q_1(X)$ and $r_2(X) = b(X) - a(X)q_2(X)$. Then

$$r_1(X) - r_2(X) = a(X)(q_2(X) - q_1(X)).$$

If $q_1(X) \neq q_2(X)$, then $\deg(a(X)(q_2(X) - q_1(X))) \geqslant \deg a(X)$, while $\deg(r_1(X) - r_2(X)) < \deg a(X)$, a contradiction. It follows that $q(X)$, and hence $r(X)$, is unique. $\bigcirc$

Recall the Fundamental theorem of algebra, that for any polynomial $b(X) \in \mathbb{C}[X]$, a number $x \in \mathbb{C}$ is a root of $b(X)$ if and only if $X - x$ is a factor of $b(X)$. Our task here is to prove the analogue for a commutative polynomial ring with unity. We need some intermediate results. The proof of the first of these is simple.

LEMMA 8.7. *Suppose that R is a ring, and that $p(X) = a(X) + b(X)$ in $R[X]$. Then for every $x \in R$, $p(x) = a(x) + b(x)$.*

Note that we do not require the ring R to be commutative in Lemma 8.7. However, for our next intermediate result, we have to make this assumption.

LEMMA 8.8. *Suppose that R is a commutative ring, and that $p(X) = a(X)b(X)$ in $R[X]$. Then for every $x \in R$, $p(x) = a(x)b(x)$.*

PROOF. Note that if $a(X) = a_0+a_1X+a_2X^2+\ldots+a_nX^n$ and $b(X) = b_0+b_1X+b_2X^2+\ldots+b_mX^m$, then $p(X) = a(X)b(X)$ satisfies (8.1) and (8.2), so that

$$p(x) = c_0 + c_1x + c_2x^2 + \ldots + c_{n+m}x^{n+m} = \sum_{j=0}^{n+m} c_jx^j. \tag{8.3}$$

On the other hand, since R is a commutative ring,

$$\begin{aligned} a(x)b(x) &= (a_0 + a_1x + a_2x^2 + \ldots + a_nx^n)(b_0 + b_1x + b_2x^2 + \ldots + b_mx^m) \\ &= \sum_{j=0}^{n+m}\sum_{i=0}^{j} a_ix^ib_{j-i}x^{j-i} = \sum_{j=0}^{n+m}\sum_{i=0}^{j} a_ib_{j-i}x^ix^{j-i} \\ &= \sum_{j=0}^{n+m}\left(\sum_{i=0}^{j} a_ib_{j-i}\right)x^j = \sum_{j=0}^{n+m} c_jx^j. \end{aligned} \tag{8.4}$$

It follows on combining (8.3) and (8.4) that $p(x) = a(x)b(x)$. ○

Our next result is a generalization of the Division algorithm to monic divisors over a commutative ring.

LEMMA 8.9. *Suppose that R is a commutative ring. Suppose further that $b(X) \in R[X]$, and that $x \in R$. Then there exist unique polynomials $q(X), r(X) \in R[X]$ such that $b(X) = (X-x)q(X)+r(X)$ and $r(X)$ is a constant polynomial.*

PROOF. This is similar to Proposition 8.6 with $a(X) = X - x$. However, R is only a commutative ring, so we need to make modifications. Note that in the terminology of the proof of Proposition 8.6, we have $n = 1$ and $a_n = a_1 = 1$. It follows that the polynomial $r(X)$ in the proof of Proposition 8.6 has degree less than $\deg(X - x) = 1$, so that $r(X)$ is a constant. We need to prove that $q(X)$, and hence $r(X)$, is uniquely determined. Suppose that $q_1(X), q_2(X) \in R[X]$ are such that both $b(X)-(X-x)q_1(X)$ and $b(X)-(X-x)q_2(X)$ are constant but different. Then $(X-x)(q_1(X)-q_2(X))$ is a non-zero constant. On the other hand, writing $q_1(X) - q_2(X) = s_0 + s_1X + s_2X^2 + \ldots + s_kX^k$, where $s_k \neq 0$, we conclude that $(X - x)(q_1(X) - q_2(X)) = -xs_0 + \ldots + s_kX^{k+1}$ is non-constant, a contradiction. ○

THEOREM 8.10. *Suppose that R is a commutative ring with unity, and that $b(X) \in R[X]$ is non-constant. Then $x \in R$ is a root of $b(X)$ if and only if $X - x$ is a factor of $b(X)$.*

PROOF. ($\Rightarrow$) By Lemma 8.9, there exist a unique polynomial $q(X) \in R[X]$ and a unique element $r \in R$ such that $b(X) = (X - x)q(X) + r$. It now follows from Lemmas 8.7 and 8.8 that

$$0 = b(x) = (x - x)q(x) + r = r.$$

Hence $r = 0$, so that $b(X) = (X - x)q(X)$, whence $(X - x)$ is a factor of $b(X)$.

($\Leftarrow$) Suppose that $(X - x)$ is a factor of $b(X)$, so that $b(X) = (X - x)q(X)$ for some $q(X) \in R[X]$. It follows from Lemmas 8.7 and 8.8 that $b(x) = (x - x)q(x) = 0$, so that x is a root of $b(X)$. ○

We conclude this chapter by proving the following important result.

THEOREM 8.11. *Suppose that R is an integral domain, and that the polynomial $b(X) \in R[X]$ is non-zero and has degree $n \geqslant 0$. Then $b(X)$ has at most n roots in R.*

PROOF. We shall prove the following by induction on n:

$P(n)$: Any polynomial $b(X) \in R[X]$ of degree n has at most n roots in R. If these roots are $x_1, x_2, \ldots, x_m$, where $m \leqslant n$, then $b(X) = (X - x_1)(X - x_2)\ldots(X - x_m)s(X)$, where $s(X) \in R[X]$ has no roots in R.

Clearly $P(0)$ is true. Suppose now that $P(k)$ is true. Let $b(X) \in R[X]$ have degree $k + 1$. If $b(X)$ has no roots in R, the proof is complete. Otherwise, let $x_0 \in X$ be a root of $b(X)$. Then by Theorem 8.10, $b(X) = (X - x_0)q(X)$, where $q(X) \in R[X]$ has degree k, and therefore has at most k roots in R. Let the roots of $q(X)$ be $x_1, x_2, \ldots, x_m$, where $m \leqslant k$. Then $q(X)$ has factorization

$q(X) = (X - x_1)(X - x_2) \dots (X - x_m)s(X)$, where $s(X) \in R[X]$ has no roots in R. It follows that $b(X) = (X - x_0)(X - x_1)(X - x_2) \dots (X - x_m)s(X)$. Now let $x \in R \setminus \{x_0, x_1, x_2, \dots, x_m\}$. Then

$$b(x) = (x - x_0)(x - x_1)(x - x_2) \dots (x - x_m)s(x).$$

Note that the terms on the right hand side are all non-zero. Since R is an integral domain, it follows that $b(x) \neq 0$. Hence $b(X)$ has $m + 1 \leqslant k + 1$ roots. $\bigcirc$

However, if the ring R is not an integral domain, then we may have more roots than the degree of the polynomial. See Problems 2 and 3.

Problems for Chapter 8

1. For each of the following polynomials, factorize the polynomial within the given polynomial ring:
   (i) $X^2 + X + 3$ in $\mathbb{Z}_5[X]$
   (ii) $X^3 + 2X^2 + 6X + 1$ in $\mathbb{Z}_{11}[X]$
   (iii) $X^4 + X^3 + 2X + 2$ in $\mathbb{Z}_3[X]$
2. For each of the following polynomials within the given polynomial rings, find all the roots:
   (i) $X^2 + X + 8$ in $\mathbb{Z}_{10}[X]$
   (ii) $X^2 + 4X + 4$ in $\mathbb{Z}_8[X]$
   (iii) $X^3 + 7X$ in $\mathbb{Z}_8[X]$
3. Consider the polynomial $X^3 + 5X^2 + 6X$ in $\mathbb{Z}_{10}[X]$.
   (i) Find all the roots $x \in \mathbb{Z}_{10}$ of the polynomial.
   (ii) Find three different factorizations of the polynomial in $\mathbb{Z}_{10}[X]$.
   (iii) Comment on the results.
4. Consider the collection of all cubic polynomials in $\mathbb{Z}_2[X]$.
   (i) Determine which of these are irreducible in $\mathbb{Z}_2[X]$.
   (ii) Find a proper factorization of each of the remaining cases.
5. Give an example of a polynomial $a(X) \in \mathbb{Z}[X]$ which satisfies all the following conditions:
   (i) $a(X)$ has degree 3.
   (ii) There exist three polynomials $b_1(X), b_2(X), b_3(X) \in \mathbb{Z}[X]$, each one of degree 1, such that $a(X) = b_1(X)b_2(X)b_3(X)$ in $\mathbb{Z}[X]$.
   (iii) $a(X)$ has no roots in $\mathbb{Z}$.