Chapter 2

Polynomial Rings and Factorization

2.1 Polynomial Rings

If R is any ring, we can define the ring $R[x]$ of polynomials with coefficients in R. If F is a field, then the polynomial ring $F[x]$ is a particular interest. Polynomial rings over fields have some resemblance to the ring $\mathbb{Z}$ of integers in terms of their divisibility properties. Integers can sometimes be factorized in nontrivial ways and sometimes not, and every integer $\geqslant 2$ can be written in a (more or less) unique manner as a product of primes, which are "elementary components" of integers with respect to multiplication. The theme of this chapter is to explore analagous properties of polynomial rings over fields. Note that notions like factorization and prime are lost when we move from the integers to the rational numbers. That every non-zero element is a unit in $\mathbb{Q}$ means that essentially everything is a divisor of everything, so the elaborate structure of factorization in $\mathbb{Z}$ just collapses when we move to $\mathbb{Q}$.

The theory of divsibility and factorization in $\mathbb{Z}$ is really driven by the *division algorithm*, which says that for any integers a and b, with $b > 0$, there are unique integers q (the quotient) and r the remainder, for which

$$a = qb + r,$$

and $0 \leqslant r < b$. The statement of the division algorithm makes important reference to the order relation on $\mathbb{Z}$ ("$0 \leqslant r < b$"). In this chapter we will think about other classes of rings that have a division algorithm. This requires some properties, but not necessarily anything as strong as the order relation that we have in $\mathbb{Z}$.

Definition 12. *Let R be a ring. A* polynomial *in X with coefficients in R is an expression of the form*

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

where $n \geqslant 0$ is an integer and $a_i \in R$ for $i = 0, \ldots, n$.
The set of all such expressions is denoted by $R[X]$.

Note: The symbol X is an *indeterminate*. The expressions

$$a_m X^m + a_{m-1} X^{m-1} + \cdots + a_1 X + a_0 \text{ and } b_n X^n + b_{n-1} X^{n-1} + \cdots + b_1 X + b_0$$

are (by definition) equal in $R[X]$ if and only if $a_i = b_i$ for all $i \geqslant 0$. (Here we assign $a_j = 0$ for $j > m$ and $b_j = 0$ for $j > n$, in order for the statement " $a_i = b_i$ for all $i \geqslant 0$" to make sense.)

The set $R[X]$ is a ring under polynomial addition and multiplication, which are defined as follows. Let

$$\begin{aligned} f(X) &= a_m X^m + a_{m-1} X^{m-1} + \cdots + a_1 X + a_0 \\ g(X) &= b_n X^n + b_{n-1} X^{n-1} + \cdots + b_1 X + b_0 \end{aligned}$$

be elements of $R[X]$.

- The sum $f(X)+g(X)$ is the polynomial in which the constant term is a_0+b_0 and the coefficient of X^i is $a_i + b_i$ for $i \geqslant 1$.
- The product $f(X)g(X)$ has constant term a_0b_0. For $i > m + n$ the coefficient of X^i is 0 and for $i \leqslant m + n$ the coefficient of X^i is

$$\sum_{j=0}^{i} a_j b_{i-j}.$$

(For example the coefficient of X^2 is $a_0b_2 + a_1b_1 + a_2b_0$).

Notes:

1. $R[X]$ is commutative if and only if R is commutative.
2. The identity element for multiplication in $R[X]$ is the identity element 1_R of R.
3. Those polynomials in $R[X]$ in which the coefficient of X^i is zero whenever $i \geqslant 1$ (i.e. those in which the indeterminate X does not actually appear) are called the *constant* polynomials. They are just the elements of R.

   The set of constant polynomials is itself a ring under the operations of $R[X]$ (which for the constant polynomials are just the addition and multiplication of R). We say that R is a *subring* of $R[X]$).

The remarks above show that the properties of $R[X]$ are influenced by the properties of R. We will shortly assume that R is an integral domain, and later that R is a field.

Definition 13. *Let R be a ring. The* degree *of a (non-zero) polynomial $f(X)$ in $R[X]$ is defined to be the maximum i for which X^i appears with non-zero coefficient in $f(X)$, if any such i exists. The degree of a non-zero constant polynomial is zero. The degree of the zero polynomial is not defined.*

So associated to every non-zero polynomial we have its *degree*, which is a non-negative integer. The next item describes how the degree behaves with regard to multiplication in polynomial rings over integral domains.

Lemma 14. *Let R be an integral domain and let $f(X)$ and $g(X)$ be non-zero elements of $R[X]$ of degrees m and n respectively. Then the polynomial $f(X)g(X)$ has degree $m + n$.*

Proof: Write

$$\begin{aligned} f(X) &= a_mX^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0,\ a_m \neq 0 \\ g(X) &= b_nX^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0,\ b_n \neq 0 \end{aligned}$$

Then the highest power of X to possibly appear in the product $f(X)g(X)$ is X^{m+n} which has coefficient a_mb_n. This element is not zero in R since it is the product of two non-zero elements in a ring without zero-divisors. □

Corollary 15. *If R is an integral domain then $R[X]$ is also an integral domain.*

Corollary 16. *Let R be an integral domain. Then the unit group of $R[X]$ is just the unit group of R.*

NOTE: This is saying that the only elements of $R[X]$ that are units in $R[X]$ are those constant polynomials which are units in R.

Proof: The identity element of $R[X]$ is the constant polynomial 1_R, which is also the identity element of R. Since $R \subset R[X]$ and $1_R \in R$, it is clear that $\mathcal{U}(R) \subseteq \mathcal{U}(R[X])$.

On the other hand suppose that $f(X)$ is a non-constant polynomial in $R[X]$, so $\deg(f(X)) \geqslant 1$. If $g(X)$ is a non-zero element of $F[X]$, then

$$\deg(f(X)g(X)) = \deg(f(X)) + \deg(g(X)) \geqslant 1,$$

so $f(X)g(X) \neq 1_R$. Thus $f(X)$ has no inverse in $R[X]$ and $f(X)$ does not belong to $\mathcal{U}(R[X])$.

Example: If F is a field then $\mathcal{U}(F[X]) = F^\times$, the multiplicative group of non-zero elements of F.

Question to think about Suppose that R is not an integral domain. Then could it happen that a non-constant polynomial could be a unit in $R[X]$?