

Chapter 2

Factorization in Polynomial Rings

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 ≥ 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.

QUESTION FOR THE SEMINAR : Why is this?

Definition 2.1.1 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 $n \geq 0$ is an integer and $a_i \in R$ for $i = 0, \dots, n$.

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 $i \geq 0$. (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 $i \geq 0$ ” 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 $i \geq 1$.
- The product $f(x)g(x)$ has constant term $a_0 b_0$. For $i > m + n$ the coefficient of x^i is 0 and for $i \leq m + n$ the coefficient of x^i is

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

(For example the coefficient of x^2 is $a_0 b_2 + a_1 b_1 + a_2 b_0$).

NOTES:

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

Of course 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 2.1.2 *Let R be a ring. The degree of a 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 result describes how the degree behaves with regard to multiplication in polynomial rings over integral domains.

Lemma 2.1.3 *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

$$\begin{aligned}f(x) &= a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0, \quad a_m \neq 0 \\g(x) &= b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0, \quad b_n \neq 0\end{aligned}$$

Then the highest power of x to possibly appear in the product $f(x)g(x)$ is x^{m+n} which has coefficient $a_m b_n$. Note that this element is not zero in R since it is the product of two non-zero elements in a ring without zero-divisors. \square

Corollary 2.1.4 *If R is an integral domain then $R[x]$ is also an integral domain.*

Proof: Exercise for the seminar.

Corollary 2.1.5 *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 $\deg(f(x)) \geq 1$. If $g(x)$ is a non-zero element of $R[x]$, then

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)) \geq 1,$$

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 FOR THE SEMINAR: Suppose that R is not an integral domain. Then could it happen that a non-constant polynomial could be a unit in $R[x]$?