5 Polynomial Rings

Definition 5.1 Let R be a commutative ring. The set of formal symbols

$$R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in R,\ n \in \boldsymbol{Z}^+\}$$

is called the *ring of polynomials over* R *in the indeterminate* x.

Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \text{ and } g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

be elements of $R[x]$. (Assume $a_i = 0$ if $i > n$ and $b_j = 0$ if $j > m$.)

(i) Two elements f and g are equal if and only if $a_i = b_i$ for all i.

(ii) $f(x) + g(x) = (a_\ell + b_\ell)x^\ell + \cdots + (a_1 + b_1)x + (a_0 + b_0)$. where $\ell = \max\{n, m\}$.

(iii) $f(x)g(x) = c_{m+n}x^{m+n} + c_{m+n-1}x^{m+n-1} + \cdots + c_1 x + c_0$, where

$$c_k = a_k b_0 + a_{k-1}b_1 + \cdots + a_1 b_{k-1} + a_0 b_k$$

for $k = 0, 1, \ldots, m + n$.

When $a_n \neq 0$, we write $\deg f(x) = n$, a_n is called the *leading coefficient* and n the *degree* of $f(x)$. We define $\deg 0 = -\infty$[12]. When R has a unity, a polynomial with unity as its leading coefficient is said to be *monic*.

Remarks. Formally it is better to define

$$R[x] = \{(a_0, a_1, a_2, \ldots, a_i, \ldots) \mid a_i \in R \text{ only finitely many } a_i\text{'s are nonzero}\}.$$

Consider also $R[[x]]$, the ring of formal power series

$$R[[x]] = \{(a_0, a_1, a_2, \ldots, a_i, \ldots) \mid a_i \in R\},$$

$R[x, x^{-1}]$. the ring of Laurent polynomials

$$R[x, x^{-1}] = \{(\ldots, a_{-i}, \ldots, a, a_{-1}, a_0, a_1, a_2, \ldots, a_i, \ldots) \mid \text{ only finitely many } a_i \in R \text{ are nonzero}\},$$

and $R((x))$, the ring of Laurent series,

$$R((x)) = \{(\ldots, a_{-i}, \ldots, a, a_{-1}, a_0, a_1, a_2, \ldots, a_i, \ldots) \mid \text{ only finitely many } a_i \in R\ i < 0 \text{ are nonzero}\}.$$

Proposition 5.1 (Theorem 16.1) *Let* R *be a commutative ring and let*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \text{ and } g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

with $a_n \neq 0 \neq b_m$.

(i) $\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$.

[12] In the textbook no degree is defined for 0.

(ii) $\deg(f(x)g(x)) \le \deg f(x) + \deg g(x)$. *Equality holds if* $a_n b_m \neq 0$.

(iii) *If* R *is an integral domain,* $R[x]$ *is an integral domain. Moreover,* $U(R[x]) = U(R)$.

Proposition 5.2 (Theorem 16.2, Corollaries 1, 2) *Let* F *be a field.*

(i) *Let* $f(x), g(x) \in F[x]$ *with* $g(x) \neq 0$. *Then there exist unique polynomials* $q(x)$ *and* $r(x)$ *in* $F[x]$ *such that* $f(x) = g(x)q(x) + r(x)$ *and (either* $r(x) = 0$ *or)* $\deg r(x) < \deg g(x)$.

(ii) *Let* $f(x) \in F[x]$ *and* $a \in F$. *Then* $f(x) = q(x)(x-a) + f(a)$ *for some* $q(x) \in F[x]$. *In particular,* $x - a$ *is a factor of* $f(x)$ *if and only if* $f(a) = 0$.

(iii) *A nonzero polynomial of degree* n *has at most* n *zeros, counting multiplicity.*

Proof. (i) Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \text{ and } g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

be elements of $F[x]$. If $m > n$, then set $q(x) = 0$ and $r(x) = f(x)$. Then $f(x) = 0 \cdot g(x) + f(x)$ and $\deg f < \deg g$. Assume $m \ge n$. Then $f_1(x) = f(x) - b_m^{-1} a_n x^{n-m} g(x)$ is a polynomial of degree at most $n-1$. Hence by induction there exists $q_1(x)$ and $r(x)$ with $\deg r < \deg g$ such that $f_1(x) = q_1(x)g(x) + r(x)$. Thus by setting $q(x) = q_1(x) + b_m^{-1} a_n x^{n-m}$,

$$f(x) = ((q_1(x) + b_m^{-1} a_n x^{n-m})g(x) + r(x) = q(x)g(x) + r(x).$$

(ii) If $f(x) = q(x)(x-a) + r(x)$ with $\deg r(x) < \deg(x-a) = 1$, with $r(x) = r \in F$, Moreover, $f(a) = r$. Thus, we have the expression.

(iii) If $f(x)$ is a nonzero constant, there is no zero. Suppose $f(a) = 0$. Then $f(x) = f_1(x)(x-a)$ and $\deg f_1(x) = n-1$. By induction, the zeros of $f(x)$ that are not equal to a are the zeros of $f_1(x)$ and its number does not exceed $n-1$. ∎

Remarks.

1. Proposition 5.2 (i) the expression $f(x) = g(x)q(x) + r(x)$ and (either $r(x) = 0$ or) $\deg r(x) < \deg g(x)$ exists if R has a unity and the leading coefficient of $g(x)$ is a unit. Moreover, if R is an integral domain, uniqueness also holds.

2. If F is an integral domain, (ii) and (iii) hold.

3. If F is an integral domain, $f(a) = g(a)$ for all $a \in F$ impies that either $f(x) = g(x)$ or $\deg(f(x) - g(x)) \ge |F|$.

Definition 5.2 A *principal ideal domain* (PID) is an integral domain R in which every ideal has the form $\langle a \rangle = \{ra \mid r \in R\}$ for some $a \in R$.

Theorem 5.3 (Theorem 16.3) *Let* F *be a field. Then* $F[x]$ *is a principal ideal domain, i.e., if* A *is an ideal of* $F[x]$, *then there is a polynomial* $f(x) \in F[x]$ *such that* $A = \langle f(x) \rangle$. *Moreover, if* A *is a nonzero ideal in* $F[x]$, $A = \langle f(x) \rangle$ *if and only if* $f(x)$ *is a nonzero polynomial of minimal degree in* A.

Proof. Let A be a nonzero ideal in $F[x]$ and let $f(x)$ be a nonzero polynomial of minimal degree in A. Let $g(x) \in A$ and let $g(x) = q(x)f(x) + r(x)$ with $q(x), r(x) \in F[x]$ and $\deg r(x) < \deg f(x)$. Since $r(x) = g(x) - q(x)f(x) \in A$ as $g(x), f(x) \in A$, we have $r(x) = 0$ by the minimality of the degree of $f(x)$ as a nonzero element in A. Hence $g(x) \in \langle f(x) \rangle$. Therefore $A = \langle f(x) \rangle$ and $F[x]$ is a principal ideal domain. Conversely if $A = \langle h(x) \rangle$, and $f(x)$ is the polynomial chosen above. Then $f(x) \in A$ and $0 \neq f(x) = g(x)h(x)$. So $\deg h(x) \leq \deg f(x) \leq \deg h(x)$, and $h(x)$ is a nonzero polynomial of minimal degree in A. ∎