Course 12: 17.05.2021

2.7 Polynomial rings (continued)

Definition 2.7.7 Let $0 \neq f \in R[X]$ be a polynomial with unique algebraic form

$$f = a_0 + a_1X + \cdots + a_nX^n \,,$$

where $a_0, \ldots, a_n \in R$ and $a_n \neq 0$. Then n is called the *degree* of f and is denoted by $deg(f)$.

By convention, the degree of the zero polynomial is $-\infty$.

Theorem 2.7.8 *Let $f, g \in R[X]$. Then:*
(i) $deg(f + g) \leq \max(deg(f), deg(g))$;
(ii) $deg(f \cdot g) \leq deg(f) + deg(g)$;
(iii) If R is an integral domain, then

$$deg(f \cdot g) = deg(f) + deg(g) \,.$$

Proof. If $f = 0$ or $g = 0$, then the properties (i) and (ii) hold by assuming the conventions $-\infty + n = n + (-\infty) = -\infty$, $(-\infty) + (-\infty) = -\infty$ and $-\infty \leq n$, $\forall n \in \mathbb{N}$.

Consider now the non-trivial cases, when $f = \sum_{i=0}^{m} a_iX^i$, $g = \sum_{j=0}^{n} b_jX^j \in R[X]$, where $a_m \neq 0$ and $b_n \neq 0$. Hence $deg(f) = m \geq 0$ and $deg(g) = n \geq 0$.

(i) We may suppose that $m \geq n$. Then

$$f + g = \sum_{j=0}^{n}(a_j + b_j)X^j + \sum_{i=n+1}^{m} a_iX^i \in R[X] \,,$$

hence $deg(f + g) \leq m$.

(ii) We have

$$f \cdot g = a_0b_0 + (a_0b_1 + a_1b_0)X + \cdots + (a_mb_n)X^{m+n} \in R[X] \,,$$

hence $deg(f \cdot g) \leq m + n$.

(iii) In the proof of (ii), notice that if $a_mb_n \neq 0$, then $deg(f \cdot g) = m + n$. But since $a_m \neq 0$, $b_n \neq 0$ and R is an integral domain, we have $a_mb_n \neq 0$ and consequently $deg(f \cdot g) = deg(f) + deg(g)$. $\square$

Example 2.7.9 (a) Let $f = 1 + X + X^2$, $g = 1 - X^2 \in \mathbb{Z}[X]$. Then $f + g = 2 + X$ and we have $deg(f + g) = 1 < 2 = \max(deg(f), deg(g))$.

(b) Let $f = \widehat{1} + \widehat{2}X$, $g = \widehat{1} + \widehat{3}X^2 \in \mathbb{Z}_6[X]$. Then $f \cdot g = \widehat{1} + \widehat{2}X + \widehat{3}X^2$ and we have $deg(f \cdot g) = 2 \neq 3 = deg(f) + deg(g)$.

Corollary 2.7.10 *If R is an integral domain, then $R[X]$ is an integral domain.*

Proof. Let $f, g \in R[X]$ with $f \neq 0$ and $g \neq 0$. Then $deg(f) \geq 0$ and $deg(g) \geq 0$. Now by Theorem 2.7.8, we have

$$deg(f \cdot g) = deg(f) + deg(g) \geq 0 \,,$$

whence it follows that $f \cdot g \neq 0$. Hence $R[X]$ has no zero divisors. Clearly, $R[X] \neq 0$ is commutative and has identity. Consequently, $R[X]$ is an integral domain. $\square$

Theorem 2.7.11 *Let R be an integral domain. Then the invertible elements in the ring $R[X]$ coincide with the invertible elements in the ring R.*

Proof. First, let $f \in R[X]$ be invertible in $R[X]$. Then there exists $g \in R[X]$ such that $f \cdot g = 1$. It follows that $deg(f \cdot g) = 0$, whence

$$deg(f) + deg(g) = 0$$

by Theorem 2.7.8. Then $deg(f) = deg(g) = 0$ (note that $f \neq 0$ and $g \neq 0$), that is, $f, g \in R$. But since $f \cdot g = 1$, it follows that f is invertible in R.

Secondly, if $f \in R$ is invertible in R, then clearly f is invertible in $R[X]$. $\square$

Corollary 2.7.12 *Let K be a field. Then the invertible elements in the ring $K[X]$ are exactly the polynomials of degree zero.*

We denote by $U(R)$ the set (group) of invertible elements in the ring R.

Example 2.7.13 (a) $U(\mathbb{Z}[X]) = U(\mathbb{Z}) = \{-1, 1\}$.

(b) $U(\mathbb{Q}[X]) = \mathbb{Q}^*$, $U(\mathbb{R}[X]) = \mathbb{R}^*$, $U(\mathbb{C}[X]) = \mathbb{C}^*$.

(c) $U(\mathbb{Z}_p[X]) = \mathbb{Z}_p^*$ (where p is a prime number).

2.8 Polynomial functions. Roots of polynomials

Definition 2.8.1 Let $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$ and $c \in R$.

The element

$$a_0 + a_1c + \cdots + a_nc^n \,,$$

obtained by formally replacing in f the indeterminate X by c, is called the *value of the polynomial f at the point c*, and is denoted by $f(c)$.

An element $c \in R$ is called a *root* of f if $f(c) = 0$.

The function $\overline{f} : R \to R$ defined by

$$\overline{f}(c) = f(c) = a_0 + a_1c + \cdots + a_nc^n \,,$$

is called the *polynomial function* associated to the polynomial f.

Theorem 2.8.2 *The function $\varphi : R[X] \to R^R$ defined by $\varphi(f) = \overline{f}$ is a unitary ring homomorphism between the rings $(R[X], +, \cdot)$ and $(R^R, +, \cdot)$.*

Proof. Recall that R^R denotes the set of all functions $f : R \to R$.

Clearly, $f(1) = 1_R$. Let $f, g \in R[X]$. For every $c \in R$, we have:

$$\overline{(f+g)}(c) = (f+g)(c) = f(c) + g(c) = \overline{f}(c) + \overline{g}(c) = (\overline{f} + \overline{g})(c),$$

$$\overline{(f \cdot g)}(c) = (f \cdot g)(c) = f(c) \cdot g(c) = \overline{f}(c) \cdot \overline{g}(c) = (\overline{f} \cdot \overline{g})(c).$$

It follows that:

$$\varphi(f+g) = \overline{f+g} = \overline{f} + \overline{g} = \varphi(f) + \varphi(g),$$

$$\varphi(f \cdot g) = \overline{f \cdot g} = \overline{f} \cdot \overline{g} = \varphi(f) \cdot \varphi(g).$$

Hence φ is a unitary ring homomorphism.

Definition 2.8.3 With the above notation, $Im\,\varphi$ is a subring of the ring $(R^R, +, \cdot)$, called the *ring of polynomial functions*.

Remark 2.8.4 (1) If the ring R is finite and $R \neq \{0\}$, then the ring $R[X]$ is infinite, while the ring R^R is finite. Hence φ is not injective, and so there are different polynomials having the same associated polynomial function.

For instance, $f = X + X^2 \in \mathbb{Z}_2[X]$ and $g = \hat{0} \in \mathbb{Z}_2[X]$ have the same associated polynomial function. Indeed, we have $\overline{f}(\hat{0}) = f(\hat{0}) = \hat{0} = g(\hat{0})$ and $\overline{f}(\hat{1}) = f(\hat{1}) = \hat{0} = g(\hat{1})$, and so $\overline{f} = \overline{g}$.

(2) Let $f \in R[X]$. Then $f \in Ker\,\varphi \Leftrightarrow \overline{f} = 0$ (the zero function) $\Leftrightarrow f(a) = 0$, $\forall a \in R$.

Theorem 2.8.5 (The Division Algorithm for polynomials) *Let R be an integral domain and let $f \in R[X]$ and $g = \sum_{j=0}^{n} b_jX^j \in R[X]$ with b_n invertible in R. Then there exist unique polynomials $q, r \in R[X]$ such that*

$$f = gq + r \,, \quad \textit{where} \quad deg(r) < deg(g) \,.$$

Proof. Let us first discuss two trivial cases.

If $f = 0$ or $deg(f) < deg(g)$, then clearly $f = g \cdot 0 + f$, whence $q = 0$ and $r = f$.

If $n = 0$, then $g = b_0 \in R$ is invertible by hypothesis and we have

$$f = g \cdot (g^{-1} \cdot f) + 0\,,$$

whence $q = g^{-1} \cdot f$ and $r = 0$.

In the sequel suppose that $f \neq 0$ and $deg(f) \geq deg(g) = n \geq 1$. Let $f = \sum_{i=0}^{m} a_i X^i$ with $a_m \neq 0$. We will prove the existence of the requested $q, r \in R[X]$ by induction on $m = deg(f)$.

If $m = 1$, then we have $m = n = 1$, say $f = a_0 + a_1 X$ and $g = b_0 + b_1 X$. It follows that

$$f = g \cdot (a_1 b_1^{-1}) + (a_0 - b_0 a_1 b_1^{-1})\,,$$

whence $q = a_1 b_1^{-1}$ and $r = a_0 - b_0 a_1 b_1^{-1}$.

Suppose now that the result holds for every polynomial of degree less than m and we prove that it holds for every polynomial f of degree m. Consider

$$h = f - (a_m b_n^{-1} X^{m-n}) \cdot g\,.$$

Then $deg(h) < m$ and we may apply the induction hypothesis. Hence there exist $q', r \in R[X]$ such that

$$h = gq' + r\,, \quad \text{where} \quad deg(r) < deg(g)\,.$$

Then

$$f = h + (a_m b_n^{-1} X^{m-n}) \cdot g = g \cdot (a_m b_n^{-1} X^{m-n} + q') + r\,,$$

whence $q = a_m b_n^{-1} X^{m-n} + q'$. Therefore, we have proved the existence of the required $q, r \in R[X]$.

Let us now prove the uniqueness. Suppose that there exist $q, q_1, r, r_1 \in R[X]$ such that

$$f = gq + r\,, \quad \text{where} \quad deg(r) < deg(g)\,,$$

$$f = gq_1 + r_1\,, \quad \text{where} \quad deg(r_1) < deg(g)\,.$$

Then $r_1 - r_2 = g \cdot (q_2 - q_1)$. But $deg(r_1 - r_2) < deg(g)$. Since $g \neq 0$, we get $q_2 - q_1 = 0$. Then $q_1 = q_2$ and $r_1 = r_2$, that end the proof. □

Corollary 2.8.6 *Let K be a field and let $f, g \in K[X]$ with $g \neq 0$. Then there exist unique polynomials $q, r \in K[X]$ such that*

$$f = gq + r\,, \quad \textit{where} \quad deg(r) < deg(g)\,.$$

Corollary 2.8.7 *Let R be an integral domain, $f \in R[X]$ and $c \in R$.*

(i) The remainder of the division of f by the polynomial $X - c$ is $f(c)$.

(ii) $X - c | f$ if and only if $f(c) = 0$ (Bézout).

(iii) If $deg(f) = n \geq 0$, then f has at most n roots in R. Hence every polynomial of degree n over an integral domain R has at most n roots in R.

Proof. (i) By Theorem 2.8.5, there exist $q, r \in R[X]$ such that

$$f = (X - c)q + r\,,$$

where either $deg(r) = 0$ or $deg(r) = -\infty$. Hence $r \in R$. It follows that $f(c) = r$.

(ii) Immediate by (i).

(iii) The proof is by induction on the degree of f.

For $n = 0$ the result holds, since polynomials of degree zero do not have any roots.

Suppose that the result holds for any polynomial of degree less than n and let us prove it for f with $deg(f) = n$. Let $c \in R$ be a root of f, that is, $f(c) = 0$. Then clearly, $f = (X - c) \cdot g$, where $deg(g) < deg(f) = n$. By the induction hypothesis, g has at most $n - 1$ roots in R. But R is an integral domain, hence the roots of g are also roots of f. It follows that f has at most n roots in R, which completes the proof. □

Theorem 2.8.8 *Let R be an infinite integral domain. Then the unitary ring homomorphism $\varphi : R[X] \to R^R$ defined by $\varphi(f) = \overline{f}$ (see Theorem 2.8.2) is injective. Hence the polynomial ring $R[X]$ is isomorphic to the ring $Im\,\varphi$ of polynomial functions.*

Proof. Let $f \in Ker\,\varphi$. Then $\overline{f} =$ (the zero function), and so $f(a) = 0$, $\forall a \in R$. Hence f has an infinite number of roots. It follows that $f = 0$ by Corollary 2.8.7 (iii). Hence $Ker\,\varphi = 0$, and so φ is injective. By the first isomorphism theorem for rings it follows that $R[X] \cong R[X]/\{0\} \cong Im\,\varphi$.

Corollary 2.8.9 *Let R be an infinite integral domain and let $f, g \in R[X]$. Then:*

$$\overline{f} = \overline{g} \Leftrightarrow f = g.$$

Example 2.8.10 (a) Let $f = X^2 - \hat{4} \in \mathbb{Z}_{12}[X]$. Then its roots are $\hat{2}$, $\hat{4}$, $\hat{8}$ and $\widehat{10}$. Hence f has more roots than its degree.

(b) If $\mathbb{H}$ is the quaternion division ring, then the polynomial $f = X^2 + 1 \in \mathbb{H}[X]$ has an infinite number of roots. Indeed, there are infinitely many $a, b, c \in \mathbb{R}$ such that $a^2 + b^2 + c^2 = 1$. Then every $x = ai + bj + ck$ is a root of f, because $f(x) = x^2 + 1 = -(a^2 + b^2 + c^2) + 1 = 0$.

We mention without proof the following result, also called the *Fundamental Theorem of Algebra.*

Theorem 2.8.11 (D'Alembert-Gauss) *Every polynomial of degree $n \geq 1$ with complex coefficients has at least one complex root.*

Corollary 2.8.12 *Every polynomial of degree $n \geq 0$ with complex coefficients has exactly n complex roots.*