Section III.5. Rings of Polynomials and Formal Power Series

Note. Since we are ultimately interested in polynomial equations, we need to introduce polynomials and they must be somewhere. We deal with polynomials as elements of a ring. We are mostly interested in polynomials in a single indeterminate, but will also define polynomials in several indeterminates.

Theorem III.5.1. Let R be a ring and let $R[x]$ denote the set of all sequences of elements of R, $(a_0, a_1, \ldots)$, such that $a_i = 0$ for all but a finite number of indices i.

(i) $R[x]$ is a ring with addition and multiplication defined by

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots)$$

$$(a_0, a_1, \ldots)(b_0, b_1, \ldots) = (c_0, c_1, \ldots)$$

where

$$c_n = \sum_{i=0}^{n} a_{n-i}b_i = a_n b_0 + a_{n-1}b_1 + \cdots + a_0 b_n = \sum_{k+j=n} a_k b_j.$$

(ii) If R is commutative (respectively, a ring with identity/a ring with no zero divisor/an integral domain) then so is $R[x]$.

(iii) The map $R \to R[x]$ given by $r \mapsto (r, 0, 0, \ldots)$ is a monomorphism (one to one homomorphism) of rings.

Note. The proof of Theorem II.5.1(i) and commutativity in (ii) are straightforward as proved in Fraleigh as Theorem 22.2.

Note. If 1_R is the identity in R then $(1_R, 0, 0, \ldots)$ is the identity in $R[x]$. We may denote $(r, 0, 0, \ldots) \in R[x]$ simply as r.

Definition. Ring $R[x]$ of Theorem III.5.1 is the *ring of polynomials* over R. Elements of $R[x]$ are called *polynomials*.

Theorem III.5.2. Let R be a ring with identity and denote by x the element $(0, 1_R, 0, 0, \ldots)$ of $R[x]$.

(i) $x^n = (0, 0, \ldots, 0, 1_R, 0, 0, \ldots)$ where 1_R is the $(n+1)$-st coordinate.

(ii) If $r \in R$, then for each $n \geq 0$, $rx^n = x^n r = (0, 0, \ldots, 0, r, 0, \ldots)$ where r is the $(n+1)$-st coordinate.

(iii) For every nonzero polynomial $f \in R[x]$ there exists integer $n \in \mathbb{N} \cup \{0\}$ and elements $a_0, a_1, \ldots, a_n \in R$ such that

$$f = a_0 x^0 + a_1 x^1 + a_2 x^2 + \cdots + a_n x^n.$$

The integer n and elements a_i are unique in the sense that

$$f = b_0 x^0 + b_1 x^1 + b_2 x^2 + \cdots b_m x^m$$

where $b_i \in R$ implies $m \geq n$, $a_i = b_i$ for $i = 1, 2, \ldots, n$, and $b_i = 0$ for $n < i \leq m$.

Note. The proof of Theorem III.5.2 is routine and is left as an "exercise."

Note. We adopt an obvious notation (the same notation used by Fraleigh). We denote $f = a_0x^0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n$ as

$$f = a_0x^0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n = \sum_{i=0}^{n} a_ix^i.$$

Thus we have

$$\left(\sum_{i=0}^{n} a_ix^i\right)\left(\sum_{j=0}^{m} b_jx^j\right) = \sum_{k=0}^{m+n} c_kx^k$$

where $c_k = \sum_{i+j=k} a_ib_j$. For $f = \sum_{i=0}^{n} a_ix^i \in R[x]$, the a_i are *coefficients* of f. a_0 is the *constant term.* A polynomial of the form $f = r$ where $r \in R$ is a *constant polynomial* (Fraleigh does not count 0 degree polynomials as "polynomials"). If $a_n \neq 0$ and $a_m = 0$ for $m > n$ in polynomial f, then a_n is the *leading coefficient* of f. If R has identity 1_R and the leading coefficient of f is 1_R, then f is a *monic polynomial.*

Note. Recall that for $n \in \mathbb{N}$, we have

$$(\mathbb{N} \cup \{0\})^n = (\mathbb{N} \cup \{0\}) \times (\mathbb{N} \cup \{0\}) \times \cdots (\mathbb{N} \cup \{0\})$$

and the elements of this set are n-tuples of nonnegative integers. So $(\mathbb{N} \cup \{0\})^n$ is an additive abelian monoid (a "group without inverses").

Note. The following is analogous to Theorem III.5.1, but for polynomials of several indeterminates.

Theorem III.5.3. Let R be a ring and denote by $R[x_1, x_2, \ldots, x_n]$ the set of all functions $f : (\mathbb{N} \cup \{0\})^n \to R$ such that $f(u) \neq 0$ for at most a finite number of elements $u \in (\mathbb{N} \cup \{0\})^n$.

(i) $R[x_1, x_2, \ldots, x_n]$ is a ring with addition and multiplication defined by

$$(f+g)(u) = f(u) + g(u) \text{ and } (fg)(u) = \sum_{\substack{v+w=u \\ v,w \in (\mathbb{N}\cup\{0\})^n}} f(v)g(w),$$

where $f, g \in R[x_1, x_2, \ldots, x_n]$ and $u \in (\mathbb{N} \cup \{0\})^n$.

(ii) If R is commutative (respectively, a ring with identity/a ring without zero divisors/an integral domain) then so is $R[x_1, x_2, \ldots, x_n]$.

(iii) The map $R \mapsto R[x_1, x_2, \ldots, x_n]$ given by $r \mapsto f_r$ where $f_r(0, 0, \ldots, 0) = r$ and $f(u) = 0$ for all other $u \in (\mathbb{N} \cup \{0\})^n$ is a monomorphism (one to one homomorphism) of rings.

Note. Think of the n-tuples as exponents on $x_1, x_2, \ldots, x_n$. For example, if $n = 3$ and $R = \mathbb{Z}$ with $f((0,0,0)) = 4$, $f((1,1,1)) = 2$, $f((1,0,5)) = -2$, and $f(u) = 0$ for all other 3-tuples u, then f corresponds to the polynomial in 3 indeterminates of $4 + 2x_1x_2x_3 - 2x_1x_3^5$.

Definition. The ring $R[x_1, x_2, \ldots, x_n]$ of Theorem III.5.3(i) is the *ring of polynomials in n indeterminates.* For $n \in \mathbb{N}$ and each $i = 1, 2, \ldots, n$ denote

$$\varepsilon_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in (\mathbb{N} \cup \{0\})^n$$

where 1 is the ith coordinate of ε_i.

Theorem III.5.4. Let R be a ring with identity and $n \in \mathbb{N}$. For each $i = 1, 2, \ldots, n$ let $x_i \in R[x_1, x_2, \ldots, x_n]$ be defined as $x_i(\varepsilon_i) = 1_R$ and $x_i(u) = 0$ for $u \neq \varepsilon_i$.

(i) For each integer $k \in (\mathbb{N} \cup \{0\})^n$, $x_i^k(k\varepsilon_i) = 1_R$ and $x_i^k(u) = 0$ for $u \neq k\varepsilon_i$.

(ii) For each

$$(k_1, k_2, \ldots, k_n) \in (\mathbb{N} \cup \{0\})^n, x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}(k_1\varepsilon_1 + k_2\varepsilon_2 + \cdots + k_n\varepsilon_n) = 1_R$$

and $x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}(u) = 0$ for $u \neq k_1\varepsilon_1 + k_2\varepsilon_2 + \cdots + k_n\varepsilon_n$.

(iii) $x_i^s x_j^t = x_j^t x_i^s$ for all $s, t \in \mathbb{N} \cup \{0\}$ and all $i, j = 1, 2, \ldots, n$.

(iv) $x_i^t r = r x_i^t$ for all $r \in R$ and all $t \in \mathbb{N}$.

(v) For every polynomial f in $R[x_1, x_2, \ldots, x_n]$ there exists unique elements $a_{k_1,k_2,\ldots,k_n} \in R$ indexed by all $(k_1, k_2, \ldots, k_n) \in (\mathbb{N} \cup \{0\})^n$ and nonzero for at most a finite number of $(k_1, k_2, \ldots, k_n) \in (\mathbb{N} \cup \{0\})^n$ such that

$$f = \sum a_{k_1,k_2,\ldots,k_n} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n},$$

where the sum is over all $(k_1, k_2, \ldots, k_n) \in (\mathbb{N} \cup \{0\})^n$.

Definition. A polynomial of the form $a x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} \in R[x_1, x_2, \ldots, x_n]$ is a *monomial.*

Definition. Let $\varphi : R \to S$ be a homomorphism of rings, $f \in R[x_1, x_2, \ldots, x_n]$, and $s_1, s_2, \ldots, s_n \in S$. By Theorem III.5.4(v), we know that

$$f = \sum_{i=0}^{m} a_i x_1^{k_{i1}} x_2^{k_{i2}} \cdots x_n^{k_{in}}$$

with $a_i \in R$ and $k_{ij} \in \mathbb{N}$ (we omit all x_i with 0 exponent). Define

$$\varphi(f(s_1, s_2, \ldots, s_n)) = \sum_{i=0}^{m} \varphi(a_i) s_1^{k_{i1}} s_2^{k_{i2}} \cdots s_n^{k_{in}} \in S.$$

Note. Since the a_i and k_i in the previous definition are uniquely determined by Theorem III.5.4(v), so $\varphi(f(s_1, s_2, \ldots, s_n))$ is well-defined.

Theorem III.5.5. Let R and S be commutative rings with identity and $\varphi : R \to S$ is a homomorphism of rings such that $\varphi(1_R) = 1_S$. If $s_1, s_2, \ldots, s_n \in S$ then there is a unique homomorphism of rings $\overline{\varphi} : R[x_1, x_2, \ldots, x_n] \to S$ such that $\overline{\varphi}|_R = \varphi$ and $\overline{\varphi}(x_i) = s_i$ for $i = 1, 2, \ldots, n$. This property (that is, the mapping properties of φ and $\overline{\varphi}$; Hungerford calls this "a universal mapping property") completely determines the polynomial ring $R[x_1, x_2, \ldots, x_n]$ up to isomorphism.

Corollary III.5.6. If $\varphi : R \to S$ is a homomorphism of commutative rings and $s_1, s_2, \ldots, s_n \in S$, then the map $R[x_1, x_2, \ldots, x_n] \to S$, where $f = \sum_{i=0}^{m} a_i x_1^{k_{i1}} x_2^{k_{i2}} \cdots x_n^{k_{in}}$ is mapped to $\overline{\varphi}(f) = \varphi(f(x_1, x_2, \ldots, x_n)) = \sum_{i=0}^{m} \varphi(a_i) s_1^{k_{i1}} s_2^{k_{i2}} \cdots s_n^{k_{in}}$, is a homomorphism of rings.

Note. Theorem III.5.5 and Corollary 5.6 hold for rings of polynomials in an infinite number of indeterminates as well (see Exercise III.5.4).

Definition. If $\varphi : R \to S$ is a homomorphism of commutative rings then the map $R[x_1, x_2, \ldots, x_n] \to S$, where $f = \sum_{i=0}^m a_i x_1^{k_{i1}} x_2^{k_{i2}} \cdots x_n^{k_{in}}$ is mapped to $\overline{\varphi}(f) = \varphi(f(x_1, x_2, \ldots, x_n)) = \sum_{i=0}^m \varphi(a_i) s_1^{k_{i1}} s_2^{k_{i2}} \cdots s_n^{k_{in}}$, of Corollary III.5.6 is the *evaluation homomorphism* (or *substitution homomorphism*).

Note. Another application of Theorem III.5.5 is to show that $(R[x_1])[x_2] \cong (R[x_2])[x_1] \cong R[x_1, x_2]$ That is, a ring of polynomials in x_2 over ring $R[x_1]$ is isomorphic to a ring of polynomials in x_1 and x_2 over ring R. More generally, we have the following.

Corollary III.5.7. Let R be a commutative ring with identity and n a positive integer. For each k (with $1 \leq k < n$) there are isomorphic rings

$$R[x_1, x_2, \ldots, x_k][x_{k+1}, x_{k+2}, \ldots, x_n] \cong R[x_1, x_2, \ldots, x_n]$$

$$\cong R[x_{k+1}, x_{k+2}, \ldots, x_n][x_1, x_2, \ldots, x_k].$$

Note. We now address a ring of "formal power series." Fraleigh starts with formal power series and then deals with polynomials in the setting of formal power series. The remainder of this section is not needed for the rest of the material to be covered, so we may skip this if we are short of time.

Proposition III.5.8. Let R be a ring and denote by $R[[x]]$ the set of all sequences of elements of R.

(i) $R[[x]]$ is a ring with addition and multiplication defined by

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots)$$

and

$$(a_0, a_1, \ldots)(b_0, b_1, \ldots) = (c_0, c_1, \ldots)$$

where $c_n = \sum_{i=0}^{n} a_i b_{n-i} = \sum_{k+j=n} a_k b_j$.

(ii) The polynomial ring $R[x]$ is a subring of $R[[x]]$.

(iii) If R is commutative (respectively, a ring with identity/a ring with no zero divisors/an integral domain), then so is $R[[x]]$.

Definition. The ring $R[[x]] = \{(a_0, a_1, \ldots) \mid a_i \in R\}$ where addition and multiplication are defined in Proposition III.5.8, is the *ring of formal power series* over ring R.

Note. If R has an identity then the polynomial $x = (0, 1_R, 0, \ldots) \in R[[x]]$ is an indeterminate in $R[[x]]$. So we have for $(a_0, a_1, \ldots) \in R[[x]]$ that $(a_0, a_1, \ldots) = \sum_{i=0}^{\infty} a_i x^i$.

Proposition III.5.9. Let R be a ring with identity and $f = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$.

(i) f is a unit in $R[[x]]$ if and only if its constant term a_0 is a unit in R.

(ii) If a_0 is irreducible in R, then f is irreducible in $R[[x]]$.

Note III.5.A. Intuitively, we might expect a nonconstant polynomial in $R[x]$ *not* to have an inverse (since it doesn't seem that the "reciprocal" of a polynomial would be a polynomial). If R has zero divisors, then a nonconstant polynomial may have an inverse. For example, in $\mathbb{Z}_4[x]$ we have $(\bar{1}+\bar{2}x)(\bar{1}+\bar{2}x) = \bar{1}+\bar{4}x+\bar{4}x^2 = \bar{1}$. However, if R is an integral domain, then the units of $R[x]$ are the constant polynomials where the constant is a unit of R (see Exercise IV.22.25(a) in John Fraleigh's *A First Course In Abstract Algebra*, 7th Edition, Pearson, 2002). Similarly, we'll show in Corollary III.6.4 that if F is a field then the units in $F[x]$ are precisely the nonzero constant polynomials.

Note. Recall from Section III.4 that a *local ring* is a commutative ring with identity which has a unique maximal ideal.

Corollary III.5.10. If R is a division ring, then the units in $R[[x]]$ are precisely those power series with nonzero constant terms. The principal ideal (x) consists precisely of the nonunits in $R[[x]]$ and is the unique maximal ideal of $R[[x]]$. Thus if R is a field, $R[[x]]$ is a local ring.

Note III.5.B. It might seem surprising that a formal power series could be a unit when it does not consist only of a constant term, given the observation in Note III.5.A. However, if we consider the power series for e^x we see that it is a unit since, when it is multiplied by the power series for e^{-x}, we get 1. The formal power series associated with e^x is $\left(1, 1, \frac{1}{2!}, \frac{1}{3!}, \ldots, \frac{1}{n!}, \ldots\right)$ and the formal power series associated with e^{-x} is $\left(1, -1, \frac{1}{2!}, \frac{-1}{3!}, \ldots, \frac{(-1)^n}{n!}, \ldots\right)$. These formal power series satisfy the equations in the proof of Proposition III.5.9(i), as follows:

$$\begin{aligned}
1 &= a_0b_0 = (1)(1) \\
0 &= a_0b_1 + a_1b_0 = (1)(-1) + (1)(1) \\
0 &= a_0b_2 + a_1b_1 + a_2b_0 = (1)(1/2) + (1)(-1) + (1/2)(1) \\
0 &= a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 = (1)(-1/6) + (1)(1/2) + (1/2)(-1) + (1/6)(1) \\
0 &= a_0b_4 + a_1b_3 + a_2b_2 + a_3b_1 + a_4b_0 \\
&= (1)(1/24) + (1)(-1/6) + (1/2)(1/2) + (1/6)(-1) + (1/24)(1) \\
&\vdots
\end{aligned}$$

In fact, a polynomial can have a formal power series as an inverse (though the polynomial itself would have to be interpreted as a formal power series, so that it is in the same ring as its inverse, namely $R[[x]]$). With $f = 1 - x \in R[[x]]$ and $g = 1 + x + x^2 + x^3 + \cdots \in R[[x]]$ we have $fg = 1$, for example.

Revised: 4/24/2024