

## §33 Polynomial Rings

The reader is familiar with polynomials. In high school, it is taught that expressions like

$$x^2 + 2x + 5 \qquad x^3 + 2x^2 - 7x + 1$$

are polynomials. One learns how to add, subtract, multiply and divide two polynomials. Although one acquires a working knowledge about polynomials, a satisfactory definition of polynomials is hardly given. In this paragraph, we give a rigorous definition of polynomials.

Polynomials are treated in the calculus as functions. For example,  $x^2 + 2x + 5$  is considered to be the function (defined on  $\mathbb{R}$ , say) that maps any  $x \in \mathbb{R}$  to  $x^2 + 2x + 5$ . With this interpretation, a polynomial is a function and  $x$  is a generic element in its domain. The equality of two polynomials means then the equality of their domains and the equality of the function values at any element in their domain.

This is a perfectly sound approach, but it will prove convenient to treat polynomials differently in algebra. We propose to define the equality of two polynomials as the equality of their corresponding coefficients. This definition is motivated by the so-called comparison of coefficients. Note that this definition of equality does not involve  $x$  at all. Whatever  $x$  may be, it is not relevant to the definition of equality. Nor is it relevant to the addition and multiplication of two polynomials. So we may forget about  $x$  completely. We then deprive of a polynomial  $a_0 + a_1x + \cdots + a_nx^n$  of the symbols  $x^r$ . What remains is a finite number of coefficients and "+" signs. The "+" signs can be thought of as connectives. Then a polynomial is essentially a finite number of coefficients. This leads to the following definition.

**33.1 Definitions:** Let  $R$  be a ring. A sequence

$$f = (a_0, a_1, a_2, \dots)$$

of elements  $a_0, a_1, a_2, \dots$  in  $R$ , where only finitely many of them are distinct from the zero element of  $R$ , is called a *polynomial over  $R$* .

The terms  $a_0, a_1, a_2, \dots$  are called the *coefficients* of the polynomial  $f = (a_0, a_1, a_2, \dots)$ . The term  $a_0$  will be referred to as the *constant term of  $f$* .

Two polynomials  $f = (a_0, a_1, a_2, \dots)$  and  $g = (b_0, b_1, b_2, \dots)$  over  $R$  are declared *equal* when they are equal as sequences of course, that is to say, when  $a_i = b_i$  for all  $i = 0, 1, 2, \dots$ . In this case, we write  $f = g$ . Otherwise we put  $f \neq g$ .

If  $f = (a_0, a_1, a_2, \dots)$  is a polynomial over  $R$ , there is an index  $d$  such that  $a_n = 0 \in R$  whenever  $n > d$ . If the coefficients  $a_0, a_1, a_2, \dots$  are not all equal to zero, there is an index  $d$ , uniquely determined by  $f$ , such that  $a_d \neq 0$  and  $a_n = 0$  for all  $n > d$ . This index  $d$  is called the *degree of  $f$* . We write then  $d = \deg f$ . If  $d$  is the degree of  $f$ , then  $a_d$  is said to be the *leading coefficient of  $f$* . It is the last nonzero coefficient of  $f$ . If  $R$  happens to be a ring with identity  $1$  and if  $f$  is a polynomial over  $R$  with leading coefficient equal to  $1$ , then  $f$  is called a *monic polynomial*.

A polynomial of degree one is called a *linear polynomial*, one of degree two is called a *quadratic polynomial*, one of degree three is called a *cubic polynomial*, one of degree four is called a *biquadratic* or *quartic polynomial* and one of degree five is called a *quintic polynomial*.

The polynomial  $0^* = (0, 0, 0, \dots)$  over  $R$ , whose terms are all equal to the zero element  $0 \in R$  of  $R$ , is called the *zero polynomial over  $R$* . The leading coefficient and the degree of the zero polynomial are *not* defined. The leading coefficient of any other polynomial *is* defined. The constant term of the zero polynomial *is* defined, and is  $0 \in R$ .

Notice that indexing begins with 0, not with 1. For example,  $(1, 0, 2, 5, 0, 0, 0, \dots)$  is a polynomial over  $\mathbb{Z}$  of degree 3, not of degree 4. Its constant term is  $1 \in \mathbb{Z}$ , leading coefficient is  $5 \in \mathbb{Z}$ .

**33.2 Definition:** Let  $R$  be a ring and let

$$f = (a_0, a_1, a_2, \dots) \quad \text{and} \quad g = (b_0, b_1, b_2, \dots)$$

be two polynomials over  $R$ . Then the *sum of  $f$  and  $g$* , denoted by  $f + g$ , is the sequence

$$f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots)$$

obtained by termwise addition of the coefficients. The *product of  $f$  by  $g$* , denoted by  $f \cdot g$  or by  $fg$ , is the sequence

$$fg = (c_0, c_1, c_2, \dots)$$

where the terms  $c \in R$  are given by

$$\begin{aligned} c_0 &= a_0 b_0 \\ c_1 &= a_0 b_1 + a_1 b_0 \\ c_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0 \\ c_3 &= a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 \\ &\dots\dots\dots \\ c_k &= a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \dots + a_{k-2} b_2 + a_{k-1} b_1 + a_k b_0 \\ &\dots\dots\dots \end{aligned}$$

To find the  $k$ -th term  $c_k$  in  $fg$ , we multiply all  $a$ 's with all  $b$ 's in such a way that the sum of the indices is  $k$ , and add the results. We write  $c_k = \sum_{i=0}^k a_i b_{k-i}$ . The summation variable runs through different values for different  $k$ 's (through 0,1,2,3 for  $k = 3$ , through 0,1,2,3,4,5 for  $k = 5$ , etc.).

It will be convenient to write  $c_k = \sum_{i+j=k} a_i b_j$ , it being understood that  $i$  and  $j$  run through nonnegative integers in such a way that their sum is  $k$ .

**33.3 Lemma:** Let  $R$  be a ring and let  $f = (a_0, a_1, a_2, \dots)$  and  $g = (b_0, b_1, b_2, \dots)$  be arbitrary polynomials over  $R$ . Let  $0^* = (0, 0, 0, \dots)$  be the zero polynomial over  $R$ .

- (1)  $f + 0^* = f$  and  $0^* + g = g$ . Also  $f 0^* = 0^*$  and  $0^* g = 0^*$ .
- (2) The sum  $f + g$  is a polynomial over  $R$ . If  $\deg f = m$  and  $\deg g = n$ , then

$$\begin{aligned} \deg(f+g) &= \max\{m,n\} && \text{in case } m \neq n, \\ \deg(f+g) &\leq m && \text{in case } m = n \text{ and } f+g \neq 0^*. \end{aligned}$$

(3) The product  $fg$  is a polynomial over  $R$ . If  $\deg f = m$  and  $\deg g = n$ , then

$$\begin{aligned} \deg fg &\leq m+n && \text{in case } fg \neq 0^*, \\ \deg fg &= m+n && \text{in case } R \text{ has no zero divisors.} \end{aligned}$$

**Proof:** (1) The assertions  $f+0^* = f$  and  $0^* + g = g$  are immediate from the definitions:  $f+0^* = (a_0, a_1, a_2, \dots) + (0, 0, 0, \dots) = (a_0+0, a_1+0, a_2+0, \dots) = (a_0, a_1, a_2, \dots) = f$  and similarly  $0^* + g = g$ . Also, the  $k$ -th coefficient of  $f0^*$  is  $a_0 \cdot 0 + a_1 \cdot 0 + a_2 \cdot 0 + \dots + a_k \cdot 0 = 0 + 0 + 0 + \dots + 0 = 0$  by Lemma 29.6, for any  $k$ . This proves  $f0^* = 0^*$ . Likewise  $0^*g = 0^*$ .

(2) We must show that  $f+g$  has only finitely many terms distinct from 0. We proved it in part (1) when  $f=0^*$  or  $g=0^*$ . Now we assume  $f \neq 0^* \neq g$ . Then  $f$  and  $g$  have degrees. Suppose  $\deg f = m$  and  $\deg g = n$ , so that  $a_m \neq 0, a_r = 0$  for all  $r > m$  and  $b_n \neq 0, b_r = 0$  for all  $r > n$ .

If  $m < n$ , then  $f+g = (a_0 + b_0, a_1 + b_1, \dots, a_m + b_m, b_{m+1}, \dots, b_n, 0, 0, 0, \dots)$ . So the  $n$ -th term in  $f+g$  is  $b_n \neq 0$ , and the later terms are  $a_r + b_r = 0 + 0 = 0$  for  $r > n > m$ . This shows that  $f+g$  is a nonzero polynomial and  $\deg f+g = n = \max\{m,n\}$ .

If  $n < m$ , then  $f+g = (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n, a_{n+1}, \dots, a_m, 0, 0, 0, \dots)$ . So the  $m$ -th term in  $f+g$  is  $a_m \neq 0$ , and the later terms are  $a_r + b_r = 0 + 0 = 0$  for  $r > m > n$ . This shows that  $f+g$  is a nonzero polynomial and  $\deg f+g = m = \max\{m,n\}$ . [Question: why cannot we combine the two cases  $m < n$  and  $n < m$  into a single one by assuming  $m < n$  without loss of generality?]

If  $m = n$ , then  $f+g = (a_0 + b_0, a_1 + b_1, \dots, a_m + b_m, 0, 0, 0, \dots)$ . The  $r$ -th term in  $f+g$  is  $a_r + b_r = 0$  for all  $r > m$ . This shows that  $f+g$  is a polynomial. Either it is the zero polynomial, or it is not the zero polynomial. In the latter case, the nonzero terms in  $f+g$  have indices  $\leq m$ . In particular, the degree of  $f+g$  is  $\leq m$ . (More exactly,  $\deg f+g = m$  if  $a_m + b_m \neq 0$ , and  $\deg f+g < m$  if  $a_m + b_m = 0$ .)

(3) To prove that the product  $fg$  is a polynomial over  $R$ , we must show that  $fg$  has only finitely many terms distinct from zero. We proved it in part (1) when  $f=0^*$  or  $g=0^*$ . Now we assume  $f \neq 0^* \neq g$ . Then  $f$  and  $g$

have degrees. Suppose  $\deg f = m$  and  $\deg g = n$ , so that  $a_m \neq 0$ ,  $a_r = 0$  for all  $r > m$  and  $b_n \neq 0$ ,  $b_r = 0$  for all  $r > n$ .

The  $k$ -th term in  $fg = (c_0, c_1, c_2, \dots)$  is given by  $c_k = \sum_{i+j=k} a_i b_j$ . Suppose now

$k > m + n$ . If  $i + j = k$ , then either  $i > m$  or  $j > n$  (for  $i \leq m$  and  $j \leq n$  implies the contradiction  $k = i + j \leq m + n < k$ ), so either  $a_i = 0$  or  $b_j = 0$

for each one of the summands  $a_i b_j$  in  $c_k = \sum_{i+j=k} a_i b_j$ . So each summand is

either  $0b_j = 0$  or  $a_i 0 = 0$  by Lemma 29.6 and  $c_k = 0 + 0 + \dots + 0 = 0$ . This shows that  $c_k = 0$  for all  $k > m + n$ . Hence  $fg$  has at most  $m + n$  terms distinct from 0 and  $fg$  is a polynomial over  $R$  and  $\deg fg \leq m + n$  in case  $fg \neq 0^*$ .

The  $(m + n)$ -th term  $c_{m+n}$  in  $fg$  is

$$\begin{aligned} c_{m+n} &= a_0 b_{m+n} + a_1 b_{m+n-1} + a_2 b_{m+n-2} + \dots + a_{m-1} b_{n+1} \\ &\quad + a_m b_n \\ &\quad + a_{m+1} b_{n-1} + a_{m+2} b_{n-2} + \dots + a_{m+n-1} b_1 + a_{m+n} b_0. \end{aligned}$$

Here the summands in the first line are 0 since  $b_{m+n}, b_{m+n-1}, b_{m+n-2}, \dots, b_{n+1}$  are 0 and the summands in the third line are 0 since  $a_{m+1}, a_{m+2}, \dots, a_{m+n-1}, a_{m+n}$  are 0. This gives  $c_{m+n} = a_m b_n$ . If  $R$  has no zero divisors, then  $c_{m+n} = a_m b_n$  since  $a_m \neq 0$  and  $b_n \neq 0$ . So  $m + n$  is the greatest index  $k$  for which the  $k$ -th term in  $fg$  is distinct from 0. This proves that  $\deg fg = m + n$  in case  $R$  has no zero divisors.  $\square$

**33.4 Remark:** The last argument shows in fact that the leading coefficient of  $fg$  is the leading coefficient of  $f$  times the leading coefficient of  $g$ , provided  $R$  has no zero divisors.

**33.5 Theorem:** Let  $R$  be a ring. The set of all polynomials over  $R$  is a ring with respect to the operations  $+$  and  $\cdot$  given in Definition 33.2 (called the addition and multiplication of polynomials, respectively).

**Proof:** First of all, we must prove that  $+$  makes the set of all polynomials over  $R$  into an abelian group. The closure property was shown in Lemma 33.3(2). The associativity and commutativity of addition of polynomials

follow from the associativity and commutativity of addition in  $R$ . The zero polynomial  $0^*$  is the zero element (Lemma 33.3(1)) and each polynomial  $(a_0, a_1, a_2, \dots)$  over  $R$  has an opposite  $(-a_0, -a_1, -a_2, \dots)$ . The details are left to the reader.

Now the properties of multiplication in Definition 29.1. The closure of the set of all polynomial over  $R$  under multiplication was shown in Lemma 33.3(3). The associativity of multiplication is proved by observing that the  $m$ -th term in  $(fg)h$ , where

$$f = (a_0, a_1, a_2, \dots), \quad g = (b_0, b_1, b_2, \dots), \quad h = (c_0, c_1, c_2, \dots)$$

are arbitrary polynomials over  $R$ , is given by

$$\sum_{k+l=m} (\textit{k-th term in } fg)c_l = \sum_{k+l=m} \left( \sum_{i+j=k} a_i b_j \right) c_l = \sum_{i+j+l=m} (a_i b_j) c_l$$

and that the  $m$ -th term in  $f(gh)$  is given by

$$\sum_{i+s=m} a_i (\textit{s-th term in } gh) = \sum_{i+s=m} a_i \left( \sum_{j+l=s} b_j c_l \right) = \sum_{i+j+l=m} a_i (b_j c_l).$$

Here we used the distributivity in  $R$ . Since  $(a_i b_j) c_l = a_i (b_j c_l)$ , the  $m$ -th term in  $(fg)h$  and  $f(gh)$  are equal, and this for all  $m$ . So  $(fg)h = f(gh)$  for all polynomials  $f, g, h$  over  $R$  and the multiplication is associative.

It remains to prove the distributivity laws. For any polynomials  $f = (a_0, a_1, a_2, \dots)$ ,  $g = (b_0, b_1, b_2, \dots)$ ,  $h = (c_0, c_1, c_2, \dots)$  over  $R$ , we have

$$\begin{aligned} f(g+h) &= (a_0, a_1, a_2, \dots)(b_0 + c_0, b_1 + c_1, b_2 + c_2, \dots) \\ &= \textit{polynomial whose } k\text{-th coefficient is } \sum_{i+j=k} a_i (b_j + c_j) \\ &= \textit{polynomial whose } k\text{-th coefficient is } \sum_{i+j=k} (a_i b_j + a_i c_j) \\ &= \textit{polynomial whose } k\text{-th coefficient is } \sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_j \\ &= (\textit{polynomial whose } k\text{-th coefficient is } \sum_{i+j=k} a_i b_j) \\ &\quad + (\textit{polynomial whose } k\text{-th coefficient is } \sum_{i+j=k} a_i c_j) \end{aligned}$$

$$= fg + fh$$

and a similar argument proves  $(f + g)h = fh + gh$  for all polynomials  $f, g, h$  over  $R$ . This completes the proof.  $\square$

The ring of all polynomials over  $R$  will be denoted by  $R[x]$ . When  $f \in R[x]$ , we say  $f$  is a *polynomial with coefficients in  $R$* .

We now want to simplify our notation. A polynomial  $f = (a_0, a_1, a_2, \dots)$  over  $R$ , for which  $a_n = 0$  whenever, say,  $n > d$ , can be written as

$$(a_0, 0, 0, 0, \dots) + (0, a_1, 0, 0, \dots) + (0, 0, a_2, 0, \dots) + \cdots + (0, 0, \dots, a_d, 0, \dots).$$

Each one of the polynomials above has at most one nonzero coefficient. A polynomial over  $R$  which has at most one nonzero coefficient will be called a *monomial over  $R$* . We can write monomials over  $R$  more compactly as follows. If, for example,  $g$  is a monomial over  $R$  whose  $r$ -th coefficient is  $a$  (the possibility  $a = 0$  is not excluded) and whose other coefficients are zero, then we can write  $g = (0, 0, \dots, a, 0, \dots)$  shortly as  $(a, r)$ . Here  $r$  denotes the index with the only the possibly nonzero element, and  $a \in R$  is that possibly nonzero element in the  $r$ -th place. Then our  $f$  would be written as  $(a_0, 0) + (a_1, 1) + (a_2, 2) + \cdots + (a_d, d)$ . The essential point is that a polynomial can be written as a sum of monomials, and a monomial is determined as soon as the index  $r$  and the possibly nonzero element  $a$  is given. We can choose other notations for monomials, of course, as long as they display the index  $r$  and the possibly nonzero element  $a$ . We prefer to write  $ax^r$  instead of  $(a, r)$  for the monomial  $(0, 0, \dots, a, 0, \dots)$ . In this notation, both the index  $r$  and the element  $a$  are displayed. It should be noted that  $x$  does *not* have a meaning by itself. It is like the comma in  $(a, r)$ . In particular,  $x^r$  is *not* the  $r$ -th power of anything.  $r$  in  $ax^r$  is an index, a superscript showing where the element  $a$  sits in. With this notation, our  $f$  is written as

$$f = a_0x^0 + a_1x^1 + a_2x^2 + \cdots + a_dx^d.$$

The product of two monomials  $ax^r$  and  $bx^s$  is easily evaluated to be  $abx^{r+s}$ . The multiplication of two polynomials can be carried out in the familiar way by using this rule and the distributivity. The symbol  $x$  is a convenient device that simplifies computations.  $x$  will be called an

*indeterminate (over R)*. This does not mean that  $x$  fails to be determined in some way. "Indeterminate" is just an odd name of a computational device. Finally, we agree to write  $a_0$  for  $a_0x^0$  and  $a_1x$  for  $a_1x^1$ . In particular, we write 0 for the zero polynomial  $0^*$ . This convention brings  $f$  to the form

$$a_0 + a_1x + a_2x^2 + \cdots + a_dx^d.$$

With the convention of writing  $a_0$  for  $a_0x^0$ , we regard  $R$  as a subring of  $R[x]$ . In particular, we can multiply polynomials by elements of  $R$  in the natural way:

$$\begin{aligned} b(a_0 + a_1x + a_2x^2 + \cdots + a_dx^d) &= ba_0 + ba_1x + ba_2x^2 + \cdots + ba_dx^d, \\ (a_0 + a_1x + a_2x^2 + \cdots + a_dx^d)b &= a_0b + a_1bx + a_2bx^2 + \cdots + a_dbx^d. \end{aligned}$$

If  $R$  is a ring with identity 1, then  $x$  can be interpreted in another way. The rule  $ax^r \cdot bx^s = abx^{r+s}$  yields  $1x^r \cdot 1x^s = 1x^{r+s}$ . Let  $p$  denote the polynomial  $1x = 1x^1 = (0,1,0,0, \dots)$ . We calculate that  $p^2 = 1x^2$ ,  $p^3 = 1x^3$ ,  $p^4 = 1x^4$ , etc. Our  $f$  can now be written as

$$f = a_0p + a_1p + a_2p^2 + \cdots + a_dp^d,$$

where this time the superscripts indicate the appropriate powers of  $p = (0,1,0,0, \dots)$ , taken according to the definition of multiplication given in Definition 33.2. So any polynomial over  $R$  can be written as a sum of powers of  $p$ , and calculations are performed by using the distributivity. Since  $x$  obeys the same rules as a computational device as  $p$  does as a polynomial, we write the polynomial  $p = 1x$  as  $x$ . Then  $x$  is the polynomial  $(0,1,0,0, \dots)$  in  $R[x]$ . We emphasize again that this interpretation of  $x$  as a polynomial is possible only when  $R$  has an identity. If  $R$  has no identity, then  $x$  is *not* a polynomial in  $R[x]$ .

The ring  $R[x]$  is said to be constructed by *adjoining  $x$  to  $R$* . When we want to examine several copies of  $R[x]$  at the same time, we use different letters to denote the indeterminates of the copies of  $R[x]$ . Thus we may have  $R[x], R[y], R[z]$ , etc.

Whenever convenient, we shall write  $\sum_{i=0}^d a_i x^i$  for the polynomial

$$a_0 + a_1x + a_2x^2 + \cdots + a_dx^d.$$

**33.6 Lemma:** *Let  $R$  be a ring.*

- (1) *If  $R$  is commutative, then  $R[x]$  is commutative.*
- (2) *If  $R$  has an identity, then  $R[x]$  has an identity.*
- (3) *If  $R$  has no zero divisors, then  $R[x]$  has no zero divisors.*
- (4) *If  $R$  is an integral domain, then  $R[x]$  is an integral domain.*

**Proof:** Let  $f = \sum_{i=0}^m a_i x^i$  and  $g = \sum_{j=0}^n b_j x^j$  be arbitrary polynomials in  $R[x]$ .

- (1) If  $R$  is commutative, then  $a_i b_j = b_j a_i$  for all  $i = 0, 1, \dots, m$  and  $j = 0, 1, \dots, n$ . We have then

$$fg = \sum_{k=0}^{m+n} \left( \sum_{i+j=k} a_i b_j \right) x^k = \sum_{k=0}^{m+n} \left( \sum_{j+i=k} b_j a_i \right) x^k = gf$$

and  $R[x]$  is commutative.

- (2) If  $R$  has an identity 1, then  $1 = 1x^0 = (1, 0, 0, 0, \dots)$  is a polynomial in  $R[x]$  and

$$f \cdot 1 = \left( \sum_{i=0}^m a_i x^i \right) 1 = \sum_{i=0}^m a_i 1 x^i = \sum_{i=0}^m a_i x^i = f,$$

$$1 \cdot f = 1 \left( \sum_{i=0}^m a_i x^i \right) = \sum_{i=0}^m 1 a_i x^i = \sum_{i=0}^m a_i x^i = f$$

for arbitrary  $f \in R[x]$ . Thus 1 is an identity element of  $R[x]$ .

- (3) Assume now  $R$  has no zero divisors. Let us suppose also that  $f \neq 0$  and  $g \neq 0$ . Without loss of generality, we may assume that  $a_m$  is the leading coefficient of  $f$  and that  $b_n$  is the leading coefficient of  $g$ . Then  $a_m \neq 0$ ,  $b_n \neq 0$ . By remark 33.4, the leading coefficient of  $fg$  is  $a_m b_n$  and  $a_m b_n \neq 0$  since  $R$  has no zero divisors. Thus  $fg$  has a nonzero coefficient, namely the  $(m+n)$ -th coefficient and  $fg \neq 0$ . This shows that  $R[x]$  has no zero divisors.

- (4) An integral domain is a commutative ring with identity having no zero divisors, distinct from the null ring. Now if  $R$  is an integral domain, then  $R$  is not the null ring, and since  $R \subseteq R[x]$ , the polynomial ring  $R[x]$  is not the null ring, either. The claim follows then immediately from (1), (2), and (3).

□

**33.7 Lemma:** Let  $R$  and  $S$  be two rings and let  $\varphi: R \rightarrow S$  be a ring homomorphism. Then the mapping  $\hat{\varphi}: R[x] \rightarrow S[x]$ , defined by

$$\left( \sum_{i=0}^m a_i x^i \right) \hat{\varphi} = \sum_{i=0}^m (a_i \varphi) x^i$$

is also a ring homomorphism. Furthermore,  $\text{Ker } \hat{\varphi} = (\text{Ker } \varphi)[x]$  and  $\text{Im } \hat{\varphi} = (\text{Im } \varphi)[x]$ . (Note:  $\text{Ker } \varphi$  and  $\text{Im } \varphi$  are rings by Theorem 30.13, so  $(\text{Ker } \varphi)[x]$  and  $\text{Im } \hat{\varphi} = (\text{Im } \varphi)[x]$  are meaningful.)

**Proof:** Let  $f = \sum_{i=0}^m a_i x^i$ ,  $g = \sum_{j=0}^n b_j x^j$  be arbitrary polynomials in  $R[x]$ . We

show that  $\hat{\varphi}$  preserves addition. Here we may assume  $m = n$ , for we may add  $0x^{m+1} + 0x^{m+2} + \dots + 0x^n$  to  $f$  in case  $m < n$  and  $0x^{n+1} + 0x^{n+2} + \dots + 0x^m$  to  $g$  in case  $n < m$ . We have

$$\begin{aligned} (f+g)\hat{\varphi} &= \left( \sum_{i=0}^m a_i x^i + \sum_{j=0}^n b_j x^j \right) \hat{\varphi} \\ &= \left( \sum_{i=0}^m a_i x^i + \sum_{i=0}^m b_i x^i \right) \hat{\varphi} \\ &= \left( \sum_{i=0}^m (a_i + b_i) x^i \right) \hat{\varphi} \\ &= \sum_{i=0}^m [(a_i + b_i)\varphi] x^i \\ &= \sum_{i=0}^m (a_i \varphi + b_i \varphi) x^i \\ &= \sum_{i=0}^m (a_i \varphi) x^i + \sum_{i=0}^m (b_i \varphi) x^i \\ &= f\hat{\varphi} + g\hat{\varphi} \end{aligned}$$

and so  $\hat{\varphi}$  preserves addition. As for multiplication (here we do not have to assume  $m = n$ ), we observe

$$\begin{aligned} (fg)\hat{\varphi} &= \left[ \sum_{k=0}^{m+n} \left( \sum_{i+j=k} a_i b_j \right) x^k \right] \hat{\varphi} \\ &= \sum_{k=0}^{m+n} \left[ \left( \sum_{i+j=k} a_i b_j \right) \varphi \right] x^k \end{aligned}$$

$$\begin{aligned}
&= \sum_{k=0}^{m+n} \left( \sum_{i+j=k} (a_i b_j) \varphi \right) x^k \\
&= \sum_{k=0}^{m+n} \left( \sum_{i+j=k} a_i \varphi \cdot b_j \varphi \right) x^k \\
&= \left( \sum_{i=0}^m (a_i \varphi) x^i \right) \left( \sum_{j=0}^n (b_j \varphi) x^j \right) \\
&= f \hat{\varphi} \cdot g \hat{\varphi}.
\end{aligned}$$

Thus  $\hat{\varphi}$  preserves multiplication as well. So  $\hat{\varphi}$  is a ring homomorphism.

A polynomial  $\sum_{i=0}^m a_i x^i$  belongs to the kernel of  $\hat{\varphi}$  if and only if  $\left( \sum_{i=0}^m a_i x^i \right) \hat{\varphi} = \sum_{i=0}^m (a_i \varphi) x^i$  is the zero polynomial in  $S[x]$ , so if and only if the coefficients  $a_i \varphi$  are all equal to  $0 \in S$  ( $i = 0, 1, \dots, m$ ), so if and only if  $a_i \in \text{Ker } \varphi$  for all  $i = 0, 1, \dots, m$ , so if and only if  $\sum_{i=0}^m a_i x^i \in (\text{Ker } \varphi)[x]$ .

A polynomial  $\sum_{i=0}^m c_i x^i \in S[x]$  belongs to the image of  $\hat{\varphi}$  if and only if  $\sum_{i=0}^m c_i x^i = \left( \sum_{i=0}^m a_i x^i \right) \hat{\varphi}$  for some  $\sum_{i=0}^m a_i x^i \in R[x]$ , so (assuming  $m = n$  without loss of generality) if and only if, for each  $i = 0, 1, \dots, m$ , there is an  $a_i \in R$  such that  $c_i = a_i \varphi$ , so if and only if  $c_i \in \text{Im } \varphi$  for all  $i = 0, 1, \dots, m$ , and so if and only if  $\sum_{i=0}^m c_i x^i \in (\text{Im } \varphi)[x]$ . □

As an illustration of Lemma 33.7, we consider the natural homomorphism  $v: \mathbb{Z} \rightarrow \mathbb{Z}_3$ . Then the mapping  $\hat{v}: \mathbb{Z}[x] \rightarrow \mathbb{Z}_3[x]$  is given by reducing the coefficients modulo 3. For example,

$$\begin{aligned}
(5x^3 - 4x^2 + 2x + 1) \hat{v} &= \bar{2}x^3 + \bar{2}x^2 + \bar{2}x + \bar{1} \\
(6x^4 - 3x^2 + x + 5) \hat{v} &= \bar{1}x + \bar{2}.
\end{aligned}$$

The reader will easily verify that

$$\begin{aligned}
&(5x^3 - 4x^2 + 2x + 1)(6x^4 - 3x^2 + x + 5) \\
&= 30x^7 - 24x^6 - 3x^5 + 23x^4 + 15x^3 - 21x^2 + 11x + 5,
\end{aligned}$$

whose image under  $\hat{v}$  is

$$\begin{aligned} &= \overline{30}x^7 - \overline{24}x^6 - \overline{3}x^5 + \overline{23}x^4 + \overline{15}x^3 - \overline{21}x^2 + \overline{11}x + \overline{5} \\ &= \overline{2}x^4 + \overline{2}x + \overline{2}. \end{aligned}$$

We have also  $(\overline{2}x^3 + \overline{2}x^2 + \overline{2}x + \overline{1})(\overline{1}x + \overline{2}) = \overline{2}x^4 + \overline{2}x + \overline{2}$ .

If  $\varphi: R \rightarrow S$  is an isomorphism, then  $\text{Ker } \varphi = 0$  and  $\text{Im } \varphi = S$ . This gives the following corollary to Lemma 33.7.

**33.8 Theorem:** *If  $R$  and  $S$  are isomorphic rings, then  $R[x]$  and  $S[x]$  are isomorphic.* □

Let  $R$  be a ring. Adjoining an indeterminate  $x$  to  $R$ , we get the ring  $R[x]$ . Now we can adjoin a new indeterminate  $y$  to  $R[x]$  and get the ring

$(R[x])[y] := R[x][y]$ . The elements of  $R[x][y]$  are of the form  $\sum_{i=0}^m f_i y^i$ , where

$f_i \in R[x]$ . Similarly we can construct the ring  $R[y][x] := (R[y])[x]$ . We show that they are isomorphic.

**33.9 Lemma:** *Let  $R$  be a ring and let  $x, y$  be two indeterminates over  $R$ . Then  $R[x][y] \cong R[y][x]$ .*

**Proof:** We consider the mapping  $T: R[x][y] \rightarrow R[y][x]$ , given by

$$\sum_{i=0}^m \left( \sum_{j=0}^n a_{ij} x^j \right) y^i \longrightarrow \sum_{j=0}^n \left( \sum_{i=0}^m a_{ij} y^i \right) x^j,$$

which seems to be the only reasonable mapping from  $R[x][y]$  to  $R[y][x]$ . It certainly preserves addition, for we have

$$\begin{aligned} & \left[ \sum_{i=0}^m \left( \sum_{j=0}^n a_{ij} x^j \right) y^i + \sum_{i=0}^r \left( \sum_{j=0}^s b_{ij} x^j \right) y^i \right] T \\ &= \left[ \sum_{i=0}^m \left( \sum_{j=0}^n a_{ij} x^j + \sum_{j=0}^s b_{ij} x^j \right) y^i \right] T \quad (\text{assuming } r = m \text{ without loss of} \\ & \hspace{20em} \text{generality}) \\ &= \left[ \sum_{i=0}^m \left( \sum_{j=0}^{\max(n,s)} (a_{ij} + b_{ij}) x^j \right) y^i \right] T \quad (\text{assuming } s = n \text{ without loss of generality}) \end{aligned}$$

$$\begin{aligned}
&= \sum_{j=0}^m \left( \sum_{i=0}^m (a_{ij} + b_{ij}) y^i \right) x^j \\
&= \sum_{j=0}^m \left( \sum_{i=0}^m a_{ij} y^i + \sum_{i=0}^m b_{ij} y^i \right) x^j \\
&= \sum_{j=0}^m \left( \sum_{i=0}^m a_{ij} y^i \right) x^j + \sum_{j=0}^m \left( \sum_{i=0}^m b_{ij} y^i \right) x^j \\
&= \left[ \sum_{i=0}^m \left( \sum_{j=0}^m a_{ij} x^j \right) y^i \right] T + \left[ \sum_{i=0}^m \left( \sum_{j=0}^m b_{ij} x^j \right) y^i \right] T
\end{aligned}$$

for all  $\sum_{i=0}^m \left( \sum_{j=0}^m a_{ij} x^j \right) y^i$ ,  $\sum_{i=0}^m \left( \sum_{j=0}^m b_{ij} x^j \right) y^i \in R[x][y]$ .

Secondly  $T$  preserves multiplication of polynomials of the form  $(ax^j)y^i$  (i.e., monomials over  $R[x]$ , whose eventually nonzero coefficients in  $R[x]$  are themselves monomials over  $R$ ; they will be referred to as *monomials in  $R[x][y]$  over  $R$* ). We indeed have

$$\begin{aligned}
[(a_{ij} x^j) y^i \cdot (b_{rs} x^s) y^r] T &= [(a_{ij} x^j)(b_{rs} x^s) y^{i+r}] T \quad (\text{def. of multiplication in } R[x][y]) \\
&= [(a_{ij} b_{rs} x^{j+s}) y^{i+r}] T \quad (\text{def. of multiplication in } R[x]) \\
&= (a_{ij} b_{rs} y^{i+r}) x^{j+s} \\
&= [(a_{ij} y^i)(b_{rs} y^r)] x^{j+s} \\
&= (a_{ij} y^i) x^j \cdot (b_{rs} y^r) x^s \\
&= [(a_{ij} x^j) y^i] T \cdot [(b_{rs} x^s) y^r] T
\end{aligned}$$

for all monomials  $(a_{ij} x^j) y^i$ ,  $(b_{rs} x^s) y^r$  in  $R[x][y]$ .

Thirdly,  $T$  preserves multiplication of arbitrary polynomials. Any polynomial can be written as  $p_1 + p_2 + \cdots + p_t$ , where  $p_1, p_2, \dots, p_t$  are suitable monomials. Now for all polynomials  $p_1 + p_2 + \cdots + p_t$ ,  $q_1 + q_2 + \cdots + q_u$  in  $R[x][y]$ , where  $p$ 's and  $q$ 's are monomials, we have

$$\begin{aligned}
&[(p_1 + p_2 + \cdots + p_t)(q_1 + q_2 + \cdots + q_u)] T \\
&= \left( \sum_{i,j} p_i q_j \right) T \quad (\text{by distributivity}) \\
&= \sum_{i,j} (p_i q_j) T \quad (\text{since } T \text{ preserves addition})
\end{aligned}$$

$$\begin{aligned}
&= \sum_{i,j} p_i T \cdot q_j T && \text{(since } T \text{ preserves products of monomials)} \\
&= (p_1 T + p_2 T + \cdots + p_r T)(q_1 T + q_2 T + \cdots + q_u T) \\
&= (p_1 + p_2 + \cdots + p_r) T \cdot (q_1 + q_2 + \cdots + q_u) T,
\end{aligned}$$

so  $T$  preserves arbitrary products. Hence  $T$  is a ring homomorphism.

$T$  is one-to-one, for if  $\sum_{i=0}^{\infty} \left( \sum_{j=0}^{\infty} a_{ij} x^j \right) y^i \in R[x][y]$  is in the kernel of  $T$ , then

its image  $\sum_{j=0}^{\infty} \left( \sum_{i=0}^{\infty} a_{ij} y^i \right) x^j$  is the zero polynomial in  $R[y][x]$ , so all the

coefficients  $\sum_{i=0}^{\infty} a_{ij} y^i$  are equal to the zero polynomial in  $R[y]$ , so all

elements  $a_{ij}$  of  $R$  are equal to the zero element in  $R$ , so all polynomials

$\sum_{j=0}^{\infty} a_{ij} x^j$  are the zero polynomial in  $R[x]$ , so  $\sum_{i=0}^{\infty} \left( \sum_{j=0}^{\infty} a_{ij} x^j \right) y^i$  is the zero

polynomial in  $R[x][y]$ . Thus  $\text{Ker } T$  consists of the zero polynomial and  $T$  is one-to-one.

Moreover,  $T$  is onto, for any polynomial  $\sum_{j=0}^{\infty} \left( \sum_{i=0}^{\infty} a_{ij} y^i \right) x^j$  in  $R[y][x]$  is the

image of the polynomial  $\sum_{i=0}^{\infty} \left( \sum_{j=0}^{\infty} a_{ij} x^j \right) y^i$  in  $R[x][y]$ .

Hence  $T$  is an isomorphism from  $R[x][y]$  onto  $R[y][x]$ . □

In view of this result, we identify  $R[x][y]$  and  $R[y][x]$ . To simplify the notation, we write  $R[x,y]$  for  $R[x][y]$ . The elements of  $R[x,y]$  are of the

form  $\sum_{i,j} a_{ij} x^i y^j$ , where  $a_{ij} \in R$  and there are finitely many terms in the

sum. Multiplication is carried out in the customary way, using distributivity and collecting terms. We have  $R[x,y] = R[y,x]$ .

We can of course adjoin a new indeterminate  $z$  to  $R[x,y]$  and obtain  $(R[x,y])[z] = (R[x][y])[z] =: R[x][y][z]$ . We see

$$\begin{aligned}
 R[x][y][z] &= (R[x][y])[z] && \text{(definition)} \\
 &\cong (R[x][z])[y] && \text{(Lemma 33.9 with } R[x],z \text{ in place of } R,x) \\
 &\cong (R[z][x])[y] && \text{(Lemma 33.9 and Theorem 33.8)} \\
 &\cong (R[z][y])[x] && \text{(Lemma 33.9 with } R[z] \text{ in place of } R) \\
 &\cong (R[y][z])[x] \\
 &\cong (R[y][x])[z].
 \end{aligned}$$

We regard these six rings as identical and write  $R[x,y,z]$  for it. The notations " $R[x,y,z]$ ", " $R[x,z,y]$ ", " $R[z,x,y]$ ", " $R[z,y,x]$ ", " $R[y,z,x]$ ", " $R[y,x,z]$ " will mean the same ring.

More generally, if  $x_1, x_2, \dots, x_n$  are indeterminates over a ring  $R$ , then  $R[x_1, x_2, \dots, x_n]$  is defined to be the ring  $R[x_1, x_2, \dots, x_{n-1}][x_n]$ . It is isomorphic to each one of the  $n!$  rings  $R[x_{i_1}, x_{i_2}, \dots, x_{i_n}]$ , where  $\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$  runs through the permutations in  $S_n$ . These  $n!$  isomorphic rings will be considered identical. Elements of  $R[x_1, x_2, \dots, x_n]$  are of the form

$$\sum_{i=0}^{N_1} \sum_{j=0}^{N_2} \dots \sum_{l=0}^{N_n} a_{ij\dots l} x_1^i x_2^j \dots x_n^l, \quad a_{ij\dots l} \in R.$$

The polynomials in  $R[x_1, x_2, \dots, x_n]$  of the form  $ax_1^i x_2^j \dots x_n^l$  will be called *monomials over  $R$* . It is customary to omit the indeterminates with exponent zero in a monomial. For example,  $ax_1^0 x_2^2 x_3^0 x_4^3$  in  $R[x_1, x_2, x_3, x_4]$  is written  $ax_2^2 x_4^3$ . An exponent is dropped when it is equal to 1. If  $R$  does not have an identity, the indeterminates  $x_1, x_2, \dots, x_n$  are *not* elements of  $R[x_1, x_2, \dots, x_n]$  and the expressions  $x_1^i x_2^j \dots x_n^l$  are *not* polynomials.

The *degree* of a nonzero monomial  $ax_1^i x_2^j \dots x_n^l$  is defined to be the nonnegative integer  $i + j + \dots + l$ . The *total degree* of a polynomial  $f =$

$\sum_{i=0}^{N_1} \sum_{j=0}^{N_2} \dots \sum_{l=0}^{N_n} a_{ij\dots l} x_1^i x_2^j \dots x_n^l$  is defined to be the maximum of the degrees of the monomials  $a_{ij\dots l} x_1^i x_2^j \dots x_n^l$  with  $a_{ij\dots l} \neq 0$ . The total degree of  $f$  will be denoted by  $\deg f$ . The degree of  $f$ , considered as an element of  $R[x_1, \dots, x_{h-1}, x_{h+1}, \dots, x_n][x_h]$  will be called the *degree of  $f$  in  $x_h$* ; this will

be written  $\deg_h f$  ( $h = 1, 2, \dots, n$ ). The analog of Lemma 33.3 holds for polynomials in  $n$  indeterminates, both with the total degree and the degree in  $x_h$  in place of  $\deg f$ .

We record a lemma that can be proved by induction on the number of indeterminates.

**33.10 Lemma:** *Let  $R$  be a ring and  $x_1, x_2, \dots, x_n$  indeterminates over  $R$ .*

- (1) *If  $R$  is commutative, then  $R[x_1, x_2, \dots, x_n]$  is commutative.*
- (2) *If  $R$  has an identity, then  $R[x_1, x_2, \dots, x_n]$  has an identity.*
- (3) *If  $R$  has no zero divisors, then  $R[x_1, x_2, \dots, x_n]$  has no zero divisors.*
- (4) *If  $R$  is an integral domain, then  $R[x_1, x_2, \dots, x_n]$  is an integral domain.*

### Exercises

1. Evaluate:  $(5x^2 - 3x + 1)(7x^3 + 6x - 1)$  in  $\mathbb{Z}_8[x]$ ,  
 $(3x^3 + 4x + 1)(3x^2 + 7x + 2)$  in  $\mathbb{Z}_9[x]$ ,

$\left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}x^4 + \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}x^2 + \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}\right] \left[\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}x^2 - \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}x + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\right]$  in  
 $(\text{Mat}_2(\mathbb{Z}))[x]$ ,

$\left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}x^3 + \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}x^2 + \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\right] \left[\begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}x^2 + \begin{pmatrix} 1 & 5 \\ 2 & 0 \end{pmatrix}x + \begin{pmatrix} 2 & 4 \\ 1 & 0 \end{pmatrix}\right]$  in  
 $(\text{Mat}_2(\mathbb{Z}_7))[x]$ ,

(we dropped the bars for ease of notation).

2. Let  $R, R_1, R_2$  be rings. Prove that

$$(\text{Mat}_2(R))[x] \cong \text{Mat}_2 R[x] \quad \text{and} \quad (R_1 \oplus R_2)[x] \cong R_1[x] \oplus R_2[x]$$

(see §29, Ex. 10).

3. Generalize Lemma 33.7 to polynomial rings in  $n$  indeterminates.

4. Let  $R$  be a commutative ring with identity and let  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$  be a zero divisor in  $R[x]$ . Show that there exists a nonzero  $b$  in  $R$  such that  $ba_n = ba_{n-1} = \dots = ba_0 = 0$ .

5. Let  $R$  be a ring and  $f = \sum_{i=0}^{N_1} \sum_{j=0}^{N_2} \dots \sum_{l=0}^{N_n} a_{ij\dots l} x_1^i x_2^j \dots x_n^l \in R[x_1, x_2, \dots, x_n]$ .

Prove that  $\deg_1 f$  is the largest  $i$  such that  $a_{ij\dots l} \neq 0$ ,  $\deg_2 f$  is the largest  $j$  such that  $a_{ij\dots l} \neq 0$ , ...,  $\deg_n f$  is the largest  $l$  such that  $a_{ij\dots l} \neq 0$ .

6. Extend Lemma 33.3 to polynomial rings in  $n$  indeterminates, both with total degree and the degree in  $x_h$  in place of the degree of  $f$ .