Appendix D

Proof that $R[x]$ is a Ring

In this appendix, we will give a formal proof that $R[x]$ is a commutative ring when R is a commutative ring. Before we give the proof, we will show how to write the sum and product of two polynomials using summation notation. Let $f(x), g(x) \in R[x]$ with

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \text{ with } a_n \neq 0, \text{ and}$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0 \text{ with } b_m \neq 0.$$

Since it must be true that $m \leq n$ or $n \leq m$, we can assume that $m \leq n$ without loss of generality. We will then use the fact that $b_{m+1} = b_{m+2} = \cdots = b_n = 0$, and so we can write

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0, \text{ and}$$
$$g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_2 x^2 + b_1 x + b_0.$$

Using summation notation, we can write the sum and product of these two polynomials as follows:

$$f(x) + g(x) = \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i)\, x^i, \quad \text{and}$$
$$f(x)g(x) = \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{j=0}^{n+m}\left(\sum_{i=0}^{j}(a_{j-i}b_i)\right) x^j, \quad \text{or equivalently}$$
$$f(x)g(x) = \sum_{j=0}^{n+m}\left(\sum_{r+s=j}(a_r b_s)\right) x^j.$$

Theorem D.-1. *If R is a commutative ring, then $R[x]$ is a commutative ring. In addition, if the ring R has an identity, then the ring $R[x]$ has an identity.*

Proof. Let R be a commutative ring and let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0, \text{and}$$
$$h(x) = c_k x^k + c_{k-1}x^{k-1} + \cdots + c_1 x + c_0$$

be elements of $R[x]$. In proving the ring properties for $R[x]$, we will assume (without loss of generality) that $k \leq m \leq n$ and extend the polynomials $g(x)$ and $h(x)$ to have n coefficients. This means that for $m < i \leq n$, $b_i = 0$, and for $k < i \leq n$, $c_i = 0$.

The definitions of addition and multiplication of polynomials show that $f(x) + g(x)$ and $f(x)g(x)$ are polynomials in $R[x]$, so $R[x]$ is closed under addition and multiplication.

To show that addition is commutative in $R[x]$, we use the commutativity of addition in R and obtain

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i)x^i = \sum_{i=0}^{n} (b_i + a_i)x^i = g(x) + f(x).$$

Thus, addition is commutative in $R[x]$.

For associativity of addition in $R[x]$, the associativity of addition in R gives us

$$\begin{aligned}
[f(x) + g(x)] + h(x) &= \left(\sum_{i=0}^{n} (a_i + b_i)x^i \right) + \sum_{i=0}^{n} c_i x^k \\
&= \sum_{i=0}^{n} [(a_i + b_i) + c_i]x^i \\
&= \sum_{i=0}^{n} [a_i + (b_i + c_i)]x^i \\
&= \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} (b_i + c_i)x^i \\
&= f(x) + [g(x) + h(x)].
\end{aligned}$$

Therefore, addition is associative in $R[x]$.

We can show that an additive identity in $R[x]$ is the polynomial $z(x) = 0_R$, the polynomial all of whose coefficients are 0_R, as follows:

$$f(x) + z(x) = \sum_{i=1}^{n} a_i x^i + z(x) = \sum_{i=1}^{n} (a_i + 0_R)\, x^i = \sum_{i=0}^{n} a_i x^i = f(x).$$

Therefore, $z(x)$ is an additive identity in $R[x]$.

We will now show that $R[x]$ contains an additive inverse for $f(x)$ (and hence for any element of $R[x]$). For each i with $0 \leq i \leq n$, we know that $a_i \in R$ and hence, a_i has an additive inverse, $-a_i \in R$. Let

$$q(x) = \sum_{i=0}^{n} (-a_i)x^i = (-a_n)x^n + (-a_{n-1})x^{n-1} + \cdots + (-a_1)x + (-a_0).$$

Then $q(x) \in R[x]$ and

$$f(x) + q(x) = \sum_{i=0}^{n} [a_i + (-a_i)]\, x^i = \sum_{i=0}^{n} 0_R x^i = z(x).$$

Therefore, $R[x]$ contains an additive inverse for each of its elements.

We now turn our attention to multiplication in $R[x]$. We will first show that multiplication is commutative. Using the definition of multiplication of polynomials, we see that

$$\begin{aligned}
f(x)g(x) &= \left(\sum_{i=0}^{n} a_i x^i \right) \left(\sum_{i=0}^{m} b_i x^i \right) \\
&= \left(\sum_{i=0}^{n+m} \left(\sum_{r+s=i} (a_r b_s) \right) x^i \right). \qquad \text{(D.1)}
\end{aligned}$$

Since $s + r = r + s = i$ and multiplication in R is commutative, we see that $a_r b_s = b_s a_r$ and hence, we can rewrite equation (D.1) as follows:

$$\begin{aligned} f(x)g(x) &= \left(\sum_{i=0}^{n+m} \left(\sum_{s+r=i} (b_s a_r) \right) x^i \right) \\ &= \left(\sum_{i=0}^{n} a_i x^i \right) \left(\sum_{i=0}^{n} b_i x^i \right) \\ &= g(x)f(x). \end{aligned}$$

This shows that multiplication in $R[x]$ is commutative.

We will now show that multiplication is an associative operation in $R[x]$. (Note that the notation in this part of the proof can be a bit overwhelming; this is why we explored a special case of the associative property of multiplication in Activity 8.16. It will help in understanding the notation in this proof to have the work from this activity to refer to while reading the proof.) We will start with the formula for $f(x)g(x)$ in equation (D.1). To simplify the notation, for $0 \leq i \leq n + m$, we let $u_i = \sum_{r+s=i} a_r b_s$. We then obtain

$$\begin{aligned} [f(x)g(x)]h(x) &= \left(\sum_{i=0}^{n+m} u_i x^i \right) \left(\sum_{i=0}^{k} c_i x^i \right) \\ &= \sum_{j=0}^{(n+m)+k} \left(\sum_{p+q=j} u_p c_q \right) x^j. \end{aligned}$$

We can now substitute for u_p and then use the fact that

$$\left(\sum_{r+s=p} a_r b_s \right) c_q = \sum_{r+s=p} (a_r b_s)\, c_q,$$

which is true by the distributive property in R. This gives

$$\begin{aligned} [f(x)g(x)]h(x) &= \sum_{j=0}^{(n+m)+k} \left[\sum_{p+q=j} \left(\sum_{r+s=p} a_r b_s \right) c_q \right] x^j \\ &= \sum_{j=0}^{(n+m)+k} \left[\sum_{p+q=j} \left(\sum_{r+s=p} (a_r b_s)\, c_q \right) \right] x^j. \end{aligned} \tag{D.2}$$

In equation (D.2), notice that $r+s+q = p+q = j$, and so equation (D.2) shows that the coefficient of x^j in $[f(x)g(x)]h(x)$ is the sum of all products of the form $(a_r b_s)\, c_q$ where $r + s + q = j$. This means that we can rewrite equation (D.2) as follows:

$$[f(x)g(x)]h(x) = \sum_{j=0}^{(n+m)+k} \left[\sum_{r+s+q=j} (a_r b_s)\, c_q \right] x^j. \tag{D.3}$$

Using a similar procedure for $f(x)[g(x)h(x)]$, we see that

$$\begin{aligned} f(x)[g(x)h(x)] &= \left(\sum_{i=0}^{n} a_i x^i\right)\left[\sum_{w=0}^{m+k}\left(\sum_{s+q=w} b_s c_q\right)x^w\right] \\ &= \sum_{j=0}^{n+(m+k)}\left[\sum_{r+w=j}\left(a_r \sum_{s+q=w} b_s c_q\right)\right]x^j \\ &= \sum_{j=0}^{n+(m+k)}\left[\sum_{r+w=j}\left(\sum_{s+q=w} a_r\left(b_s c_q\right)\right)\right]x^j. \end{aligned} \tag{D.4}$$

In equation (D.4), $r+s+q = r+w = j$, and so equation (D.4) shows that the coefficient of x^j in $f(x)[g(x)h(x)]$ is the sum of all products of the form $a_r\left(b_s c_q\right)$ where $r+s+q=j$. Therefore, we can write

$$f(x)[g(x)h(x)] = \sum_{j=0}^{n+(m+k)}\left[a_r\left(b_s c_q\right)\right]x^j. \tag{D.5}$$

Since multiplication in R is associative, we know that $a_r\left(b_s c_q\right) = \left(a_r b_s\right)c_q$, so using this and equation (D.5), we can conclude that

$$f(x)[g(x)h(x)] = \sum_{j=0}^{n+(m+k)}\left[\left(a_r b_s\right)c_q\right]x^j. \tag{D.6}$$

Comparing equations (D.3) and (D.6), we see that $[f(x)g(x)]h(x) = f(x)[g(x)h(x)]$, which proves that multiplication in $R[x]$ is associative.

We will now prove the distributive law. (Since we have proved that multiplication in $R[x]$ is commutative, we only have to prove one of the distributive laws.) For this, recall that we have assumed that $k \leq m \leq n$, and so

$$\begin{aligned} f(x)[g(x)+h(x)] &= \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m}(b_j + c_j)x^j\right) \\ &= \sum_{j=0}^{n+m}\left[\sum_{r+s=j} a_r(b_s + c_s)\right]x^j \\ &= \sum_{j=0}^{n+m}\left[\sum_{r+s=j}\left(a_r b_s + a_r c_s\right)\right]x^j \\ &= \sum_{j=0}^{n+m}\left(\sum_{r+s=j} a_r b_s\right)x^j + \sum_{j=0}^{n+m}\left(\sum_{r+s=j} a_r c_s\right)x^j \\ &= f(x)g(x) + f(x)h(x). \end{aligned}$$

Therefore, multiplication distributes over addition in $R[x]$, and we conclude that $R[x]$ is a ring.

Finally, we will prove that if R has an identity, 1_R, then $R[x]$ also contains an identity. Let

$u(x) = 1_R$. Then $u(x) \in R[x]$ and

$$\begin{aligned} f(x)u(x) &= \left(\sum_{i=0}^{n} a_i x^i \right) (1_R) \\ &= f(x). \end{aligned}$$

Therefore, if R is a commutative ring with identity, then $R[x]$ is also a commutative ring with identity. ■