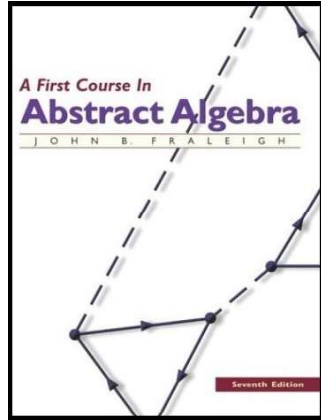


Introduction to Modern Algebra

Part IV. Rings and Fields IV.22. Rings of Polynomials



()

Theorem 22.2

Theorem 22.2. The set $R[x]$ of all polynomials in an indeterminate x with coefficients in a ring R is a ring under polynomial addition and multiplication as defined above. If R is commutative, then so is $R[x]$, and if R has units $1 \neq 0$, then 1 (a constant polynomial) is also unity for $R[x]$.

Proof. Since $\langle R, + \rangle$ is an abelian group, then $\langle R[x], + \rangle$ is an abelian group since $c_n = a_n + b_n = b_n + a_n (R_1)$. For associativity of

multiplication, let $f(x), g(x), h(x) \in R[x]$ such that $f(x) = \sum_{i=0}^{\infty} a_i x^i$,

$$g(x) = \sum_{j=0}^{\infty} b_j x^j, \text{ and } h(x) = \sum_{k=0}^{\infty} c_k x^k. \text{ Then}$$

$$(f(x) \cdot g(x)) \cdot h(x) = \left[\left(\sum_{n=0}^{\infty} a_n x^n \right) \cdot \left(\sum_{j=0}^{\infty} b_j x^j \right) \right] \cdot \left(\sum_{k=0}^{\infty} c_k x^k \right)$$

()

Theorem 22.2 (continued 1)

Proof (continued).

$$\begin{aligned} &= \left[\sum_{n=0}^{\infty} \left(\sum_{i=0}^{\infty} a_i b_{n-i} \right) x^n \right] \cdot \left(\sum_{k=0}^{\infty} c_k x^k \right) \\ &= \sum_{s=0}^{\infty} \left[\sum_{n=0}^s \left(\sum_{i=0}^n a_i b_{n-i} \right) c_{s-n} \right] x^s \\ &= \sum_{s=0}^{\infty} \left(\sum_{i+j+k=s} a_i b_j c_k \right) x^s \text{ since } (i) + (n-i) + (s-n) = s \\ &= \sum_{s=0}^{\infty} \left[\sum_{m=0}^s a_{s-m} \left(\sum_{j=0}^m b_j c_{m-j} \right) \right] x^s \text{ since } (s-m) + (j) + (m-j) = s \\ &= \left(\sum_{i=0}^{\infty} a_i x^i \right) \cdot \left[\sum_{m=0}^{\infty} \left(\sum_{k=0}^m b_j c_{m-j} \right) x^m \right] \end{aligned}$$

()

Theorem 22.2 (continued 2)

Proof (continued).

$$= \left(\sum_{i=0}^{\infty} a_i x^i \right) \cdot \left[\left(\sum_{j=0}^{\infty} b_j x^j \right) \left(\sum_{k=0}^{\infty} c_k x^k \right) \right] = f(x) \cdot (g(x) \cdot h(x))$$

and R_2 holds. Now for the distribution laws. With the notation above,

$$\begin{aligned} f(x) \cdot (g(x) + h(x)) &= \left(\sum_{i=0}^{\infty} a_i x^i \right) \cdot \left[\left(\sum_{j=0}^{\infty} b_j x^j \right) + \left(\sum_{k=0}^{\infty} c_k x^k \right) \right] \\ &= \left(\sum_{i=0}^{\infty} a_i x^i \right) \left(\sum_{j=0}^{\infty} (b_j + c_j) x^j \right) = \sum_{n=0}^{\infty} \left(\sum_{i=0}^n a_i (b_{n-i} + c_{n-i}) \right) x^n \\ &= \sum_{n=0}^{\infty} \left(\sum_{i=0}^n (a_i b_{n-i} + a_i c_{n-i}) \right) x^n \end{aligned}$$

()

Theorem 22.2 (continued 3)

Proof (continued).

$$\begin{aligned}
 &= \sum_{n=0}^{\infty} \left[\left(\sum_{i=0}^n a_i b_{n-i} \right) + \left(\sum_{i=0}^n a_i c_{n-i} \right) \right] x^n \\
 &= \sum_{n=0}^{\infty} \left(\sum_{i=0}^n a_i b_{n-i} \right) x^n + \sum_{n=0}^{\infty} \left(\sum_{i=0}^n a_i c_{n-i} \right) x^n \\
 &= \left(\sum_{i=0}^{\infty} a_i x^i \right) \left(\sum_{j=0}^{\infty} b_j x^j \right) + \left(\sum_{i=0}^{\infty} a_i x^i \right) \left(\sum_{n=0}^{\infty} c_n x^n \right) \\
 &= f(x) \cdot g(x) + f(x) \cdot h(x).
 \end{aligned}$$

Similarly,

$$(f(x) + g(x)) \cdot h(x) = \left[\left(\sum_{i=0}^{\infty} a_i x^i \right) + \left(\sum_{j=0}^{\infty} b_j x^j \right) \right] \cdot \left(\sum_{n=0}^{\infty} c_n x^n \right)$$

()

Theorem 22.2 (continued 4)

Proof (continued).

$$\begin{aligned}
 &= \left(\sum_{n=0}^{\infty} (a_i + b_i) x^i \right) \cdot \left(\sum_{n=0}^{\infty} c_n x^n \right) = \sum_{n=0}^{\infty} \left(\sum_{i=0}^n (a_i + b_i) c_{n-i} \right) x^n \\
 &= \sum_{n=0}^{\infty} \left(\sum_{i=0}^n (a_i c_{n-i} + b_i c_{n-i}) \right) x^n \\
 &= \sum_{n=0}^{\infty} \left[\left(\sum_{i=0}^n a_i c_{n-i} \right) + \left(\sum_{i=0}^n b_i c_{n-i} \right) \right] x^n \\
 &= \sum_{n=0}^{\infty} \left(\sum_{i=0}^n a_i c_{n-i} \right) x^n + \sum_{n=0}^{\infty} \left(\sum_{i=0}^n b_i c_{n-i} \right) x^n \\
 &= \left(\sum_{i=0}^{\infty} a_i x^i \right) \left(\sum_{n=0}^{\infty} c_n x^n \right) + \left(\sum_{j=0}^{\infty} b_j x^j \right) \left(\sum_{n=0}^{\infty} c_n x^n \right) \\
 &= f(x) \cdot h(x) + g(x) \cdot h(x).
 \end{aligned}$$

()

Theorem 22.2 (continued 5)

Proof (continued). So the left and right distribution laws hold (R_3) and $R[x]$ is a ring, A claimed. If R is commutative, then

$$\begin{aligned}
 f(x) \cdot g(x) &= \left(\sum_{i=0}^{\infty} a_i x^i \right) \cdot \left(\sum_{j=0}^{\infty} b_j x^j \right) = \sum_{n=0}^{\infty} \left(\sum_{i=1}^n a_i b_{n-i} \right) x^n \\
 &= \sum_{n=0}^{\infty} \left(\sum_{i=1}^n b_{n-i} a_i \right) x^n = \sum_{n=0}^{\infty} \left(\sum_{i=1}^n b_i a_{n-i} \right) x^n \\
 &= \left(\sum_{j=0}^{\infty} b_j x^j \right) \cdot \left(\sum_{i=1}^{\infty} a_i x^i \right) = g(x) \cdot f(x)
 \end{aligned}$$

and $R[x]$ is commutative, as claimed.

()

Theorem 22.2 (continued 6).

Proof (continued). If $1 \neq 0$ is unity in $R[x]$, then

$$\begin{aligned}
 1 \cdot g(x) &= \left(\sum_{i=0}^n a_i x^i \right) \cdot \left(\sum_{j=0}^{\infty} b_j x^j \right) \text{ where } a_0 = 1, a_i = 0 \text{ for } i \in \mathbb{N} \\
 &= \sum_{n=0}^{\infty} \left(\sum_{i=0}^n a_i b_{n-i} \right) x^n = \sum_{n=0}^{\infty} (a_0 b_n) x^n \\
 &= \sum_{n=0}^{\infty} (1 b_n) x^n = \sum_{n=0}^{\infty} b_n x^n = g(x),
 \end{aligned}$$

and similarly $g(x) \cdot 1 = g(x)$. So the constant polynomial $1 \in R[x]$ is unity in $R[x]$, as claimed. \square

()

Theorem 22.4 The Evaluation Homomorphism for Field Theory.

Theorem 22.4. The Evaluation Homomorphism for Field Theory.

Let F be a subfield of a field E , let $\alpha \in E$, and let x be an indeterminate.

The map $\varphi_\alpha : F[x] \rightarrow E$ defined by

$\varphi_\alpha(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n$ where $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in F[x]$ is a homomorphism of $F[x]$ into E .

Also, $\varphi_\alpha(x) = \alpha$, and φ_α maps F isomorphically by the identity map; that is, $\varphi_\alpha(a) = a$ for $a \in F$. The homomorphism φ_α is the evaluation at α .

Proof. Let $f(x), g(x), h(x) \in F[x]$ where

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m, \text{ and}$$

$$h(x) = f(x) + g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_rx^r \text{ where } c_i = a_i + b_i \text{ for all } i, \text{ and } r = \max\{n, m\}.$$

Theorem 22.4 (continued).

Proof (continued). Then

$$\varphi_\alpha(f(x) + g(x)) = \varphi_\alpha(h(x)) = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_r\alpha^r \text{ and}$$

$$\varphi_\alpha(f(x)) + \varphi_\alpha(g(x)) = (a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n) =$$

$$(a_0 + b_0) + (a_1 + b_1)\alpha + (a_2 + b_2)\alpha^2 + \cdots + (a_r + b_r)\alpha^r =$$

$$c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_r\alpha^r = \varphi_\alpha(h(x)) = \varphi_\alpha(f(x) + g(x)). \text{ Suppose}$$

$$f(x)g(x) = d_0 + d_1x + d_2x^2 + \cdots + d_sx^s \text{ where } d_j = \sum_{i=0}^j a_i b_{j-i}. \text{ Then}$$

$$\varphi_\alpha(f(x)g(x)) = d_0 + d_1\alpha + d_2\alpha^2 + \cdots + d_s\alpha^s, \text{ where } s = m + n, \text{ and}$$

$$\varphi_\alpha(f(x))\varphi_\alpha(g(x)) =$$

$$(a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n) \cdot (b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_m\alpha^m) =$$

$$d_0 + d_1\alpha + d_2\alpha^2 + \cdots + d_s\alpha^s = \varphi_\alpha(\varphi_\alpha(f(x)g(x))). \text{ So } \varphi_\alpha \text{ is a}$$

homomorphism, as claimed.

By the definition of φ_α , we have $\varphi_\alpha(x) = \alpha$ and for constant polynomial $a \in F[x]$, $\varphi_\alpha(a) = a$ for all $a \in F$ (since F is the set of constant polynomials in $F[x]$). □