Example 2. The space of all linear operators on a vector space, with composition as the product, is a linear algebra with identity. It is commutative if and only if the space is one-dimensional.

The reader may have had some experience with the dot product and cross product of vectors in R^3. If so, he should observe that neither of these products is of the type described in the definition of a linear algebra. The dot product is a 'scalar product,' that is, it associates with a pair of vectors a scalar, and thus it is certainly not the type of product we are presently discussing. The cross product does associate a vector with each pair of vectors in R^3; however, this is not an associative multiplication.

The rest of this section will be devoted to the construction of an algebra which is significantly different from the algebras in either of the preceding examples. Let F be a field and S the set of non-negative integers. By Example 3 of Chapter 2, the set of all functions from S into F is a vector space over F. We shall denote this vector space by F^∞. The vectors in F^∞ are therefore infinite sequences $f = (f_0, f_1, f_2, \ldots)$ of scalars f_i in F. If $g = (g_0, g_1, g_2, \ldots)$, g_i in F, and a, b are scalars in F, $af + bg$ is the infinite sequence given by

$$af + bg = (af_0 + bg_0, af_1 + bg_1, af_2 + bg_2, \ldots). \tag{4-1}$$

We define a product in F^∞ by associating with each pair of vectors f and g in F^∞ the vector fg which is given by

$$(fg)_n = \sum_{i=0}^{n} f_i g_{n-i}, \qquad n = 0, 1, 2, \ldots. \tag{4-2}$$

Thus

$$fg = (f_0g_0, f_0g_1 + f_1g_0, f_0g_2 + f_1g_1 + f_2g_0, \ldots)$$

and as

$$(gf)_n = \sum_{i=0}^{n} g_i f_{n-i} = \sum_{i=0}^{n} f_i g_{n-i} = (fg)_n$$

for $n = 0, 1, 2, \ldots$, it follows that multiplication is commutative, $fg = gf$. If h also belongs to F^∞, then

$$\begin{aligned}
[(fg)h]_n &= \sum_{i=0}^{n} (fg)_i h_{n-i} \\
&= \sum_{i=0}^{n} \left(\sum_{j=0}^{i} f_j g_{i-j} \right) h_{n-i} \\
&= \sum_{i=0}^{n} \sum_{j=0}^{i} f_j g_{i-j} h_{n-i} \\
&= \sum_{j=0}^{n} f_j \sum_{i=0}^{n-j} g_i h_{n-i-j} \\
&= \sum_{j=0}^{n} f_j (gh)_{n-j} = [f(gh)]_n
\end{aligned}$$

for $n = 0, 1, 2, \ldots$, so that

$$(fg)h = f(gh). \tag{4-3}$$

We leave it to the reader to verify that the multiplication defined by (4-2) satisfies (b) and (c) in the definition of a linear algebra, and that the vector $1 = (1, 0, 0, \ldots)$ serves as an identity for F^∞. Then F^∞, with the operations defined above, is a commutative linear algebra with identity over the field F.

The vector $(0, 1, 0, \ldots, 0, \ldots)$ plays a distinguished role in what follows and we shall consistently denote it by x. Throughout this chapter x will never be used to denote an element of the field F. The product of x with itself n times will be denoted by x^n and we shall put $x^0 = 1$. Then

$$x^2 = (0, 0, 1, 0, \ldots), \qquad x^3 = (0, 0, 0, 1, 0, \ldots)$$

and in general for each integer $k \geq 0$, $(x^k)_k = 1$ and $(x^k)_n = 0$ for all non-negative integers $n \neq k$. In concluding this section we observe that the set consisting of $1, x, x^2, \ldots$ is both independent and infinite. Thus the algebra F^∞ is not finite-dimensional.

The algebra F^∞ is sometimes called the **algebra of formal power series** over F. The element $f = (f_0, f_1, f_2, \ldots)$ is frequently written

$$f = \sum_{n=0}^{\infty} f_n x^n. \tag{4-4}$$

This notation is very convenient for dealing with the algebraic operations. When used, it must be remembered that it is purely formal. There are no 'infinite sums' in algebra, and the power series notation (4-4) is not intended to suggest anything about convergence, if the reader knows what that is. By using sequences, we were able to define carefully an algebra in which the operations behave like addition and multiplication of formal power series, without running the risk of confusion over such things as infinite sums.

4.2. The Algebra of Polynomials

We are now in a position to define a polynomial over the field F.

Definition. *Let* F[x] *be the subspace of* F^∞ *spanned by the vectors* 1, x, x^2, ... *An element of* F[x] *is called a* **polynomial over** F.

Since $F[x]$ consists of all (finite) linear combinations of x and its powers, a non-zero vector f in F^∞ is a polynomial if and only if there is an integer $n \geq 0$ such that $f_n \neq 0$ and such that $f_k = 0$ for all integers $k > n$; this integer (when it exists) is obviously unique and is called the **degree** of f. We denote the degree of a polynomial f by deg f, and do not assign a degree to the 0-polynomial. If f is a non-zero polynomial of degree n it follows that

$$f = f_0x^0 + f_1x + f_2x^2 + \cdots + f_nx^n, \qquad f_n \neq 0. \tag{4-5}$$

The scalars $f_0, f_1, \ldots, f_n$ are sometimes called the **coefficients** of f, and we may say that f is a polynomial with coefficients in F. We shall call polynomials of the form cx^0 **scalar polynomials,** and frequently write c for cx^0. A non-zero polynomial f of degree n such that $f_n = 1$ is said to be a **monic** polynomial.

The reader should note that polynomials are not the same sort of objects as the polynomial functions on F which we have discussed on several occasions. If F contains an infinite number of elements, there is a natural isomorphism between $F[x]$ and the algebra of polynomial functions on F. We shall discuss that in the next section. Let us verify that $F[x]$ is an algebra.

Theorem 1. *Let* f *and* g *be non-zero polynomials over* F. *Then*

(i) fg *is a non-zero polynomial;*
(ii) *deg* (fg) = *deg* f + *deg* g;
(iii) fg *is a monic polynomial if both* f *and* g *are monic polynomials;*
(iv) fg *is a scalar polynomial if and only if both* f *and* g *are scalar polynomials;*
(v) *if* f + g ≠ 0,

$$\deg (f + g) \leq \max (\deg f, \deg g).$$

Proof. Suppose f has degree m and that g has degree n. If k is a non-negative integer,

$$(fg)_{m+n+k} = \sum_{i=0}^{m+n+k} f_ig_{m+n+k-i}.$$

In order that $f_ig_{m+n+k-i} \neq 0$, it is necessary that $i \leq m$ and $m + n + k - i \leq n$. Hence it is necessary that $m + k \leq i \leq m$, which implies $k = 0$ and $i = m$. Thus

$$(fg)_{m+n} = f_mg_n \tag{4-6}$$

and

$$(fg)_{m+n+k} = 0, \qquad k > 0. \tag{4-7}$$

The statements (i), (ii), (iii) follow immediately from (4-6) and (4-7), while (iv) is a consequence of (i) and (ii). We leave the verification of (v) to the reader. ∎

Corollary 1. *The set of all polynomials over a given field* F *equipped with the operations (4-1) and (4-2) is a commutative linear algebra with identity over* F.

Proof. Since the operations (4-1) and (4-2) are those defined in the algebra F^∞ and since $F[x]$ is a subspace of F^∞, it suffices to prove that the product of two polynomials is again a polynomial. This is trivial when one of the factors is 0 and otherwise follows from (i). ▌

Corollary 2. *Suppose* f, g, *and* h *are polynomials over the field* F *such that* f $\neq$ 0 *and* fg = fh. *Then* g = h.

Proof. Since $fg = fh$, $f(g - h) = 0$, and as $f \neq 0$ it follows at once from (i) that $g - h = 0$. ▌

Certain additional facts follow rather easily from the proof of Theorem 1, and we shall mention some of these.

Suppose

$$f = \sum_{i=0}^{m} f_i x^i \quad \text{and} \quad g = \sum_{j=0}^{n} g_j x^j.$$

Then from (4-7) we obtain,

$$fg = \sum_{s=0}^{m+n} \left(\sum_{r=0}^{s} f_r g_{s-r} \right) x^s. \tag{4-8}$$

The reader should verify, in the special case $f = cx^m$, $g = dx^n$ with c, d in F, that (4-8) reduces to

$$(cx^m)(dx^n) = cdx^{m+n}. \tag{4-9}$$

Now from (4-9) and the distributive laws in $F[x]$, it follows that the product in (4-8) is also given by

$$\sum_{i,j} f_i g_j x^{i+j} \tag{4-10}$$

where the sum is extended over all integer pairs i, j such that $0 \leq i \leq m$, and $0 \leq j \leq n$.

Definition. *Let* $\mathcal{A}$ *be a linear algebra with identity over the field* F. *We shall denote the identity of* $\mathcal{A}$ *by* 1 *and make the convention that* $\alpha^0 = 1$ *for each* α *in* $\mathcal{A}$. *Then to each polynomial* $f = \sum_{i=0}^{n} f_i x^i$ *over* F *and* α *in* $\mathcal{A}$ *we associate an element* $f(\alpha)$ *in* $\mathcal{A}$ *by the rule*

$$f(\alpha) = \sum_{i=0}^{n} f_i \alpha^i.$$

EXAMPLE 3. Let C be the field of complex numbers and let $f = x^2 + 2$.

(a) If $\mathcal{A} = C$ and z belongs to C, $f(z) = z^2 + 2$, in particular $f(2) = 6$ and

$$f\left(\frac{1+i}{1-i}\right) = 1.$$

(b) If $\mathfrak{A}$ is the algebra of all 2×2 matrices over C and if

$$B = \begin{bmatrix} 1 & 0 \\ -1 & 2 \end{bmatrix}$$

then

$$f(B) = 2\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ -1 & 2 \end{bmatrix}^2 = \begin{bmatrix} 3 & 0 \\ -3 & 6 \end{bmatrix}.$$

(c) If $\mathfrak{A}$ is the algebra of all linear operators on C^3 and T is the element of $\mathfrak{A}$ given by

$$T(c_1, c_2, c_3) = (i\sqrt{2}\, c_1, c_2, i\sqrt{2}\, c_3)$$

then $f(T)$ is the linear operator on C^3 defined by

$$f(T)(c_1, c_2, c_3) = (0, 3c_2, 0).$$

(d) If $\mathfrak{A}$ is the algebra of all polynomials over C and $g = x^4 + 3i$, then $f(g)$ is the polynomial in $\mathfrak{A}$ given by

$$f(g) = -7 + 6ix^4 + x^8.$$

The observant reader may notice in connection with this last example that if f is a polynomial over any field and x is the polynomial $(0, 1, 0, \ldots)$ then $f = f(x)$, but he is advised to forget this fact.

Theorem 2. *Let* F *be a field and* $\mathfrak{A}$ *be a linear algebra with identity over* F. *Suppose* f *and* g *are polynomials over* F, *that* α *is an element of* $\mathfrak{A}$, *and that* c *belongs to* F. *Then*

(i) $(cf + g)(\alpha) = cf(\alpha) + g(\alpha)$;
(ii) $(fg)(\alpha) = f(\alpha)g(\alpha)$.

Proof. As (i) is quite easy to establish, we shall only prove (ii). Suppose

$$f = \sum_{i=0}^{m} f_i x^i \quad \text{and} \quad g = \sum_{j=0}^{n} g_j x^j.$$

By (4-10),

$$fg = \sum_{i,j} f_i g_j x^{i+j}$$

and hence by (i),

$$\begin{aligned}(fg)(\alpha) &= \sum_{i,j} f_i g_j \alpha^{i+j} \\ &= \left(\sum_{i=0}^{m} f_i \alpha^i\right)\left(\sum_{j=0}^{n} g_j \alpha^j\right) \\ &= f(\alpha)g(\alpha). \quad \blacksquare\end{aligned}$$

Exercises

1. Let F be a subfield of the complex numbers and let A be the following 2×2 matrix over F

$$A = \begin{bmatrix} 2 & 1 \\ -1 & 3 \end{bmatrix}.$$

For each of the following polynomials f over F, compute $f(A)$.

(a) $f = x^2 - x + 2$;

(b) $f = x^3 - 1$;

(c) $f = x^2 - 5x + 7$.

2. Let T be the linear operator on R^3 defined by

$$T(x_1, x_2, x_3) = (x_1, x_3, -2x_2 - x_3).$$

Let f be the polynomial over R defined by $f = -x^3 + 2$. Find $f(T)$.

3. Let A be an $n \times n$ diagonal matrix over the field F, i.e., a matrix satisfying $A_{ij} = 0$ for $i \neq j$. Let f be the polynomial over F defined by

$$f = (x - A_{11}) \cdots (x - A_{nn}).$$

What is the matrix $f(A)$?

4. If f and g are independent polynomials over a field F and h is a non-zero polynomial over F, show that fh and gh are independent.

5. If F is a field, show that the product of two non-zero elements of F^∞ is non-zero.

6. Let S be a set of non-zero polynomials over a field F. If no two elements of S have the same degree, show that S is an independent set in $F[x]$.

7. If a and b are elements of a field F and $a \neq 0$, show that the polynomials 1, $ax + b$, $(ax + b)^2$, $(ax + b)^3$, ... form a basis of $F[x]$.

8. If F is a field and h is a polynomial over F of degree ≥ 1, show that the mapping $f \to f(h)$ is a one-one linear transformation of $F[x]$ into $F[x]$. Show that this transformation is an isomorphism of $F[x]$ onto $F[x]$ if and only if $\deg h = 1$.

9. Let F be a subfield of the complex numbers and let T, D be the transformations on $F[x]$ defined by

$$T\left(\sum_{i=0}^{n} c_i x^i\right) = \sum_{i=0}^{n} \frac{c_i}{1+i} x^{i+1}$$

and

$$D\left(\sum_{i=0}^{n} c_i x^i\right) = \sum_{i=1}^{n} i c_i x^{i-1}.$$

(a) Show that T is a non-singular linear operator on $F[x]$. Show also that T is not invertible.

(b) Show that D is a linear operator on $F[x]$ and find its null space.

(c) Show that $DT = I$, and $TD \neq I$.

(d) Show that $T[(Tf)g] = (Tf)(Tg) - T[f(Tg)]$ for all f, g in $F[x]$.

(e) State and prove a rule for D similar to the one given for T in (d).

(f) Suppose V is a non-zero subspace of $F[x]$ such that Tf belongs to V for each f in V. Show that V is not finite-dimensional.

(g) Suppose V is a finite-dimensional subspace of $F[x]$. Prove there is an integer $m \geq 0$ such that $D^m f = 0$ for each f in V.