Definition 1. A **linear algebra** over a field F is a vector space $\mathcal{A}$ over F along with a **vector product** which for all $x, y, z \in \mathcal{A}$ and α in $\mathcal{F}$ satisfies

I. (Associativity) $x(yz) = (xy)z$
II. (Distributivity) $x(y+z) = xy + xz$
III. (Scaling) $\alpha xy = (\alpha x)y = x(\alpha y)$

If there is an element $1 \in \mathcal{A}$ such that $1x = x1 = x$ for all $x \in \mathcal{A}$, we have a *linear algebra with identity*. If $xy = yx$ for all $x, y \in \mathcal{A}$, then $\mathcal{A}$ is a *commutative algebra*.

Example 1. (Formal Power Series) The set $F^\infty = \{(f_0, f_1, \dots) \mid f_n \in F\}$ of infinite sequences on F forms a vector space under elementwise addition and scalar multiplication. Equipped with the product $(fg)_n = \sum_{k=0}^{n} f_k g_{n-k}$, the space F^∞ is called the **algebra of formal power series** over F. Choosing $x = (0, 1, 0, 0, \dots)$, any element of F^∞ can be written as $f = \sum_{k=1}^{\infty} f_k x^k$.

Algebra of Polynomials

Definition 2. Let $F[x] = \operatorname{span}\{1, x, x^2, \dots\} \preccurlyeq F^\infty$ contain all finite linear combinations of powers of x. Elements of $F[x]$ are called **polynomials**.

Exercise 1. Let $f, g \in F[x]$ be nonzero polynomials over a field F. Then,

I. fg is a nonzero polynomial.
II. fg is monic if and only if f and g are monic.
III. fg is scalar if and only if f and g are scalar.
IV. $\deg fg = \deg f + \deg g$
V. $\deg(f+g) \leq \max\{\deg f, \deg g\}$

Consequently, the set $F[x]$ of polynomials forms a commutative algebra with identity over F. Given another commutative algebra with identity, we can define *polynomial evaluation* as follows:

Definition 3. Let $\mathcal{A}$ be an algebra with identity over the field F. For any $a \in \mathcal{A}$, define $a^0 = 1_{\mathcal{A}}$. Then to each polynomial $f = \sum_{k=0}^{n} f_k x^k \in F[x]$ and $a \in A$ we associate an element $f(a) \in \mathcal{A}$ by the rule $f(a) = \sum_{k=0}^{n} f_k a^k$.

Exercise 2. For all polynomials $f, g \in F[x]$, scalars $c \in F$, and $a \in \mathcal{A}$,

I. $(cf + g)(a) = cf(a) + g(a)$
II. $(fg)(a) = f(a)g(a)$

Polynomial Long Division

Lemma 1. *Let $f, d \in F[x]$ be nonzero polynomials, with $\deg d \leq \deg f$. Then there exists a polynomial $g \in F[x]$ such that*

$$\text{either } f - dg = 0 \text{ or } \deg(f - dg) < \deg f$$

Proof. Let f and d have leading coefficients a and b, respectively. Choose $g = (\frac{a}{b})x^{\deg f - \deg d}$, so that subtracting dg from f deletes the leading term. □

Theorem 1, (Polynomial Long Division)**.** *For polynomials $f, d \in F[x]$ with $d \neq 0$, there exist unique **quotient** and **remainder** polynomials $q, r \in F[x]$ such that $f = dq + r$, and either $r = 0$ or $\deg r < \deg d$.*

Proof. For existence, we use an iterative process akin to long division.

(1) Initialize $q \leftarrow 0$ and $r \leftarrow f$.
(2) While $f \neq dq + r$ or ($r \neq 0$ and $\deg r \geq \deg d$),
    (a) Choose a polynomial $g \in F[x]$ by Lemma 1 such that
        (i) either $(f - dq) - dg = 0$
        (ii) or $\deg((f - dq) - dg) < \deg(f - dq)$
    (b) In the former case, set $q \leftarrow q + g$ and $r = 0$ and terminate.
    (c) In the latter, set $q \leftarrow q + g$ then $r \leftarrow f - dq$ and continue.
(3) Since $\deg r$ is strictly decreasing with each iteration, the algorithm eventually terminates, leaving us with quotient q and remainder r.

For uniqueness, suppose we have another quotient q' and remainder r'.

(1) Then $f = dq + r = dq' + r'$, so $d(q - q') = r' - r$.
(2) Assume towards contradiction that $q - q' \neq 0$. Then $d(q - q') \neq 0$.
(3) By Exercise 1, $\deg(r' - r) = \deg d(q - q') = \deg d + \deg(q - q')$.
(4) Thus $\max\{\deg r', \deg r\} \geq \deg(r' - r) \geq \deg d$, a contradiction! □

Corollary 1. *Let $c \in F$. A polynomial $f \in F[x]$ is divisible by $(x - c)$ if and only if $f(c) = 0$, in which case c is called a **root** of f.*

Proof. By the theorem, $f = (x - c)q + r$ where r is a scalar polynomial. Therefore, $f(c) = 0q(c) + r(c) = r(c)$ equals zero if and only if $r = 0$. □

Corollary 2. *A polynomial $f \in F[x]$ of degree n has at most n roots.*

Proof. The result is obviously true for polynomials of degree zero and one. Inductively, assume degree $n - 1$ polynomials have at most $n - 1$ roots and let $f \in F[x]$ have degree n. If f has at least one root $c \in F$, we can factor $f = (x - c)q$ uniquely, where $\deg q = n - 1$. Since $f(b) = 0$ if and only if $b = c$ or $q(b) = 0$, it follows inductively that f has at most n roots. □

Polynomial Ideals

Definition 4. A **polynomial ideal** is a subspace $M \preccurlyeq F[x]$ that *absorbs* multiplication, in the sense that $fg \in M$ whenever $f \in M$ and $g \in F[x]$.

Equivalently, a set $M \subset F[x]$ is an ideal if and only if it is closed under linear combinations of its elements with coefficients taken from all of $F[x]$.

EXERCISE 3. Verify the following properties of polynomial ideals:

I. The sum of two ideals is an ideal.
II. The intersection of arbitrarily many ideals is an ideal.

The **principal ideal** generated by $d \in F[x]$ is the set $dF[x]$, which is easily verified to be an ideal. Similarly, the ideal $d_1F[x] + \cdots + d_nF[x]$ is called the **principal ideal** generated by $d_1, \ldots, d_n \in F[x]$.

Theorem 2. *Every nonzero polynomial ideal $M \preccurlyeq F[x]$ is generated by a unique monic polynomial $d \in F[x]$; that is, $M = dF[x]$ for some monic d.*

(1) Let $d \in M$ be a nonzero monic polynomial of smallest degree in M.
   (a) $\underline{dF[x] \subseteq M}$, because M is an ideal and $d \in M$.
   (b) $\underline{M \subseteq dF[x]}$. Pretend $f \in M$ is not a multiple of d. Dividing f by d gives $f = dq + r$ where $dq, r \in M$ and $\deg r < \deg d$, which contradicts minimality of d! Hence $r = 0$.
(2) For uniqueness, suppose $M = d_1F[x] = d_2F[x]$ for monic $d_1, d_2 \in F[x]$.
   (a) Then $d_1p = d_2$ and $d_2q = d_1$ for some $p, q \in F[x]$.
   (b) Since $d_1 = d_2q = d_1pq$, polynomials p and q must be scalars.
   (c) Both d_1 and d_2 are monic, so $p = q = 1$, thus $d_1 = d_2$. □

Corollary 3. *If $p_1, \ldots, p_n \in F[x]$ are polynomials, not all zero, over field F, then there is a unique monic polynomial $d \in F[x]$, called the **greatest common divisor**, such that*

I. *d belongs to the ideal generated by $p_1, \ldots, p_n$*
II. *d divides each of the polynomials $p_1, \ldots, p_n$*

Any polynomial with the above two properties further satisfies:

III. *d is divisible by every polynomial which divides each $p_1, \ldots, p_n$*

Proof. The monic generator d of the ideal $M = p_1F[x] + \cdots + p_nF[x]$ immediately satisfies the first two properties. Since $d \in M$, we have

$$d = p_1g_1 + \cdots p_ng_n \qquad \text{for some } g_1, \ldots, g_n \in F[x]$$

Therefore, any $f \in F[x]$ dividing each polynomial $p_1, \ldots, p_n$ must also divide d. For uniqueness, observe that any $d' \in M$ satisfying the first two properties must divide d; but d is monic with minimal degree, so $d' = d$. □

Prime Factorization of Polynomials

Definition 5. A polynomial $f \in F[x]$ over field F is **reducible** over F if it can be written as the product of two non-scalar polynomials. Otherwise, f is called **irreducible**. A non-scalar irreducible polynomial is called **prime**.

Definition 6. Polynomials $p_1, \dots, p_n \in F[x]$ over field F are **relatively prime** if their greatest common divisor is 1, or equivalently, if they generate all of $F[x]$.

Theorem 3. (Euclid's Lemma) *If polynomial $p \in F[x]$ is prime and divides a product $f_1 f_2 \cdots f_n$, then p divides one of the factors $f_1, \dots, f_n \in F[x]$.*

Proof. By induction, it suffices to consider only two factors $p \mid fg$. Assume without loss of generality that p is monic, so that the only monic divisors of p are 1 and p itself. If $\text{GCD}(f, p)$ equals p, then $p \mid f$ and we are done. Otherwise, f and p are relatively prime and generate all of $F[x]$. So, there are polynomials $f_0, p_0 \in F[x]$ such that $1 = f_0 f + p_0 p$. Multiplying by g gives $g = (fg) f_0 + p(p_0 g)$. Therefore, $p \mid g$. □

Theorem 4. (Prime Factorization) *Every non-scalar monic polynomial can be factored uniquely as the product of monic primes, up to permutations.*

(1) Existence. Polynomials of degree one are prime. By induction on the degree, each $f \in F[x]$ of degree larger than one is either prime or can be expressed as the product of polynomials $g, h \in F[x]$ of lower degree, each with a prime factorization.

(2) Uniqueness. Assume $p_1 \cdots p_m = q_1 \cdots q_n$, with each $p_i, q_j \in F[x]$ prime, and $m \leq n$. By Euclid's lemma, $p_1 = q_j$ for some $j \in [n]$; assume $p_1 = q_1$. Dividing by this term and repeating the argument demonstrates that $p_k = q_k$ for all $k \in [\min\{m, n\}]$. The product of any leftover terms is one, so they cannot be prime. Hence $m = n$ and the factorizations are equal. □

EXERCISE 4. Let $f \in F[x]$ be a non-scalar monic polynomial over field F with prime factorization $f = p_1^{r_1} \cdots p_n^{r_n}$. Then the polynomials $f_k = f / p_k^{r_k}$ for $k \in [n]$ are relatively prime.

EXERCISE 5. Let $f \in F[x]$ be a polynomial over the field F with derivative $f' \in F[x]$. Then f is a product of distinct irreducible polynomials over F if and only if f and f' are relatively prime.

Definition 7. The field F is called **algebraically closed** if every prime polynomial over F has degree one.

References

[1] Kenneth Hoffman and Ray Kunze. *Linear Algebra*. Prentice Hall, second edition, 1971.