Basic Algebra

Final Version, August, 2006
For Publication by Birkhäuser Boston
Along with a Companion Volume *Advanced Algebra*
In the Series

Cornerstones

Selected Pages from Chapter I: pp. 1–15

Anthony W. Knapp

CHAPTER I

Preliminaries about the Integers, Polynomials, and Matrices

Abstract. This chapter is mostly a review, discussing unique factorization of positive integers, unique factorization of polynomials whose coefficients are rational or real or complex, signs of permutations, and matrix algebra.

Sections 1–2 concern unique factorization of positive integers. Section 1 proves the division and Euclidean algorithms, used to compute greatest common divisors. Section 2 establishes unique factorization as a consequence and gives several number-theoretic consequences, including the Chinese Remainder Theorem and the evaluation of the Euler φ function.

Section 3 develops unique factorization of rational and real and complex polynomials in one indeterminate completely analogously, and it derives the complete factorization of complex polynomials from the Fundamental Theorem of Algebra. The proof of the fundamental theorem is postponed to Chapter IX.

Section 4 discusses permutations of a finite set, establishing the decomposition of each permutation as a disjoint product of cycles. The sign of a permutation is introduced, and it is proved that the sign of a product is the product of the signs.

Sections 5–6 concern matrix algebra. Section 5 reviews row reduction and its role in the solution of simultaneous linear equations. Section 6 defines the arithmetic operations of addition, scalar multiplication, and multiplication of matrices. The process of matrix inversion is related to the method of row reduction, and it is shown that a square matrix with a one-sided inverse automatically has a two-sided inverse that is computable via row reduction.

1. Division and Euclidean Algorithms

The first three sections give a careful proof of unique factorization for integers and for polynomials with rational or real or complex coefficients, and they give an indication of some first consequences of this factorization. For the moment let us restrict attention to the set $\mathbb{Z}$ of integers. We take addition, subtraction, and multiplication within $\mathbb{Z}$ as established, as well as the properties of the usual ordering in $\mathbb{Z}$.

A **factor** of an integer n is a nonzero integer k such that $n = kl$ for some integer l. In this case we say also that k **divides** n, that k is a **divisor** of n, and that n is a **multiple** of k. We write $k \mid n$ for this relationship. If n is nonzero, any product formula $n = kl_1 \cdots l_r$ is a **factorization** of n. A **unit** in $\mathbb{Z}$ is a divisor

of 1, hence is either $+1$ or -1. The factorization $n = kl$ of $n \neq 0$ is called **nontrivial** if neither k nor l is a unit. An integer $p > 1$ is said to be **prime** if it has no nontrivial factorization $p = kl$.

The statement of unique factorization for positive integers, which will be given precisely in Section 2, says roughly that each positive integer is the product of primes and that this decomposition is unique apart from the order of the factors.[1] Existence will follow by an easy induction. The difficulty is in the uniqueness. We shall prove uniqueness by a sequence of steps based on the "Euclidean algorithm," which we discuss in a moment. In turn, the Euclidean algorithm relies on the following.

Proposition 1.1 (division algorithm). If a and b are integers with $b \neq 0$, then there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < |b|$.

PROOF. Possibly replacing q by $-q$, we may assume that $b > 0$. The integers n with $bn \leq a$ are bounded above by $|a|$, and there exists such an n, namely $n = -|a|$. Therefore there is a largest such integer, say $n = q$. Set $r = a - bq$. Then $0 \leq r$ and $a = bq + r$. If $r \geq b$, then $r - b \geq 0$ says that $a = b(q + 1) + (r - b) \geq b(q + 1)$. The inequality $q + 1 > q$ contradicts the maximality of q, and we conclude that $r < b$. This proves existence.

For uniqueness when $b > 0$, suppose $a = bq_1 + r_1 = bq_2 + r_2$. Subtracting, we obtain $b(q_1 - q_2) = r_2 - r_1$ with $|r_2 - r_1| < b$, and this is a contradiction unless $r_2 - r_1 = 0$. □

Let a and b be integers not both 0. The **greatest common divisor** of a and b is the largest integer $d > 0$ such that $d \mid a$ and $d \mid b$. Let us see existence. The integer 1 divides a and b. If b, for example, is nonzero, then any such d has $|d| \leq |b|$, and hence the greatest common divisor indeed exists. We write $d = \mathrm{GCD}(a, b)$.

Let us suppose that $b \neq 0$. The **Euclidean algorithm** consists of iterated application of the division algorithm (Proposition 1.1) to a and b until the remainder term r disappears:

$$\begin{aligned}
a &= bq_1 + r_1, && 0 \leq r_1 < b,\\
b &= r_1q_2 + r_2, && 0 \leq r_2 < r_1,\\
r_1 &= r_2q_3 + r_3, && 0 \leq r_3 < r_2,\\
&\vdots\\
r_{n-2} &= r_{n-1}q_n + r_n, && 0 \leq r_n < r_{n-1} \quad (\text{with } r_n \neq 0, \text{ say}),\\
r_{n-1} &= r_nq_{n+1}.
\end{aligned}$$

[1] It is to be understood that the prime factorization of 1 is as the empty product.

The process must stop with some remainder term r_{n+1} equal to 0 in this way since $b > r_1 > r_2 > \cdots \geq 0$. The last nonzero remainder term, namely r_n above, will be of interest to us.

EXAMPLE. For $a = 13$ and $b = 5$, the steps read

$$\begin{aligned} 13 &= 5 \cdot 2 + 3, \\ 5 &= 3 \cdot 1 + 2, \\ 3 &= 2 \cdot 1 + \boxed{1}, \\ 2 &= 1 \cdot 2. \end{aligned}$$

The last nonzero remainder term is written with a box around it.

Proposition 1.2. Let a and b be integers with $b \neq 0$, and let $d = \mathrm{GCD}(a, b)$. Then

(a) the number r_n in the Euclidean algorithm is exactly d,
(b) any divisor d' of both a and b necessarily divides d,
(c) there exist integers x and y such that $ax + by = d$.

EXAMPLE, CONTINUED. We rewrite the steps of the Euclidean algorithm, as applied in the above example with $a = 13$ and $b = 5$, so as to yield successive substitutions:

$$\begin{aligned} 13 &= 5 \cdot 2 + 3, & 3 &= 13 - 5 \cdot 2, \\ 5 &= 3 \cdot 1 + 2, & 2 &= 5 - 3 \cdot 1 = 5 - (13 - 5 \cdot 2) \cdot 1 = 5 \cdot 3 - 13 \cdot 1, \\ 3 &= 2 \cdot 1 + \boxed{1}, & 1 &= 3 - 2 \cdot 1 = (13 - 5 \cdot 2) - (5 \cdot 3 - 13 \cdot 1) \cdot 1 \\ & & &= 13 \cdot 2 - 5 \cdot 5. \end{aligned}$$

Thus we see that $1 = 13x + 5y$ with $x = 2$ and $y = -5$. This shows for the example that the number r_n works in place of d in Proposition 1.2c, and the rest of the proof of the proposition for this example is quite easy. Let us now adjust this computation to obtain a complete proof of the proposition in general.

PROOF OF PROPOSITION 1.2. Put $r_0 = b$ and $r_{-1} = a$, so that

$$r_{k-2} = r_{k-1}q_k + r_k \qquad \text{for } 1 \leq k \leq n. \tag{$*$}$$

The argument proceeds in three steps.

Step 1. We show that r_n is a divisor of both a and b. In fact, from $r_{n-1} = r_n q_{n+1}$, we have $r_n \mid r_{n-1}$. Let $k \leq n$, and assume inductively that r_n divides

$r_{k-1}, \dots, r_{n-1}, r_n$. Then $(*)$ shows that r_n divides r_{k-2}. Induction allows us to conclude that r_n divides $r_{-1}, r_0, \dots, r_{n-1}$. In particular, r_n divides a and b.

Step 2. We prove that $ax + by = r_n$ for suitable integers x and y. In fact, we show by induction on k for $k \le n$ that there exist integers x and y with $ax + by = r_k$. For $k = -1$ and $k = 0$, this conclusion is trivial. If $k \ge 1$ is given and if the result is known for $k - 2$ and $k - 1$, then we have

$$\begin{aligned} ax_2 + by_2 &= r_{k-2}, \\ ax_1 + by_1 &= r_{k-1} \end{aligned} \tag{$**$}$$

for suitable integers x_2, y_2, x_1, y_1. We multiply the second of the equalities of $(**)$ by q_k, subtract, and substitute into $(*)$. The result is

$$r_k = r_{k-2} - r_{k-1}q_k = a(x_2 - q_k x_1) + b(y_2 - q_k y_1),$$

and the induction is complete. Thus $ax + by = r_n$ for suitable x and y.

Step 3. Finally we deduce (a), (b), and (c). Step 1 shows that r_n divides a and b. If $d' > 0$ divides both a and b, the result of Step 2 shows that $d' \mid r_n$. Thus $d' \le r_n$, and r_n is the greatest common divisor. This is the conclusion of (a); (b) follows from (a) since $d' \mid r_n$, and (c) follows from (a) and Step 2. □

Corollary 1.3. Within $\mathbb{Z}$, if c is a nonzero integer that divides a product mn and if $\mathrm{GCD}(c, m) = 1$, then c divides n.

PROOF. Proposition 1.2c produces integers x and y with $cx + my = 1$. Multiplying by n, we obtain $cnx + mny = n$. Since c divides mn and divides itself, c divides both terms on the left side. Therefore it divides the right side, which is n. □

Corollary 1.4. Within $\mathbb{Z}$, if a and b are nonzero integers with $\mathrm{GCD}(a, b) = 1$ and if both of them divide the integer m, then ab divides m.

PROOF. Proposition 1.2c produces integers x and y with $ax + by = 1$. Multiplying by m, we obtain $amx + bmy = m$, which we rewrite in integers as $ab(m/b)x + ab(m/a)y = m$. Since ab divides each term on the left side, it divides the right side, which is m. □

2. Unique Factorization of Integers

We come now to the theorem asserting unique factorization for the integers. The precise statement is as follows.

Theorem 1.5 (Fundamental Theorem of Arithmetic). Each positive integer n can be written as a product of primes, $n = p_1 p_2 \cdots p_r$, with the integer 1 being written as an empty product. This factorization is unique in the following sense: if $n = q_1 q_2 \cdots q_s$ is another such factorization, then $r = s$ and, after some reordering of the factors, $q_j = p_j$ for $1 \le j \le r$.

The main step is the following lemma, which relies on Corollary 1.3.

Lemma 1.6. Within $\mathbb{Z}$, if p is a prime and p divides a product ab, then p divides a or p divides b.

PROOF. Suppose that p does not divide a. Since p is prime, $\mathrm{GCD}(a, p) = 1$. Taking $m = a$, $n = b$, and $c = p$ in Corollary 1.3, we see that p divides b. □

PROOF OF EXISTENCE IN THEOREM 1.5. We induct on n, the case $n = 1$ being handled by an empty product expansion. If the result holds for $k = 1$ through $k = n - 1$, there are two cases: n is prime and n is not prime. If n is prime, then $n = n$ is the desired factorization. Otherwise we can write $n = ab$ nontrivially with $a > 1$ and $b > 1$. Then $a \le n - 1$ and $b \le n - 1$, so that a and b have factorizations into primes by the inductive hypothesis. Putting them together yields a factorization into primes for $n = ab$. □

PROOF OF UNIQUENESS IN THEOREM 1.5. Suppose that $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ with all factors prime and with $r \le s$. We prove the uniqueness by induction on r, the case $r = 0$ being trivial and the case $r = 1$ following from the definition of "prime." Inductively from Lemma 1.6 we have $p_r \mid q_k$ for some k. Since q_k is prime, $p_r = q_k$. Thus we can cancel and obtain $p_1 p_2 \cdots p_{r-1} = q_1 q_2 \cdots \widehat{q_k} \cdots q_s$, the hat indicating an omitted factor. By induction the factors on the two sides here are the same except for order. Thus the same conclusion is valid when comparing the two sides of the equality $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$. The induction is complete, and the desired uniqueness follows. □

In the product expansion of Theorem 1.5, it is customary to group factors that are equal, thus writing the positive integer n as $n = p_1^{k_1} \cdots p_r^{k_r}$ with the primes p_j distinct and with the integers k_j all ≥ 0. This kind of decomposition is unique up to order if all factors $p_j^{k_j}$ with $k_j = 0$ are dropped, and we call it a **prime factorization** of n.

Corollary 1.7. If $n = p_1^{k_1} \cdots p_r^{k_r}$ is a prime factorization of a positive integer n, then the positive divisors d of n are exactly all products $d = p_1^{l_1} \cdots p_r^{l_r}$ with $0 \le l_j \le k_j$ for all j.

REMARK. A general divisor of n within $\mathbb{Z}$ is the product of a unit ± 1 and a positive divisor.

PROOF. Certainly any such product divides n. Conversely if d divides n, write $n = dx$ for some positive integer x. Apply Theorem 1.5 to d and to x, form the resulting prime factorizations, and multiply them together. Then we see from the uniqueness for the prime factorization of n that the only primes that can occur in the expansions of d and x are $p_1, \dots, p_r$ and that the sum of the exponents of p_j in the expansions of d and x is k_j. The result follows. □

If we want to compare prime factorizations for two positive integers, we can insert 0^{th} powers of primes as necessary and thereby assume that the same primes appear in both expansions. Using this device, we obtain a formula for greatest common divisors.

Corollary 1.8. If two positive integers a and b have expansions as products of powers of r distinct primes given by $a = p_1^{k_1} \cdots p_r^{k_r}$ and $b = p_1^{l_1} \cdots p_r^{l_r}$, then

$$\mathrm{GCD}(a, b) = p_1^{\min(k_1, l_1)} \cdots p_r^{\min(k_r, l_r)}.$$

PROOF. Let d' be the right side of the displayed equation. It is plain that d' is positive and that d' divides a and b. On the other hand, two applications of Corollary 1.7 show that the greatest common divisor of a and b is a number d of the form $p_1^{m_1} \cdots p_r^{m_r}$ with the property that $m_j \le k_j$ and $m_j \le l_j$ for all j. Therefore $m_j \le \min(k_j, l_j)$ for all j, and $d \le d'$. Since any positive divisor of both a and b is $\le d$, we have $d' \le d$. Thus $d' = d$. □

In special cases Corollary 1.8 provides a useful way to compute $\mathrm{GCD}(a, b)$, but the Euclidean algorithm is usually a more efficient procedure. Nevertheless, Corollary 1.8 remains a handy tool for theoretical purposes. Here is an example: Two nonzero integers a and b are said to be **relatively prime** if $\mathrm{GCD}(a, b) = 1$. It is immediate from Corollary 1.8 that two nonzero integers a and b are relatively prime if and only if there is no prime p that divides both a and b.

Corollary 1.9 (Chinese Remainder Theorem). Let a and b be positive relatively prime integers. To each pair (r, s) of integers with $0 \le r < a$ and $0 \le s < b$ corresponds a unique integer n such that $0 \le n < ab$, a divides $n - r$, and b divides $n - s$. Moreover, every integer n with $0 \le n < ab$ arises from some such pair (r, s).

REMARK. In notation for congruences that we introduce formally in Chapter IV, the result says that if $\mathrm{GCD}(a, b) = 1$, then the congruences $n \equiv r \bmod a$ and $n \equiv s \bmod b$ have one and only one simultaneous solution n with $0 \le n < ab$.

PROOF. Let us see that n exists as asserted. Since a and b are relatively prime, Proposition 1.2c produces integers x' and y' such that $ax' - by' = 1$. Multiplying by $s - r$, we obtain $ax - by = s - r$ for suitable integers x and y. Put $n' = ax + r = by + s$, and write by the division algorithm (Proposition 1.1) $n' = abq + n$ for some integer q and for some integer n with $0 \le n < ab$. Then $n - r = n' - abq - r = ax - abq$ is divisible by a, and similarly $n - s$ is divisible by b.

Suppose that n and n' both have the asserted properties. Then a divides $n - n' = (n - r) - (n' - r)$, and b divides $n - n' = (n - s) - (n' - s)$. Since a and b are relatively prime, Corollary 1.4 shows that ab divides $n - n'$. But $|n - n'| < ab$, and the only integer N with $|N| < ab$ that is divisible by ab is $N = 0$. Thus $n - n' = 0$ and $n = n'$. This proves uniqueness.

Finally the argument just given defines a one-one function from a set of ab pairs (r, s) to a set of ab elements n. Its image must therefore be all such integers n. This proves the corollary. □

If n is a positive integer, we define $\varphi(n)$ to be the number of integers k with $0 \le k < n$ such that k and n are relatively prime. The function φ is called the **Euler φ function**.

Corollary 1.10. Let $N > 1$ be an integer, and let $N = p_1^{k_1} \cdots p_r^{k_r}$ be a prime factorization of N. Then

$$\varphi(N) = \prod_{j=1}^{r} p_j^{k_j - 1}(p_j - 1).$$

REMARK. The conclusion is valid also for $N = 1$ if we interpret the right side of the formula to be the empty product.

PROOF. For positive integers a and b, let us check that

$$\varphi(ab) = \varphi(a)\varphi(b) \qquad \text{if} \quad \mathrm{GCD}(a, b) = 1. \tag{$*$}$$

In view of Corollary 1.9, it is enough to prove that the mapping $(r, s) \mapsto n$ given in that corollary has the property that $\mathrm{GCD}(r, a) = \mathrm{GCD}(s, b) = 1$ if and only if $\mathrm{GCD}(n, ab) = 1$.

To see this property, suppose that n satisfies $0 \le n < ab$ and $\mathrm{GCD}(n, ab) > 1$. Choose a prime p dividing both n and ab. By Lemma 1.6, p divides a or p divides b. By symmetry we may assume that p divides a. If (r, s) is the pair corresponding to n under Corollary 1.9, then the corollary says that a divides $n - r$. Since p divides a, p divides $n - r$. Since p divides n, p divides r. Thus $\mathrm{GCD}(r, a) > 1$.

Conversely suppose that (r, s) is a pair with $0 \le r < a$ and $0 \le s < b$ such that $\mathrm{GCD}(r, a) = \mathrm{GCD}(s, b) = 1$ is false. Without loss of generality, we may

assume that $\mathrm{GCD}(r, a) > 1$. Choose a prime p dividing both r and a. If n is the integer with $0 \le n < ab$ that corresponds to (r, s) under Corollary 1.9, then the corollary says that a divides $n - r$. Since p divides a, p divides $n - r$. Since p divides r, p divides n. Thus $\mathrm{GCD}(n, ab) > 1$. This completes the proof of $(*)$.

For a power p^k of a prime p with $k > 0$, the integers n with $0 \le n < p^k$ such that $\mathrm{GCD}(n, p^k) > 1$ are the multiples of p, namely $0, p, 2p, \ldots, p^k - p$. There are p^{k-1} of them. Thus the number of integers n with $0 \le n < p^k$ such that $\mathrm{GCD}(n, p^k) = 1$ is $p^k - p^{k-1} = p^{k-1}(p-1)$. In other words,

$$\varphi(p^k) = p^{k-1}(p-1) \qquad \text{if } p \text{ is prime and } k \ge 1. \tag{$**$}$$

To prove the corollary, we induct on r, the case $r = 1$ being handled by $(**)$. If the formula of the corollary is valid for $r - 1$, then $(*)$ allows us to combine that result with the formula for $\varphi(p^{k_r})$ given in $(**)$ to obtain the formula for $\varphi(N)$. □

We conclude this section by extending the notion of greatest common divisor to apply to more than two integers. If $a_1, \ldots, a_t$ are integers not all 0, their **greatest common divisor** is the largest integer $d > 0$ that divides all of $a_1, \ldots, a_t$. This exists, and we write $d = \mathrm{GCD}(a_1, \ldots, a_t)$ for it. It is immediate that d equals the greatest common divisor of the nonzero members of the set $\{a_1, \ldots, a_t\}$. Thus, in deriving properties of greatest common divisors, we may assume that all the integers are nonzero.

Corollary 1.11. Let $a_1, \ldots, a_t$ be positive integers, and let d be their greatest common divisor. Then

(a) if for each j with $1 \le j \le t$, $a_j = p_1^{k_{1,j}} \cdots p_r^{k_{r,j}}$ is an expansion of a_j as a product of powers of r distinct primes $p_1, \ldots, p_r$, it follows that

$$d = p_1^{\min_{1 \le j \le r}\{k_{1,j}\}} \cdots p_r^{\min_{1 \le j \le r}\{k_{r,j}\}},$$

(b) any divisor d' of all of $a_1, \ldots, a_t$ necessarily divides d,

(c) $d = \mathrm{GCD}\big(\mathrm{GCD}(a_1, \ldots, a_{t-1}), a_t\big)$ if $t > 1$,

(d) there exist integers $x_1, \ldots, x_t$ such that $a_1x_1 + \cdots + a_tx_t = d$.

PROOF. Part (a) is proved in the same way as Corollary 1.8 except that Corollary 1.7 is to be applied r times rather than just twice. Further application of Corollary 1.7 shows that any positive divisor d' of $a_1, \ldots, a_t$ is of the form $d' = p_1^{m_1} \cdots p_r^{m_r}$ with $m_1 \le k_{1,j}$ for all $j, \ldots$, and with $m_r \le k_{r,j}$ for all j. Therefore $m_1 \le \min_{1 \le j \le r}\{k_{1,j}\}, \ldots$, and $m_r \le \min_{1 \le j \le r}\{k_{r,j}\}$, and it follows that d' divides d. This proves (b). Conclusion (c) follows by using the formula in (a), and (d) follows by combining (c), Proposition 1.2c, and induction. □

3. Unique Factorization of Polynomials

This section establishes unique factorization for ordinary rational, real, and complex polynomials. We write $\mathbb{Q}$ for the set of rational numbers, $\mathbb{R}$ for the set of real numbers, and $\mathbb{C}$ for the set of complex numbers, each with its arithmetic operations. The rational numbers are constructed from the integers by a process reviewed in Section A3 of the appendix, the real numbers are defined from the rational numbers by a process reviewed in that same section, and the complex numbers are defined from the real numbers by a process reviewed in Section A4 of the appendix. Sections A3 and A4 of the appendix mention special properties of $\mathbb{R}$ and $\mathbb{C}$ beyond those of the arithmetic operations, but we shall not make serious use of these special properties here until nearly the end of the section—after unique factorization of polynomials has been established. Let $\mathbb{F}$ denote any of $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. The members of $\mathbb{F}$ are called **scalars**.

We work with ordinary polynomials with coefficients in $\mathbb{F}$. Informally these are expressions $P(X) = a_n X^n + \cdots + a_1 X + a_0$ with $a_n, \ldots, a_1, a_0$ in $\mathbb{F}$. Although it is tempting to think of $P(X)$ as a function with independent variable X, it is better to identify P with the sequence $(a_0, a_1, \ldots, a_n, 0, 0, \ldots)$ of coefficients, using expressions $P(X) = a_n X^n + \cdots + a_1 X + a_0$ only for conciseness and for motivation of the definitions of various operations.

The precise definition therefore is that a **polynomial** in **one indeterminate** with **coefficients** in $\mathbb{F}$ is an infinite sequence of members of $\mathbb{F}$ such that all terms of the sequence are 0 from some point on. The indexing of the sequence is to begin with 0. We may refer to a polynomial P as $P(X)$ if we want to emphasize that the indeterminate is called X. Addition, subtraction, and scalar multiplication are defined in coordinate-by-coordinate fashion:

$$\begin{aligned}
&(a_0, a_1, \ldots, a_n, 0, 0, \ldots) + (b_0, b_1, \ldots, b_n, 0, 0, \ldots) \\
&\qquad = (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, 0, 0, \ldots), \\
&(a_0, a_1, \ldots, a_n, 0, 0, \ldots) - (b_0, b_1, \ldots, b_n, 0, 0, \ldots) \\
&\qquad = (a_0 - b_0, a_1 - b_1, \ldots, a_n - b_n, 0, 0, \ldots), \\
&c(a_0, a_1, \ldots, a_n, 0, 0, \ldots) = (ca_0, ca_1, \ldots, ca_n, 0, 0, \ldots).
\end{aligned}$$

Polynomial multiplication is defined so as to match multiplication of expressions $a_n X^n + \cdots + a_1 X + a_0$ if the product is expanded out, powers of X are added, and then terms containing like powers of X are collected:

$$(a_0, a_1, \ldots, 0, 0, \ldots)(b_0, b_1, \ldots, 0, 0, \ldots) = (c_0, c_1, \ldots, 0, 0, \ldots),$$

where $c_N = \sum_{k=0}^{N} a_k b_{N-k}$. We take it as known that the usual associative, commutative, and distributive laws are then valid. The set of all polynomials in the indeterminate X is denoted by $\mathbb{F}[X]$.

The polynomial with all entries 0 is denoted by 0 and is called the **zero polynomial**. For all polynomials $P = (a_0, \dots, a_n, 0, \dots)$ other than 0, the **degree** of P, denoted by $\deg P$, is defined to be the largest index n such that $a_n \neq 0$. The **constant polynomials** are by definition the zero polynomial and the polynomials of degree 0. If P and Q are nonzero polynomials, then

$$\begin{aligned} P + Q = 0 \qquad \text{or} \qquad & \deg(P + Q) \leq \max(\deg P, \deg Q), \\ & \deg(cP) = \deg P, \\ & \deg(PQ) = \deg P + \deg Q. \end{aligned}$$

In the formula for $\deg(P + Q)$, equality holds if $\deg P \neq \deg Q$. Implicit in the formula for $\deg(PQ)$ is the fact that PQ cannot be 0 unless $P = 0$ or $Q = 0$. A cancellation law for multiplication is an immediate consequence:

$$PR = QR \text{ with } R \neq 0 \qquad \text{implies} \qquad P = Q.$$

In fact, $PR = QR$ implies $(P - Q)R = 0$; since $R \neq 0$, $P - Q$ must be 0.

If $P = (a_0, \dots, a_n, 0, \dots)$ is a polynomial and r is in $\mathbb{F}$, we can **evaluate** P at r, obtaining as a result the number $P(r) = a_n r^n + \cdots + a_1 r + a_0$. Taking into account all values of r, we obtain a mapping $P \mapsto P(\,\cdot\,)$ of $\mathbb{F}[X]$ into the set of functions from $\mathbb{F}$ into $\mathbb{F}$. Because of the way that the arithmetic operations on polynomials have been defined, we have

$$\begin{aligned} (P + Q)(r) &= P(r) + Q(r), \\ (P - Q)(r) &= P(r) - Q(r), \\ (cP)(r) &= cP(r), \\ (PQ)(r) &= P(r)Q(r). \end{aligned}$$

In other words, the mapping $P \mapsto P(\,\cdot\,)$ respects the arithmetic operations. We say that r is a **root** of P if $P(r) = 0$.

Now we turn to the question of unique factorization. The definitions and the proof are completely analogous to those for the integers. A **factor** of a polynomial A is a nonzero polynomial B such that $A = BQ$ for some polynomial Q. In this case we say also that B **divides** A, that B is a **divisor** of A, and that A is a **multiple** of B. We write $B \mid A$ for this relationship. If A is nonzero, any product formula $A = BQ_1 \cdots Q_r$ is a **factorization** of A. A **unit** in $\mathbb{F}[X]$ is a divisor of 1, hence is any polynomial of degree 0; such a polynomial is a constant polynomial $A(X) = c$ with c equal to a nonzero scalar. The factorization $A = BQ$ of $A \neq 0$ is called **nontrivial** if neither B nor Q is a unit. A **prime** P in $\mathbb{F}[X]$ is a nonzero polynomial that is not a unit and has no nontrivial factorization $P = BQ$. Observe that the product of a prime and a unit is always a prime.

Proposition 1.12 (division algorithm). If A and B are polynomials in $\mathbb{F}[X]$ and if B not the 0 polynomial, then there exist unique polynomials Q and R in $\mathbb{F}[X]$ such that

(a) $A = BQ + R$ and
(b) either R is the 0 polynomial or $\deg R < \deg B$.

REMARK. This result codifies the usual method of dividing polynomials in high-school algebra. That method writes $A/B = Q + R/B$, and then one obtains the above result by multiplying by B. The polynomial Q is the quotient in the division, and R is the remainder.

PROOF OF UNIQUENESS. If $A = BQ + R = BQ_1 + R_1$, then $B(Q - Q_1) = R_1 - R$. Without loss of generality, $R_1 - R$ is not the 0 polynomial since otherwise $Q - Q_1 = 0$ also. Then

$$\deg B + \deg(Q - Q_1) = \deg(R_1 - R) \leq \max(\deg R, \deg R_1) < \deg B,$$

and we have a contradiction. □

PROOF OF EXISTENCE. If $A = 0$ or $\deg A < \deg B$, we take $Q = 0$ and $R = A$, and we are done. Otherwise we induct on $\deg A$. Assume the result for degree $\leq n - 1$, and let $\deg A = n$. Write $A = a_n X^n + A_1$ with $A_1 = 0$ or $\deg A_1 < \deg A$. Let $B = b_k X^k + B_1$ with $B_1 = 0$ or $\deg B_1 < \deg B$. Put $Q_1 = a_n b_k^{-1} X^{n-k}$. Then

$$A - BQ_1 = a_n X^n + A_1 - a_n X^n - a_n b_k^{-1} X^{n-k} B_1 = A_1 - a_n b_k^{-1} X^{n-k} B_1$$

with the right side equal to 0 or of degree $< \deg A$. Then the right side, by induction, is of the form $BQ_2 + R$, and $A = B(Q_1 + Q_2) + R$ is the required decomposition. □

Corollary 1.13 (Factor Theorem). If r is in $\mathbb{F}$ and if P is a polynomial in $\mathbb{F}[X]$, then $X - r$ divides P if and only if $P(r) = 0$.

PROOF. If $P = (X - r)Q$, then $P(r) = (r - r)Q(r) = 0$. Conversely let $P(r) = 0$. Taking $B(X) = X - r$ in the division algorithm (Proposition 1.12), we obtain $P = (X - r)Q + R$ with $R = 0$ or $\deg R < \deg(X - r) = 1$. Thus R is a constant polynomial, possibly 0. In any case we have $0 = P(r) = (r - r)Q(r) + R(r)$, and thus $R(r) = 0$. Since R is constant, we must have $R = 0$, and then $P = (X - r)Q$. □

Corollary 1.14. If P is a nonzero polynomial with coefficients in $\mathbb{F}$ and if $\deg P = n$, then P has at most n distinct roots.

REMARKS. Since there are infinitely many scalars in any of $\mathbb{Q}$ and $\mathbb{R}$ and $\mathbb{C}$, the corollary implies that the function from $\mathbb{F}$ to $\mathbb{F}$ associated to P, namely $r \mapsto P(r)$, cannot be identically 0 if $P \neq 0$. Starting in Chapter IV, we shall allow other $\mathbb{F}$'s besides $\mathbb{Q}$ and $\mathbb{R}$ and $\mathbb{C}$, and then this implication can fail. For example, when $\mathbb{F}$ is the two-element "field" $\mathbb{F} = \{0, 1\}$ with $1 + 1 = 0$ and with otherwise the expected addition and multiplication, then $P(X) = X^2 + X$ is not the zero polynomial but $P(r) = 0$ for $r = 0$ and $r = 1$. It is thus important to distinguish polynomials in one indeterminate from their associated functions of one variable.

PROOF. Let $r_1, \dots, r_{n+1}$ be distinct roots of $P(X)$. By the Factor Theorem (Corollary 1.13), $X - r_1$ is a factor of $P(X)$. We prove inductively on k that the product $(X - r_1)(X - r_2) \cdots (X - r_k)$ is a factor of $P(X)$. Assume that this assertion holds for k, so that $P(X) = (X - r_1) \cdots (X - r_k)Q(X)$ and

$$0 = P(r_{k+1}) = (r_{k+1} - r_1) \cdots (r_{k+1} - r_k)Q(r_{k+1}).$$

Since the r_j's are distinct, we must have $Q(r_{k+1}) = 0$. By the Factor Theorem, we can write $Q(X) = (X - r_{k+1})R(X)$ for some polynomial $R(X)$. Substitution gives $P(X) = (X - r_1) \cdots (X - r_k)(X - r_{k+1})R(X)$, and $(X - r_1) \cdots (X - r_{k+1})$ is exhibited as a factor of $P(X)$. This completes the induction. Consequently

$$P(X) = (X - r_1) \cdots (X - r_{n+1})S(X)$$

for some polynomial $S(X)$. Comparing the degrees of the two sides, we find that $\deg S = -1$, and we have a contradiction. □

We can use the division algorithm in the same way as with the integers in Sections 1–2 to obtain unique factorization. Within the set of integers, we defined greatest common divisors so as to be positive, but their negatives would have worked equally well. That flexibility persists with polynomials; the essential feature of any greatest common divisor of polynomials is shared by any product of that polynomial by a unit. A **greatest common divisor** of polynomials A and B with $B \neq 0$ is any polynomial D of maximum degree such that D divides A and D divides B. We shall see that D is indeed unique up to multiplication by a nonzero scalar.[2]

[2]For some purposes it is helpful to isolate one particular greatest common divisor by taking the coefficient of the highest power of X to be 1.

The **Euclidean algorithm** is the iterative process that makes use of the division algorithm in the form

$$\begin{aligned}
A &= BQ_1 + R_1, && R_1 = 0 \text{ or } \deg R_1 < \deg B,\\
B &= R_1Q_2 + R_2, && R_2 = 0 \text{ or } \deg R_2 < \deg R_1,\\
R_1 &= R_2Q_3 + R_3, && R_3 = 0 \text{ or } \deg R_3 < \deg R_2,\\
&\vdots\\
R_{n-2} &= R_{n-1}Q_n + R_n, && R_n = 0 \text{ or } \deg R_n < \deg R_{n-1},\\
R_{n-1} &= R_nQ_{n+1}.
\end{aligned}$$

In the above computation the integer n is defined by the conditions that $R_n \neq 0$ and that $R_{n+1} = 0$. Such an n must exist since $\deg B > \deg R_1 > \cdots \geq 0$. We can now obtain an analog for $\mathbb{F}[X]$ of the result for $\mathbb{Z}$ given as Proposition 1.2.

Proposition 1.15. Let A and B be polynomials in $\mathbb{F}[X]$ with $B \neq 0$, and let $R_1, \ldots, R_n$ be the remainders generated by the Euclidean algorithm when applied to A and B. Then

(a) R_n is a greatest common divisor of A and B,
(b) any D_1 that divides both A and B necessarily divides R_n,
(c) the greatest common divisor of A and B is unique up to multiplication by a nonzero scalar,
(d) any greatest common divisor D has the property that there exist polynomials P and Q with $AP + BQ = D$.

PROOF. Conclusions (a) and (b) are proved in the same way that parts (a) and (b) of Proposition 1.2 are proved, and conclusion (d) is proved with $D = R_n$ in the same way that Proposition 1.2c is proved.

If D is a greatest common divisor of A and B, it follows from (a) and (b) that D divides R_n and that $\deg D = \deg R_n$. This proves (c). □

Using Proposition 1.15, we can prove analogs for $\mathbb{F}[X]$ of the two corollaries of Proposition 1.2. But let us instead skip directly to what is needed to obtain an analog for $\mathbb{F}[X]$ of unique factorization as in Theorem 1.5.

Lemma 1.16. If A and B are nonzero polynomials with coefficients in $\mathbb{F}$ and if P is a prime polynomial such that P divides AB, then P divides A or P divides B.

PROOF. If P does not divide A, then 1 is a greatest common divisor of A and P, and Proposition 1.15d produces polynomials S and T such that $AS + PT = 1$. Multiplication by B gives $ABS + PTB = B$. Then P divides ABS because it divides AB, and P divides PTB because it divides P. Hence P divides B. □

Theorem 1.17 (unique factorization). Every member of $\mathbb{F}[X]$ of degree ≥ 1 is a product of primes. This factorization is unique up to order and up to multiplication of each prime factor by a unit, i.e., by a nonzero scalar.

PROOF. The existence follows in the same way as the existence in Theorem 1.5; induction on the integers is to be replaced by induction on the degree. The uniqueness follows from Lemma 1.16 in the same way that the uniqueness in Theorem 1.5 follows from Lemma 1.6. □

We turn to a consideration of properties of polynomials that take into account special features of $\mathbb{R}$ and $\mathbb{C}$. If $\mathbb{F}$ is $\mathbb{R}$, then $X^2 + 1$ is prime. The reason is that a nontrivial factorization of $X^2 + 1$ would have to involve two first-degree real polynomials and then $r^2 + 1$ would have to be 0 for some real r, namely for r equal to the root of either of the first-degree polynomials. On the other hand, $X^2 + 1$ is not prime when $\mathbb{F} = \mathbb{C}$ since $X^2 + 1 = (X + i)(X - i)$. The Fundamental Theorem of Algebra, stated below, implies that every prime polynomial over $\mathbb{C}$ is of degree 1. It is possible to prove the Fundamental Theorem of Algebra within complex analysis as a consequence of Liouville's Theorem or within real analysis as a consequence of the Heine–Borel Theorem and other facts about compactness. This text gives a proof of the Fundamental Theorem of Algebra in Chapter IX using modern algebra, specifically Sylow theory as in Chapter IV and Galois theory as in Chapter IX. One further fact is needed; this fact uses elementary calculus and is proved below as Proposition 1.20.

Theorem 1.18 (Fundamental Theorem of Algebra). Any polynomial in $\mathbb{C}[X]$ with degree ≥ 1 has at least one root.

Corollary 1.19. Let P be a nonzero polynomial of degree n in $\mathbb{C}[X]$, and let $r_1, \ldots, r_k$ be the distinct roots. Then there exist unique integers $m_j > 0$ for $1 \leq j \leq k$ such that $P(X)$ is a scalar multiple of $\prod_{j=1}^{k} (X - r_j)^{m_j}$. The numbers m_j have $\sum_{j=1}^{k} m_j = n$.

PROOF. We may assume that $\deg P > 0$. We apply unique factorization (Theorem 1.17) to $P(X)$. It follows from the Fundamental Theorem of Algebra (Theorem 1.18) and the Factor Theorem (Corollary 1.13) that each prime polynomial with coefficients in $\mathbb{C}$ has degree 1. Thus the unique factorization of $P(X)$ has to be of the form $c \prod_{l=1}^{n} (X - z_l)$ for some $c \neq 0$ and for some complex numbers z_l that are unique up to order. The z_l's are roots, and every root is a z_l by the Factor Theorem. Grouping like factors proves the desired factorization and its uniqueness. The numbers m_j have $\sum_{j=1}^{k} m_j = n$ by a count of degrees. □

The integers m_j in the corollary are called the **multiplicities** of the roots of the polynomial $P(X)$.

We conclude this section by proving the result from calculus that will enter the proof of the Fundamental Theorem of Algebra in Chapter IX.

Proposition 1.20. Any polynomial in $\mathbb{R}[X]$ with odd degree has at least one root.

PROOF. Without loss of generality, we may take the leading coefficient to be 1. Thus let the polynomial be $P(X) = X^{2n+1} + a_{2n}X^{2n} + \cdots + a_1X + a_0 = X^{2n+1} + R(X)$. For $|r| \geq 1$, the polynomial R satisfies $|R(r)| \leq C|r|^{2n}$, where $C = |a_{2n}| + \cdots + |a_1| + |a_0|$. Thus $|r| > \max(C, 1)$ implies $|P(r) - r^{2n+1}| \leq C|r|^{2n} < |r|^{2n+1}$, and it follows that $P(r)$ has the same sign as r^{2n+1} for $|r| > \max(C, 1)$. For $r_0 = \max(C, 1) + 1$, we therefore have $P(-r_0) < 0$ and $P(r_0) > 0$. By the Intermediate Value Theorem, given in Section A3 of the appendix, $P(r) = 0$ for some r with $-r_0 \leq r \leq r_0$. □

4. Permutations and Their Signs

Let S be a finite nonempty set of n elements. A **permutation** of S is a one-one function from S onto S. The elements might be listed as $a_1, a_2, \ldots, a_n$, but it will simplify the notation to view them simply as $1, 2, \ldots, n$. We use ordinary function notation for describing the effect of permutations. Thus the value of a permutation σ at j is $\sigma(j)$, and the composition of τ followed by σ is $\sigma \circ \tau$ or simply $\sigma\tau$, with $(\sigma\tau)(j) = \sigma(\tau(j))$. Composition is automatically associative, i.e., $(\rho\sigma)\tau = \rho(\sigma\tau)$, because the effect of both sides on j, when we expand things out, is $\rho(\sigma(\tau(j)))$. The composition of two permutations is also called their **product**.

The identity permutation will be denoted by 1. Any permutation σ, being a one-one onto function, has a well-defined inverse permutation σ^{-1} with the property that $\sigma\sigma^{-1} = \sigma^{-1}\sigma = 1$. One way of describing concisely the effect of a permutation is to list its domain values and to put the corresponding range values beneath them. Thus $\sigma = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 4\,3\,5\,1\,2 \end{pmatrix}$ is the permutation of $\{1, 2, 3, 4, 5\}$ with $\sigma(1) = 4$, $\sigma(2) = 3$, $\sigma(3) = 5$, $\sigma(4) = 1$, and $\sigma(5) = 2$. The inverse permutation is obtained by interchanging the two rows to obtain $\begin{pmatrix} 4\,3\,5\,1\,2 \\ 1\,2\,3\,4\,5 \end{pmatrix}$ and then adjusting the entries in the rows so that the first row is in the usual order: $\sigma^{-1} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 4\,5\,2\,1\,3 \end{pmatrix}$.

If $2 \leq k \leq n$, a k-**cycle** is a permutation σ that fixes each element in some subset of $n - k$ elements and moves the remaining elements $c_1, \ldots, c_k$ according to $\sigma(c_1) = c_2$, $\sigma(c_2) = c_3, \ldots, \sigma(c_{k-1}) = c_k$, $\sigma(c_k) = c_1$. Such a cycle may be