plicative inverse, so that $(a+M)(r+M)=1+M$ for some $r \in R$. This implies $ar+m=1$ for some $m \in M$. Since J is an ideal, we have $1 \in J$ and therefore $(1)=R \subseteq J$, hence $J=R$. Thus M is a maximal ideal of R.

(ii) Let P be a prime ideal of R; then R/P is a commutative ring with identity $1+P \neq 0+P$. Let $(a+P)(b+P)=0+P$, hence $ab \in P$. Since P is a prime ideal, either $a \in P$ or $b \in P$; that is, either $a+P=0+P$ or $b+P=0+P$. Thus, R/P has no zero divisors and is therefore an integral domain. The converse follows immediately by reversing the steps of this proof.

(iii) This follows from (i) and (ii) since every field is an integral domain.

(iv) Let $c \in R$. If c is a unit, then $(c)=R$ and the ring $R/(c)$ consists only of one element and is no field. If c is neither a unit nor a prime element, then c has a divisor $a \in R$ that is neither a unit nor an associate of c. We note that $a \neq 0$, for if $a=0$, then $c=0$ and a would be an associate of c. We can write $c=ab$ with $b \in R$. Next we claim that $a \notin (c)$. For otherwise $a=cd=abd$ for some $d \in R$, or $a(1-bd)=0$. Since $a \neq 0$, this would imply $bd=1$, so that d would be a unit, which contradicts the fact that a is not an associate of c. It follows that $(c) \subseteq (a) \subseteq R$, where all containments are proper, and so $R/(c)$ cannot be a field because of (i). Finally, we are left with the case where c is a prime element. Then $(c) \neq R$ since c is no unit. Furthermore, if $J \supseteq (c)$ is an ideal of R, then $J=(a)$ for some $a \in R$ since R is a principal ideal domain. It follows that $c \in (a)$, and so a is a divisor of c. Consequently, a is either a unit or an associate of c, so that either $J=R$ or $J=(c)$. This shows that (c) is a maximal ideal of R. Hence $R/(c)$ is a field by (i). □

As an application of this theorem, let us consider the case $R=\mathbb{Z}$. We note that $\mathbb{Z}$ is a principal ideal domain since the additive subgroups of $\mathbb{Z}$ are already generated by a single element because of Theorem 1.15(i). A prime number p fits the definition of a prime element, and so Theorem 1.47(iv) yields another proof of the known result that $\mathbb{Z}/(p)$ is a field. Consequently, (p) is a maximal ideal and a prime ideal of $\mathbb{Z}$. For a composite integer n, the ideal (n) is not a prime ideal of $\mathbb{Z}$, and so $\mathbb{Z}/(n)$ is not even an integral domain. Other applications will follow in the next section when we consider residue class rings of polynomial rings over fields.

3. POLYNOMIALS

In elementary algebra one regards a polynomial as an expression of the form $a_0+a_1x+\cdots+a_nx^n$. The a_i's are called coefficients and are usually real or complex numbers; x is viewed as a variable: that is, substituting an arbitrary number α for x, a well-defined number $a_0 + a_1\alpha + \cdots + a_n\alpha^n$ is obtained. The arithmetic of polynomials is governed by familiar rules. The concept of polynomial and the associated operations can be generalized to a formal algebraic setting in a straightforward manner.

Let R be an arbitrary ring. A *polynomial* over R is an expression of the form

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n,$$

where n is a nonnegative integer, the *coefficients* a_i, $0 \leqslant i \leqslant n$, are elements of R, and x is a symbol not belonging to R, called an *indeterminate* over R. Whenever it is clear which indeterminate is meant, we can use f as a designation for the polynomial $f(x)$. We adopt the convention that a term $a_i x^i$ with $a_i = 0$ need not be written down. In particular, the polynomial $f(x)$ above may then also be given in the equivalent form $f(x) = a_0 + a_1 x + \cdots + a_n x^n + 0x^{n+1} + \cdots + 0x^{n+h}$, where h is any positive integer. When comparing two polynomials $f(x)$ and $g(x)$ over R, it is therefore possible to assume that they both involve the same powers of x. The polynomials

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad \text{and} \quad g(x) = \sum_{i=0}^{n} b_i x^i$$

over R are considered equal if and only if $a_i = b_i$ for $0 \leqslant i \leqslant n$. We define the *sum* of $f(x)$ and $g(x)$ by

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

To define the *product* of two polynomials over R, let

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad \text{and} \quad g(x) = \sum_{j=0}^{m} b_j x^j$$

and set

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k, \quad \text{where } c_k = \sum_{\substack{i+j=k \\ 0 \leqslant i \leqslant n,\, 0 \leqslant j \leqslant m}} a_i b_j.$$

It is easily seen that with these operations the set of polynomials over R forms a ring.

1.48. Definition. The ring formed by the polynomials over R with the above operations is called the *polynomial ring* over R and denoted by $R[x]$.

The zero element of $R[x]$ is the polynomial all of whose coefficients are 0. This polynomial is called the *zero polynomial* and denoted by 0. It should always be clear from the context whether 0 stands for the zero element of R or the zero polynomial.

1.49. Definition. Let $f(x)=\sum_{i=0}^{n}a_ix^i$ be a polynomial over R that is not the zero polynomial, so that we can suppose $a_n \neq 0$. Then a_n is called the *leading coefficient* of $f(x)$ and a_0 the *constant term*, while n is called the *degree* of $f(x)$, in symbols $n=\deg(f(x))=\deg(f)$. By convention, we set $\deg(0)=-\infty$. Polynomials of degree $\leqslant 0$ are called *constant polynomials*. If R has the identity 1 and if the leading coefficient of $f(x)$ is 1, then $f(x)$ is called a *monic polynomial.*

By computing the leading coefficient of the sum and the product of two polynomials, one finds the following result.

1.50. ***Theorem.*** *Let $f, g \in R[x]$. Then*

$$\deg(f+g) \leqslant \max(\deg(f),\deg(g)),$$
$$\deg(fg) \leqslant \deg(f)+\deg(g).$$

If R is an integral domain, we have

$$\deg(fg)=\deg(f)+\deg(g). \tag{1.4}$$

If one identifies constant polynomials with elements of R, then R can be viewed as a subring of $R[x]$. Certain properties of R are inherited by $R[x]$. The essential step in the proof of part (iii) of the subsequent theorem depends on (1.4).

1.51. ***Theorem.*** *Let R be a ring. Then:*

(i) *$R[x]$ is commutative if and only if R is commutative.*
(ii) *$R[x]$ is a ring with identity if and only if R has an identity.*
(iii) *$R[x]$ is an integral domain if and only if R is an integral domain.*

In the following chapters we will deal almost exclusively with polynomials over fields. Let F denote a field (not necessarily finite). The concept of divisibility, when specialized to the ring $F[x]$, leads to the following. The polynomial $g \in F[x]$ *divides* the polynomial $f \in F[x]$ if there exists a polynomial $h \in F[x]$ such that $f=gh$. We also say that g is a *divisor* of f, or that f is a *multiple* of g, or that f is *divisible* by g. The units of $F[x]$ are the divisors of the constant polynomial 1, which are precisely all nonzero constant polynomials.

As for the ring of integers, there is a division with remainder in polynomial rings over fields.

1.52. ***Theorem*** (Division Algorithm). *Let $g \neq 0$ be a polynomial in $F[x]$. Then for any $f \in F[x]$ there exist polynomials q, $r \in F[x]$ such that*

$$f=qg+r, \quad \textit{where } \deg(r)<\deg(g).$$

1.53. Example. Consider $f(x)=2x^5+x^4+4x+3 \in \mathbb{F}_5[x]$, $g(x)=3x^2+1 \in \mathbb{F}_5[x]$. We compute the polynomials $q, r \in \mathbb{F}_5[x]$ with $f=qg+r$ by using long division:

$$\begin{array}{r|rrrrrr}
\multicolumn{1}{r}{} & & & 4x^3 & +2x^2 & +2x & +1 \\ \cline{2-7}
3x^2+1 & 2x^5 & +x^4 & & & +4x & +3 \\
\multicolumn{1}{r}{} & -2x^5 & & -4x^3 & & & \\ \cline{2-4}
\multicolumn{1}{r}{} & & x^4 & +x^3 & & & \\
\multicolumn{1}{r}{} & & -x^4 & & -2x^2 & & \\ \cline{3-5}
\multicolumn{1}{r}{} & & & x^3 & +3x^2 & +4x & \\
\multicolumn{1}{r}{} & & & -x^3 & & -2x & \\ \cline{4-6}
\multicolumn{1}{r}{} & & & & 3x^2 & +2x & +3 \\
\multicolumn{1}{r}{} & & & & -3x^2 & & -1 \\ \cline{5-7}
\multicolumn{1}{r}{} & & & & & 2x & +2
\end{array}$$

Thus $q(x) = 4x^3 + 2x^2 + 2x + 1$, $r(x) = 2x + 2$, and obviously $\deg(r) < \deg(g)$. □

The fact that $F[x]$ permits a division algorithm implies by a standard argument that every ideal of $F[x]$ is principal.

1.54. Theorem. *$F[x]$ is a principal ideal domain. In fact, for every ideal $J \neq (0)$ of $F[x]$ there exists a uniquely determined monic polynomial $g \in F[x]$ with $J = (g)$.*

Proof. $F[x]$ is an integral domain by Theorem 1.51(iii). Suppose $J \neq (0)$ is an ideal of $F[x]$. Let $h(x)$ be a nonzero polynomial of least degree contained in J, let b be the leading coefficient of $h(x)$, and set $g(x) = b^{-1}h(x)$. Then $g \in J$ and g is monic. If $f \in J$ is arbitrary, the division algorithm yields $q, r \in F[x]$ with $f = qg + r$ and $\deg(r) < \deg(g) = \deg(h)$. Since J is an ideal, we get $f - qg = r \in J$, and by the definition of h we must have $r = 0$. Therefore, f is a multiple of g, and so $J = (g)$. If $g_1 \in F[x]$ is another monic polynomial with $J = (g_1)$, then $g = c_1 g_1$ and $g_1 = c_2 g$ with $c_1, c_2 \in F[x]$. This implies $g = c_1 c_2 g$, hence $c_1 c_2 = 1$, and c_1 and c_2 are constant polynomials. Since both g and g_1 are monic, it follows that $g = g_1$, and the uniqueness of g is established. □

1.55. Theorem. *Let $f_1, \ldots, f_n$ be polynomials in $F[x]$ not all of which are 0. Then there exists a uniquely determined monic polynomial $d \in F[x]$ with the following properties: (i) d divides each f_j, $1 \leqslant j \leqslant n$; (ii) any polynomial $c \in F[x]$ dividing each f_j, $1 \leqslant j \leqslant n$, divides d. Moreover, d can be expressed in the form*

$$d = b_1 f_1 + \cdots + b_n f_n \quad \textit{with } b_1, \ldots, b_n \in F[x]. \tag{1.5}$$

Proof. The set J consisting of all polynomials of the form $c_1 f_1 + \cdots + c_n f_n$ with $c_1, \ldots, c_n \in F[x]$ is easily seen to be an ideal of $F[x]$. Since not all f_j are 0, we have $J \neq (0)$, and Theorem 1.54 implies that $J = (d)$

for some monic polynomial $d \in F[x]$. Property (i) and the representation (1.5) follow immediately from the construction of d. Property (ii) follows from (1.5). If d_1 is another monic polynomial in $F[x]$ satisfying (i) and (ii), then these properties imply that d and d_1 are divisible by each other, and so $(d)=(d_1)$. An application of the uniqueness part of Theorem 1.54 yields $d=d_1$. □

The monic polynomial d appearing in the theorem above is called the *greatest common divisor* of $f_1,\dots,f_n$, in symbols $d=\gcd(f_1,\dots,f_n)$. If $\gcd(f_1,\dots,f_n)=1$, then the polynomials $f_1,\dots,f_n$ are said to be *relatively prime*. They are called *pairwise relatively prime* if $\gcd(f_i,f_j)=1$ for $1 \leqslant i < j \leqslant n$.

The greatest common divisor of two polynomials $f, g \in F[x]$ can be computed by the *Euclidean algorithm*. Suppose, without loss of generality, that $g \neq 0$ and that g does not divide f. Then we repeatedly use the division algorithm in the following manner:

$$\begin{aligned}
f &= q_1 g + r_1 & 0 &\leqslant \deg(r_1) < \deg(g)\\
g &= q_2 r_1 + r_2 & 0 &\leqslant \deg(r_2) < \deg(r_1)\\
r_1 &= q_3 r_2 + r_3 & 0 &\leqslant \deg(r_3) < \deg(r_2)\\
&\vdots & &\vdots\\
r_{s-2} &= q_s r_{s-1} + r_s & 0 &\leqslant \deg(r_s) < \deg(r_{s-1})\\
r_{s-1} &= q_{s+1} r_s.
\end{aligned}$$

Here $q_1,\dots,q_{s+1}$ and $r_1,\dots,r_s$ are polynomials in $F[x]$. Since $\deg(g)$ is finite, the procedure must stop after finitely many steps. If the last nonzero remainder r_s has leading coefficient b, then $\gcd(f,g)=b^{-1}r_s$. In order to find $\gcd(f_1,\dots,f_n)$ for $n>2$ and nonzero polynomials f_i, one first computes $\gcd(f_1,f_2)$, then $\gcd(\gcd(f_1,f_2),f_3)$, and so on, by the Euclidean algorithm.

1.56. Example. The Euclidean algorithm applied to

$$f(x)=2x^6+x^3+x^2+2 \in \mathbb{F}_3[x], \qquad g(x)=x^4+x^2+2x \in \mathbb{F}_3[x]$$

yields:

$$\begin{aligned}
2x^6+x^3+x^2+2 &= (2x^2+1)(x^4+x^2+2x)+x+2\\
x^4+x^2+2x &= (x^3+x^2+2x+1)(x+2)+1\\
x+2 &= (x+2)1.
\end{aligned}$$

Therefore $\gcd(f,g)=1$ and f and g are relatively prime. □

A counterpart to the notion of greatest common divisor is that of least common multiple. Let $f_1,\dots,f_n$ be nonzero polynomials in $F[x]$. Then one shows (see Exercise 1.25) that there exists a uniquely determined monic polynomial $m \in F[x]$ with the following properties: (i) m is a multiple of each f_j, $1 \leqslant j \leqslant n$; (ii) any polynomial $b \in F[x]$ that is a multiple of each f_j, $1 \leqslant j \leqslant n$, is a multiple of m. The polynomial m is called the *least common multiple* of $f_1, \ldots, f_n$ and denoted by $m = \operatorname{lcm}(f_1, \ldots, f_n)$. For two nonzero polynomials $f, g \in F[x]$ we have

$$a^{-1}fg = \operatorname{lcm}(f, g)\gcd(f, g), \tag{1.6}$$

where a is the leading coefficient of fg. This relation conveniently reduces the calculation of $\operatorname{lcm}(f, g)$ to that of $\gcd(f, g)$. There is no direct analog of (1.6) for three or more polynomials. In this case, one uses the identity $\operatorname{lcm}(f_1, \ldots, f_n) = \operatorname{lcm}(\operatorname{lcm}(f_1, \ldots, f_{n-1}), f_n)$ to compute the least common multiple.

The prime elements of the ring $F[x]$ are usually called irreducible polynomials. To emphasize this important concept, we give the definition again for the present context.

1.57. Definition. A polynomial $p \in F[x]$ is said to be *irreducible over* F (or *irreducible in* $F[x]$, or *prime in* $F[x]$) if p has positive degree and $p = bc$ with $b, c \in F[x]$ implies that either b or c is a constant polynomial.

Briefly stated, a polynomial of positive degree is irreducible over F if it allows only trivial factorizations. A polynomial in $F[x]$ of positive degree that is not irreducible over F is called *reducible over* F. The reducibility or irreducibility of a given polynomial depends heavily on the field under consideration. For instance, the polynomial $x^2 - 2 \in \mathbb{Q}[x]$ is irreducible over the field $\mathbb{Q}$ of rational numbers, but $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$ is reducible over the field of real numbers.

Irreducible polynomials are of fundamental importance for the structure of the ring $F[x]$ since the polynomials in $F[x]$ can be written as products of irreducible polynomials in an essentially unique manner. For the proof we need the following result.

1.58. Lemma. *If an irreducible polynomial p in $F[x]$ divides a product $f_1 \cdots f_m$ of polynomials in $F[x]$, then at least one of the factors f_j is divisible by p.*

Proof. Since p divides $f_1 \cdots f_m$, we get the identity $(f_1 + (p)) \cdots (f_m + (p)) = 0 + (p)$ in the factor ring $F[x]/(p)$. Now $F[x]/(p)$ is a field by Theorem 1.47(iv), and so $f_j + (p) = 0 + (p)$ for some j; that is, p divides f_j. □

1.59. Theorem (Unique Factorization in $F[x]$). *Any polynomial $f \in F[x]$ of positive degree can be written in the form*

$$f = ap_1^{e_1} \cdots p_k^{e_k}, \tag{1.7}$$

where $a \in F$, $p_1, \ldots, p_k$ are distinct monic irreducible polynomials in $F[x]$, and $e_1, \ldots, e_k$ are positive integers. Moreover, this factorization is unique apart from the order in which the factors occur.

Proof. The fact that any nonconstant $f \in F[x]$ can be represented in the form (1.7) is shown by induction on the degree of f. The case $\deg(f) = 1$ is trivial since any polynomial in $F[x]$ of degree 1 is irreducible over F. Now suppose the desired factorization is established for all nonconstant polynomials in $F[x]$ of degree $< n$. If $\deg(f) = n$ and f is irreducible over F, then we are done since we can write $f = a(a^{-1}f)$, where a is the leading coefficient of f and $a^{-1}f$ is a monic irreducible polynomial in $F[x]$. Otherwise, f allows a factorization $f = gh$ with $1 \leqslant \deg(g) < n$, $1 \leqslant \deg(h) < n$, and $g, h \in F[x]$. By the induction hypothesis, g and h can be factored in the form (1.7), and so f can be factored in this form.

To prove uniqueness, suppose f has two factorizations of the form (1.7), say

$$f = ap_1^{e_1} \cdots p_k^{e_k} = bq_1^{d_1} \cdots q_r^{d_r}. \tag{1.8}$$

By comparing leading coefficients, we get $a = b$. Furthermore, the irreducible polynomial p_1 in $F[x]$ divides the right-hand side of (1.8), and so Lemma 1.58 shows that p_1 divides q_j for some $j, 1 \leqslant j \leqslant r$. But q_j is also irreducible in $F[x]$, so that we must have $q_j = cp_1$ with a constant polynomial c. Since q_j and p_1 are both monic, it follows that $q_j = p_1$. Thus we can cancel p_1 against q_j in (1.8) and continue in the same manner with the remaining identity. After finitely many steps of this type, we obtain that the two factorizations are identical apart from the order of the factors. □

We shall refer to (1.7) as the *canonical factorization* of the polynomial f in $F[x]$. If $F = \mathbb{Q}$, there is a method due to Kronecker for finding the canonical factorization of a polynomial in finitely many steps. This method is briefly described in Exercise 1.30. For polynomials over finite fields, factorization algorithms will be discussed in Chapter 4.

A central question about polynomials in $F[x]$ is to decide whether a given polynomial is irreducible or reducible over F. For our purposes, irreducible polynomials over $\mathbb{F}_p$ are of particular interest. To determine all monic irreducible polynomials over $\mathbb{F}_p$ of fixed degree n, one may first compute all monic reducible polynomials over $\mathbb{F}_p$ of degree n and then eliminate them from the set of monic polynomials in $\mathbb{F}_p[x]$ of degree n. If p or n is large, this method is not feasible, and we will develop more powerful methods in Chapter 3, Sections 2 and 3.

1.60. Example. Find all irreducible polynomials over $\mathbb{F}_2$ of degree 4 (note that a nonzero polynomial in $\mathbb{F}_2[x]$ is automatically monic). There are $2^4 = 16$ polynomials in $\mathbb{F}_2[x]$ of degree 4. Such a polynomial is reducible over $\mathbb{F}_2$ if and only if it has a divisor of degree 1 or 2. Therefore, we compute all products $(a_0 + a_1x + a_2x^2 + x^3)(b_0 + x)$ and $(a_0 + a_1x + x^2)(b_0 + b_1x + x^2)$ with $a_i, b_j \in \mathbb{F}_2$ and obtain all reducible polynomials over $\mathbb{F}_2$ of degree 4. Comparison with the 16 polynomials of degree 4 leaves us with the irreducible polynomials $f_1(x) = x^4 + x + 1$, $f_2(x) = x^4 + x^3 + 1$, $f_3(x) = x^4 + x^3 + x^2 + x + 1$ in $\mathbb{F}_2[x]$. □

Since the irreducible polynomials over a field F are exactly the prime elements of $F[x]$, the following result, one part of which was already used in Lemma 1.58, is an immediate consequence of Theorems 1.47(iv) and 1.54.

1.61. Theorem. *For $f \in F[x]$, the residue class ring $F[x]/(f)$ is a field if and only if f is irreducible over F.*

As a preparation for the next section, we shall take a closer look at the structure of the residue class ring $F[x]/(f)$, where f is an arbitrary nonzero polynomial in $F[x]$. We recall that as a residue class ring $F[x]/(f)$ consists of residue classes $g + (f)$ (also denoted by $[g]$) with $g \in F[x]$, where the operations are defined as in (1.2) and (1.3). Two residue classes $g + (f)$ and $h + (f)$ are identical precisely if $g \equiv h \bmod f$—that is, precisely if $g - h$ is divisible by f. This is equivalent to the requirement that g and h leave the same remainder after division by f. Each residue class $g + (f)$ contains a unique representative $r \in F[x]$ with $\deg(r) < \deg(f)$, which is simply the remainder in the division of g by f. The process of passing from g to r is called *reduction* mod f. The uniqueness of r follows from the observation that if $r_1 \in g + (f)$ with $\deg(r_1) < \deg(f)$, then $r - r_1$ is divisible by f and $\deg(r - r_1) < \deg(f)$, which is only possible if $r = r_1$. The distinct residue classes comprising $F[x]/(f)$ can now be described explicitly; namely, they are exactly the residue classes $r + (f)$, where r runs through all polynomials in $F[x]$ with $\deg(r) < \deg(f)$. Thus, if $F = \mathbb{F}_p$ and $\deg(f) = n \geqslant 0$, then the number of elements of $\mathbb{F}_p[x]/(f)$ is equal to the number of polynomials in $\mathbb{F}_p[x]$ of degree $< n$, which is p^n.

1.62. Examples

(i) Let $f(x) = x \in \mathbb{F}_2[x]$. The $p^n = 2^1$ polynomials in $\mathbb{F}_2[x]$ of degree < 1 determine all residue classes comprising $\mathbb{F}_2[x]/(x)$. Thus, $\mathbb{F}_2[x]/(x)$ consists of the residue classes $[0]$ and $[1]$ and is isomorphic to $\mathbb{F}_2$.

(ii) Let $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. Then $\mathbb{F}_2[x]/(f)$ has the $p^n = 2^2$ elements $[0]$, $[1]$, $[x]$, $[x + 1]$. The operation tables for this residue class ring are obtained by performing the required operations with the polynomials determining the residue classes and by carrying out reduction mod f if necessary:

$+$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[1]$	$[1]$	$[0]$	$[x+1]$	$[x]$
$[x]$	$[x]$	$[x+1]$	$[0]$	$[1]$
$[x+1]$	$[x+1]$	$[x]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[x]$	$[0]$	$[x]$	$[x+1]$	$[1]$
$[x+1]$	$[0]$	$[x+1]$	$[1]$	$[x]$

By inspecting these tables, or from the irreducibility of f over $\mathbb{F}_2$ and Theorem 1.61, it follows that $\mathbb{F}_2[x]/(f)$ is a field. This is our first example of a finite field for which the number of elements is not a prime.

(iii) Let $f(x) = x^2 + 2 \in \mathbb{F}_3[x]$. Then $\mathbb{F}_3[x]/(f)$ consists of the $p^n = 3^2$ residue classes $[0]$, $[1]$, $[2]$, $[x]$, $[x+1]$, $[x+2]$, $[2x]$, $[2x+1]$, $[2x+2]$. The operation tables for $\mathbb{F}_3[x]/(f)$ are again produced by performing polynomial operations and using reduction mod f whenever necessary. Since $\mathbb{F}_3[x]/(f)$ is a commutative ring, we only have to compute the entries on and above the main diagonal.

$+$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[0]$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[1]$		$[2]$	$[0]$	$[x+1]$	$[x+2]$	$[x]$	$[2x+1]$	$[2x+2]$	$[2x]$
$[2]$			$[1]$	$[x+2]$	$[x]$	$[x+1]$	$[2x+2]$	$[2x]$	$[2x+1]$
$[x]$				$[2x]$	$[2x+1]$	$[2x+2]$	$[0]$	$[1]$	$[2]$
$[x+1]$					$[2x+2]$	$[2x]$	$[1]$	$[2]$	$[0]$
$[x+2]$						$[2x+1]$	$[2]$	$[0]$	$[1]$
$[2x]$							$[x]$	$[x+1]$	$[x+2]$
$[2x+1]$								$[x+2]$	$[x]$
$[2x+2]$									$[x+1]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$		$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[2]$			$[1]$	$[2x]$	$[2x+2]$	$[2x+1]$	$[x]$	$[x+2]$	$[x+1]$
$[x]$				$[1]$	$[x+1]$	$[2x+1]$	$[2]$	$[x+2]$	$[2x+2]$
$[x+1]$					$[2x+2]$	$[0]$	$[2x+2]$	$[0]$	$[x+1]$
$[x+2]$						$[x+2]$	$[x+2]$	$[2x+1]$	$[0]$
$[2x]$							$[1]$	$[2x+1]$	$[x+1]$
$[2x+1]$								$[x+2]$	$[0]$
$[2x+2]$									$[2x+2]$

Note that $\mathbb{F}_3[x]/(f)$ is not a field (and not even an integral domain). This is in accordance with Theorem 1.61 since $x^2+2 = (x+1)(x+2)$ is reducible over $\mathbb{F}_3$. □

If F is again an arbitrary field and $f(x) \in F[x]$, then replacement of the indeterminate x in $f(x)$ by a fixed element of F yields a well-defined element of F. In detail, if $f(x)=a_0+a_1x+\cdots+a_nx^n\in F[x]$ and $b\in F$, then replacing x by b we get $f(b)=a_0+a_1b+\cdots+a_nb^n\in F$. In any polynomial identity in $F[x]$ we can substitute a fixed $b\in F$ for x and obtain a valid identity in F (*principle of substitution*).

1.63. Definition. An element $b\in F$ is called a *root* (or a *zero*) of the polynomial $f\in F[x]$ if $f(b)=0$.

An important connection between roots and divisibility is given by the following theorem.

1.64. Theorem. *An element $b\in F$ is a root of the polynomial $f\in F[x]$ if and only if $x-b$ divides $f(x)$.*

Proof. We use the division algorithm (see Theorem 1.52) to write $f(x)=q(x)(x-b)+c$ with $q\in F[x]$ and $c\in F$. Substituting b for x, we get $f(b)=c$, hence $f(x)=q(x)(x-b)+f(b)$. The theorem follows now from this identity. □

1.65. Definition. Let $b\in F$ be a root of the polynomial $f\in F[x]$. If k is a positive integer such that $f(x)$ is divisible by $(x-b)^k$, but not by $(x-b)^{k+1}$, then k is called the *multiplicity* of b. If $k=1$, then b is called a *simple root* (or a *simple zero*) of f, and if $k\geqslant 2$, then b is called a *multiple root* (or a *multiple zero*) of f.

1.66. Theorem. *Let $f\in F[x]$ with $\deg f=n\geqslant 0$. If $b_1,\ldots,b_m\in F$ are distinct roots of f with multiplicities $k_1,\ldots,k_m$, respectively, then $(x-b_1)^{k_1}\cdots(x-b_m)^{k_m}$ divides $f(x)$. Consequently, $k_1+\cdots+k_m\leqslant n$, and f can have at most n distinct roots in F.*

Proof. We note that each polynomial $x-b_j$, $1\leqslant j\leqslant m$, is irreducible over F, and so $(x-b_j)^{k_j}$ occurs as a factor in the canonical factorization of f. Altogether, the factor $(x-b_1)^{k_1}\cdots(x-b_m)^{k_m}$ appears in the canonical factorization of f and is thus a divisor of f. By comparing degrees, we get $k_1+\cdots+k_m\leqslant n$, and $m\leqslant k_1+\cdots+k_m\leqslant n$ shows the last statement. □

1.67. Definition. If $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n\in F[x]$, then the *derivative* f' of f is defined by $f'=f'(x)=a_1+2a_2x+\cdots+na_nx^{n-1}\in F[x]$.

1.68. Theorem. *The element $b\in F$ is a multiple root of $f\in F[x]$ if and only if it is a root of both f and f'.*

There is a relation between the nonexistence of roots and irreducibility. If f is an irreducible polynomial in $F[x]$ of degree.$\geqslant 2$, then Theorem 1.64 shows that f has no root in F. The converse holds for polynomials of degree 2 or 3, but not necessarily for polynomials of higher degree.

1.69. Theorem. *The polynomial $f \in F[x]$ of degree 2 or 3 is irreducible in $F[x]$ if and only if f has no root in F.*

Proof. The necessity of the condition was already noted. Conversely, if f has no root in F and were reducible in $F[x]$, we could write $f = gh$ with $g, h \in F[x]$ and $1 \leqslant \deg(g) \leqslant \deg(h)$. But $\deg(g)+\deg(h) = \deg(f) \leqslant 3$, hence $\deg(g) = 1$; that is, $g(x) = ax + b$ with $a, b \in F$, $a \neq 0$. Then $-ba^{-1}$ is a root of g, and so a root of f in F, a contradiction. □

1.70. Example. Because of Theorem 1.69, the irreducible polynomials in $\mathbb{F}_2[x]$ of degree 2 or 3 can be obtained by eliminating the polynomials with roots in $\mathbb{F}_2$ from the set of all polynomials in $\mathbb{F}_2[x]$ of degree 2 or 3. The only irreducible polynomial in $\mathbb{F}_2[x]$ of degree 2 is $f(x) = x^2 + x + 1$, and the irreducible polynomials in $\mathbb{F}_2[x]$ of degree 3 are $f_1(x) = x^3 + x + 1$ and $f_2(x) = x^3 + x^2 + 1$. □

In elementary analysis there is a well-known method for constructing a polynomial with real coefficients which assumes certain assigned values for given values of the indeterminate. The same method carries over to any field.

1.71. Theorem (Lagrange Interpolation Formula). *For $n \geqslant 0$, let $a_0, \ldots, a_n$ be $n+1$ distinct elements of F, and let $b_0, \ldots, b_n$ be $n+1$ arbitrary elements of F. Then there exists exactly one polynomial $f \in F[x]$ of degree $\leqslant n$ such that $f(a_i) = b_i$ for $i = 0, \ldots, n$. This polynomial is given by*

$$f(x) = \sum_{i=0}^{n} b_i \prod_{\substack{k=0 \\ k \neq i}}^{n} (a_i - a_k)^{-1}(x - a_k).$$

One can also consider polynomials in several indeterminates. Let R denote a commutative ring with identity and let $x_1, \ldots, x_n$ be symbols that will serve as indeterminates. We form the polynomial ring $R[x_1]$, then the polynomial ring $R[x_1, x_2] = R[x_1][x_2]$, and so on, until we arrive at $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$. The elements of $R[x_1, \ldots, x_n]$ are then expressions of the form

$$f = f(x_1, \ldots, x_n) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$$

with coefficients $a_{i_1 \cdots i_n} \in R$, where the summation is extended over finitely many n-tuples $(i_1, \ldots, i_n)$ of nonnegative integers and the convention $x_j^0 = 1$ $(1 \leqslant j \leqslant n)$ is observed. Such an expression is called a *polynomial in* $x_1, \ldots, x_n$ over R. Two polynomials $f, g \in R[x_1, \ldots, x_n]$ are equal if and only if all corresponding coefficients are equal. It is tacitly assumed that the indeterminates $x_1, \ldots, x_n$ commute with each other, so that, for instance, the expressions $x_1x_2x_3x_4$ and $x_4x_1x_3x_2$ are identified.

1.72. Definition. Let $f \in R[x_1, \ldots, x_n]$ be given by

$$f(x_1, \ldots, x_n) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}.$$

If $a_{i_1\cdots i_n} \neq 0$, then $a_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}$ is called a *term* of f and $i_1 + \cdots + i_n$ is the degree of the term. For $f \neq 0$ one defines the *degree* of f, denoted by $\deg(f)$, to be the maximum of the degrees of the terms of f. For $f = 0$ one sets $\deg(f) = -\infty$. If $f = 0$ or if all terms of f have the same degree, then f is called *homogeneous*.

Any $f \in R[x_1,\ldots,x_n]$ can be written as a finite sum of homogeneous polynomials. The degrees of polynomials in $R[x_1,\ldots,x_n]$ satisfy again the inequalities in Theorem 1.50, and if R is an integral domain, then (1.4) is valid and $R[x_1,\ldots,x_n]$ is an integral domain. If F is a field, then the polynomials in $F[x_1,\ldots,x_n]$ of positive degree can again be factored uniquely into a constant factor and a product of "monic" prime elements (using a suitable definition of "monic"), but for $n \geqslant 2$ there is no analog of the division algorithm (in the case of commuting indeterminates) and $F[x_1,\ldots,x_n]$ is not a principal ideal domain.

An important special class of polynomials in n indeterminates is that of symmetric polynomials.

1.73. Definition. A polynomial $f \in R[x_1,\ldots,x_n]$ is called *symmetric* if $f(x_{i_1},\ldots,x_{i_n}) = f(x_1,\ldots,x_n)$ for any permutation $i_1,\ldots,i_n$ of the integers $1,\ldots,n$.

1.74. Example. Let z be an indeterminate over $R[x_1,\ldots,x_n]$, and let $g(z) = (z - x_1)(z - x_2)\cdots(z - x_n)$. Then

$$g(z) = z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} + \cdots + (-1)^n \sigma_n$$

with

$$\sigma_k = \sigma_k(x_1,\ldots,x_n) = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} x_{i_1}\cdots x_{i_k} \quad (k = 1,2,\ldots,n).$$

Thus:

$$\begin{aligned}
\sigma_1 &= x_1 + x_2 + \cdots + x_n,\\
\sigma_2 &= x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \cdots + x_{n-1}x_n,\\
&\vdots\\
\sigma_n &= x_1x_2\cdots x_n.
\end{aligned}$$

As g remains unaltered under any permutation of the x_i, all the σ_k are symmetric polynomials; they are also homogeneous. The polynomial $\sigma_k = \sigma_k(x_1,\ldots,x_n) \in R[x_1,\ldots,x_n]$ is called the kth *elementary symmetric polynomial* in the indeterminates $x_1,\ldots,x_n$ over R. The adjective "elementary" is used because of the so-called "fundamental theorem on symmetric polynomials," which states that for any symmetric polynomial $f \in R[x_1,\ldots,x_n]$ there exists a uniquely determined polynomial $h \in R[x_1,\ldots,x_n]$ such that $f(x_1,\ldots,x_n) = h(\sigma_1,\ldots,\sigma_n)$. □

1.75. Theorem (Newton's Formula). *Let $\sigma_1,\ldots,\sigma_n$ be the elementary symmetric polynomials in $x_1,\ldots,x_n$ over R, and let $s_0 = n \in \mathbb{Z}$ and*