of a finite number of polynomials, and in particular, provides an effective means for deciding when the polynomials are relatively prime.

Definition. *Let* F *be a field. A polynomial* f *in* F[x] *is said to be* **reducible over** F *if there exist polynomials* g, h *in* F[x] *of degree* ≥ 1 *such that* f = gh, *and if not,* f *is said to be* **irreducible over** F. *A non-scalar irreducible polynomial over* F *is called a* **prime polynomial over** F, *and we sometimes say it is a* **prime in** F[x].

EXAMPLE 10. The polynomial $x^2 + 1$ is reducible over the field C of complex numbers. For

$$x^2 + 1 = (x + i)(x - i)$$

and the polynomials $x + i$, $x - i$ belong to $C[x]$. On the other hand, $x^2 + 1$ is irreducible over the field R of real numbers. For if

$$x^2 + 1 = (ax + b)(a'x + b')$$

with a, a', b, b' in R, then

$$aa' = 1, \qquad ab' + ba' = 0, \qquad bb' = 1.$$

These relations imply $a^2 + b^2 = 0$, which is impossible with real numbers a and b, unless $a = b = 0$.

Theorem 8. *Let* p, f, *and* g *be polynomials over the field* F. *Suppose that* p *is a prime polynomial and that* p *divides the product* fg. *Then either* p *divides* f *or* p *divides* g.

Proof. It is no loss of generality to assume that p is a monic prime polynomial. The fact that p is prime then simply says that the only monic divisors of p are 1 and p. Let d be the g.c.d. of f and p. Then either $d = 1$ or $d = p$, since d is a monic polynomial which divides p. If $d = p$, then p divides f and we are done. So suppose $d = 1$, i.e., suppose f and p are relatively prime. We shall prove that p divides g. Since $(f, p) = 1$, there are polynomials f_0 and p_0 such that $1 = f_0f + p_0p$. Multiplying by g, we obtain

$$\begin{aligned} g &= f_0fg + p_0pg \\ &= (fg)f_0 + p(p_0g). \end{aligned}$$

Since p divides fg it divides $(fg)f_0$, and certainly p divides $p(p_0g)$. Thus p divides g. ▌

Corollary. *If* p *is a prime and divides a product* $\mathrm{f}_1 \cdots \mathrm{f}_n$, *then* p *divides one of the polynomials* $\mathrm{f}_1, \ldots, \mathrm{f}_n$.

Proof. The proof is by induction. When $n = 2$, the result is simply the statement of Theorem 6. Suppose we have proved the corollary for $n = k$, and that p divides the product $f_1 \cdots f_{k+1}$ of some $(k + 1)$ polynomials. Since p divides $(f_1 \cdots f_k)f_{k+1}$, either p divides f_{k+1} or p divides $f_1 \cdots f_k$. By the induction hypothesis, if p divides $f_1 \cdots f_k$, then p divides f_j for some j, $1 \leq j \leq k$. So we see that in any case p must divide some f_j, $1 \leq j \leq k + 1$. ▌

Theorem 9. *If* F *is a field, a non-scalar monic polynomial in* F[x] *can be factored as a product of monic primes in* F[x] *in one and, except for order, only one way.*

Proof. Suppose f is a non-scalar monic polynomial over F. As polynomials of degree one are irreducible, there is nothing to prove if $\deg f = 1$. Suppose f has degree $n > 1$. By induction we may assume the theorem is true for all non-scalar monic polynomials of degree less than n. If f is irreducible, it is already factored as a product of monic primes, and otherwise $f = gh$ where g and h are non-scalar monic polynomials of degree less than n. Thus g and h can be factored as products of monic primes in $F[x]$ and hence so can f. Now suppose

$$f = p_1 \cdots p_m = q_1 \cdots q_n$$

where $p_1, \ldots, p_m$ and $q_1, \ldots, q_n$ are monic primes in $F[x]$. Then p_m divides the product $q_1 \cdots q_n$. By the above corollary, p_m must divide some q_i. Since q_i and p_m are both monic primes, this means that

$$q_i = p_m. \tag{4-16}$$

From (4-16) we see that $m = n = 1$ if either $m = 1$ or $n = 1$. For

$$\deg f = \sum_{i=1}^{m} \deg p_i = \sum_{j=1}^{n} \deg q_j.$$

In this case there is nothing more to prove, so we may assume $m > 1$ and $n > 1$. By rearranging the q's we can then assume $p_m = q_n$, and that

$$p_1 \cdots p_{m-1}p_m = q_1 \cdots q_{n-1}p_m.$$

Now by Corollary 2 of Theorem 1 it follows that

$$p_1 \cdots p_{m-1} = q_1 \cdots q_{n-1}.$$

As the polynomial $p_1 \cdots p_{m-1}$ has degree less than n, our inductive assumption applies and shows that the sequence $q_1, \ldots, q_{n-1}$ is at most a rearrangement of the sequence $p_1, \ldots, p_{m-1}$. This together with (4-16) shows that the factorization of f as a product of monic primes is unique up to the order of the factors. ▌

In the above factorization of a given non-scalar monic polynomial f, some of the monic prime factors may be repeated. If $p_1, p_2, \ldots, p_r$ are the distinct monic primes occurring in this factorization of f, then

$$f = p_1^{n_1}p_2^{n_2} \cdots p_r^{n_r}, \tag{4-17}$$

the exponent n_i being the number of times the prime p_i occurs in the factorization. This decomposition is also clearly unique, and is called the **primary decomposition** of f. It is easily verified that every monic divisor of f has the form

$$p_1^{m_1}p_2^{m_2}\cdots p_r^{m_r}, \qquad 0 \le m_i \le n_i. \tag{4-18}$$

From (4-18) it follows that the g.c.d. of a finite number of non-scalar monic polynomials $f_1, \ldots, f_s$ is obtained by combining all those monic primes which occur simultaneously in the factorizations of $f_1, \ldots, f_s$. The exponent to which each prime is to be taken is the largest for which the corresponding prime power is a factor of each f_i. If no (non-trivial) prime power is a factor of each f_i, the polynomials are relatively prime.

EXAMPLE 11. Suppose F is a field, and let a, b, c be distinct elements of F. Then the polynomials $x - a$, $x - b$, $x - c$ are distinct monic primes in $F[x]$. If m, n, and s are positive integers, $(x - c)^s$ is the g.c.d. of the polynomials.

$$(x-b)^n(x-c)^s \quad \text{and} \quad (x-a)^m(x-c)^s$$

whereas the three polynomials

$$(x-b)^n(x-c)^s, \qquad (x-a)^m(x-c)^s, \qquad (x-a)^m(x-b)^n$$

are relatively prime.

Theorem 10. *Let* f *be a non-scalar monic polynomial over the field* F *and let*

$$\mathrm{f} = \mathrm{p}_1^{\mathrm{n}_1}\cdots \mathrm{p}_k^{\mathrm{n}_k}$$

be the prime factorization of f. *For each* j, $1 \le \mathrm{j} \le \mathrm{k}$, *let*

$$\mathrm{f}_j = \mathrm{f}/\mathrm{p}_j^{\mathrm{n}_j} = \prod_{i\neq j} \mathrm{p}_i^{\mathrm{n}_i}.$$

Then $\mathrm{f}_1, \ldots, \mathrm{f}_k$ *are relatively prime.*

Proof. We leave the (easy) proof of this to the reader. We have stated this theorem largely because we wish to refer to it later. ▌

Theorem 11. *Let* f *be a polynomial over the field* F *with derivative* f′. *Then* f *is a product of distinct irreducible polynomials over* F *if and only if* f *and* f′ *are relatively prime.*

Proof. Suppose in the prime factorization of f over the field F that some (non-scalar) prime polynomial p is repeated. Then $f = p^2h$ for some h in $F[x]$. Then

$$f' = p^2h' + 2pp'h$$

and p is also a divisor of f'. Hence f and f' are not relatively prime.

Now suppose $f = p_1 \cdots p_k$, where $p_1, \ldots, p_k$ are distinct non-scalar irreducible polynomials over F. Let $f_j = f/p_j$. Then

$$f' = p_1'f_1 + p_2'f_2 + \cdots + p_k'f_k.$$

Let p be a prime polynomial which divides both f and f'. Then $p = p_i$ for some i. Now p_i divides f_j for $j \neq i$, and since p_i also divides

$$f' = \sum_{j=1}^{k} p'_j f_j$$

we see that p_i must divide $p'_i f_i$. Therefore p_i divides either f_i or p'_i. But p_i does not divide f_i since $p_1, \ldots, p_k$ are distinct. So p_i divides p'_i. This is not possible, since p'_i has degree one less than the degree of p_i. We conclude that no prime divides both f and f', or that, f and f' are relatively prime. ▌

Definition. *The field* F *is called* **algebraically closed** *if every prime polynomial over* F *has degree* 1.

To say that F is algebraically closed means every non-scalar irreducible monic polynomial over F is of the form $(x - c)$. We have already observed that each such polynomial is irreducible for any F. Accordingly, an equivalent definition of an algebraically closed field is a field F such that each non-scalar polynomial f in $F[x]$ can be expressed in the form

$$f = c(x - c_1)^{n_1} \cdots (x - c_k)^{n_k}$$

where c is a scalar, $c_1, \ldots, c_k$ are distinct elements of F, and $n_1, \ldots, n_k$ are positive integers. Still another formulation is that if f is a non-scalar polynomial over F, then there is an element c in F such that $f(c) = 0$.

The field R of real numbers is not algebraically closed, since the polynomial $(x^2 + 1)$ is irreducible over R but not of degree 1, or, because there is no real number c such that $c^2 + 1 = 0$. The so-called Fundamental Theorem of Algebra states that the field C of complex numbers is algebraically closed. We shall not prove this theorem, although we shall use it somewhat later in this book. The proof is omitted partly because of the limitations of time and partly because the proof depends upon a 'non-algebraic' property of the system of real numbers. For one possible proof the interested reader may consult the book by Schreier and Sperner in the Bibliography.

The Fundamental Theorem of Algebra also makes it clear what the possibilities are for the prime factorization of a polynomial with real coefficients. If f is a polynomial with real coefficients and c is a complex root of f, then the complex conjugate $\bar{c}$ is also a root of f. Therefore, those complex roots which are not real must occur in conjugate pairs, and the entire set of roots has the form $\{t_1, \ldots, t_k, c_1, \bar{c}_1, \ldots, c_r, \bar{c}_r\}$ where $t_1, \ldots, t_k$ are real and $c_1, \ldots, c_r$ are non-real complex numbers. Thus f factors

$$f = c(x - t_1) \cdots (x - t_k)p_1 \cdots p_r$$

where p_i is the quadratic polynomial

$$p_i = (x - c_i)(x - \bar{c}_i).$$

These polynomials p_i have real coefficients. We conclude that every irreducible polynomial over the real number field has degree 1 or 2. Each polynomial over R is the product of certain linear factors, obtained from the real roots of f, and certain irreducible quadratic polynomials.

Exercises

1. Let p be a monic polynomial over the field F, and let f and g be relatively prime polynomials over F. Prove that the g.c.d. of pf and pg is p.

2. Assuming the Fundamental Theorem of Algebra, prove the following. If f and g are polynomials over the field of complex numbers, then g.c.d. $(f, g) = 1$ if and only if f and g have no common root.

3. Let D be the differentiation operator on the space of polynomials over the field of complex numbers. Let f be a monic polynomial over the field of complex numbers. Prove that

$$f = (x - c_1) \cdots (x - c_k)$$

where $c_1, \ldots, c_k$ are *distinct* complex numbers if and only if f and Df are relatively prime. In other words, f has no repeated root if and only if f and Df have no common root. (Assume the Fundamental Theorem of Algebra.)

4. Prove the following generalization of Taylor's formula. Let f, g, and h be polynomials over a subfield of the complex numbers, with $\deg f \leq n$. Then

$$f(g) = \sum_{k=0}^{n} \frac{1}{k!} f^{(k)}(h)(g - h)^k.$$

(Here $f(g)$ denotes 'f of g.')

For the remaining exercises, we shall need the following definition. If f, g, and p are polynomials over the field F with $p \neq 0$, we say that f is **congruent to** g **modulo** p if $(f - g)$ is divisible by p. If f is congruent to g modulo p, we write

$$f \equiv g \bmod p.$$

5. Prove, for any non-zero polynomial p, that congruence modulo p is an equivalence relation.

(a) It is reflexive: $f \equiv f \bmod p$.
(b) It is symmetric: if $f \equiv g \bmod p$, then $g \equiv f \bmod p$.
(c) It is transitive: if $f \equiv g \bmod p$ and $g \equiv h \bmod p$, then $f \equiv h \bmod p$.

6. Suppose $f \equiv g \bmod p$ and $f_1 \equiv g_1 \bmod p$.
(a) Prove that $f + f_1 \equiv g + g_1 \bmod p$.
(b) Prove that $ff_1 \equiv gg_1 \bmod p$.

7. Use Exercise 7 to prove the following. If f, g, h, and p are polynomials over the field F and $p \neq 0$, and if $f \equiv g \bmod p$, then $h(f) \equiv h(g) \bmod p$.

8. If p is an irreducible polynomial and $fg \equiv 0 \bmod p$, prove that either $f \equiv 0 \bmod p$ or $g \equiv 0 \bmod p$. Give an example which shows that this is false if p is not irreducible.