ANOTHER EXAMPLE OF A EUCLIDEAN RING

The complex numbers $a+bi$ (a and b are ordinary integers) form the ring of *Gaussian integers.*

From the definition of a product

$$(a+bi)(c+di) = (ac-bd)+(ad+bc)i,$$

on defining the "norm" of a number $\alpha = a+bi$ by

$$N(\alpha) = (a+bi)(a-bi) = a^2+b^2,$$

we easily derive the equation

$$N(\alpha\beta) = N(\alpha)\cdot N(\beta). \tag{3.12}$$

The norm $N(\alpha)$ is an ordinary integer which, being the sum of two squares, vanishes only when α vanishes, and which is positive in any other case. From (3.12) it follows that a product $\alpha\beta$ vanishes only when α or β vanishes; hence the ring is an integral domain.

According to Section 3.3, a quotient field exists. If $\alpha = a+bi \neq 0$, then

$$\alpha^{-1} = \frac{a-bi}{N(\alpha)};$$

thus the numbers of the quotient field may be expressed by $(a/n)+(b/n)i$ (a, b, n are integers). These "fractional numbers" form the "Gaussian number field." The definition of the norm and equation (3.12) hold for the elements of this field as well.

In order to arrive at a division algorithm for the ring of the Gaussian integers, we have to find for a given α and $\beta \neq 0$ a number $\alpha-\lambda\beta$ having norm less than β. Let us first determine a fractional number $\lambda' = a'+b'i$ so that $\alpha-\lambda'\beta = 0$; then let us replace a' and b' by the nearest integers a and b, and put $\lambda = a+bi$, $\lambda'-\lambda = \varepsilon$. Then we have

$$\begin{aligned} \alpha-\lambda\beta &= \alpha-\lambda'\beta+\varepsilon\beta = \varepsilon\beta \\ N(\alpha-\lambda\beta) &= N(\varepsilon)N(\beta) \\ N(\varepsilon) &= N(\lambda'-\lambda) = (a'-a)^2+(b'-b)^2 \leqq (\tfrac{1}{2})^2+(\tfrac{1}{2})^2<1 \\ N(\alpha-\lambda\beta) &< N(\beta). \end{aligned}$$

Thus we have found a "division algorithm," which proves that the ring is a Euclidean ring.[10]

[10] *Bibliographic note:* Concerning the question whether the Euclidean algorithm or its generalization exists in arbitrary principal ideal rings, see H. Hasse in *J. reine u. angew. Math.*, **159**, 3–12 (1928). Investigations as to the question in what algebraic number rings the Euclidean algorithm is valid were carried out by O. Perron (*Math. Ann.*, Vol. 107, p. 489), A. Oppenheim (*Math. Ann.*, Vol. 109, p. 349), E. Berg (*Kgl. Fysiogr. Sällskapets Lund Förhandl.* Vol. 5N 5), N. Hofreiter (*Mh. Math. Physik*, Vol. 42, p. 397), H. Behrbohm and L. Redei (*J. reine u. angew. Math.*, Vol. 174, p. 198).

3.8 FACTORIZATION

In this section we shall be concerned solely with integral domains containing an identity. Let us first investigate what we mean by prime elements or indecomposable elements in these domains. We shall consider only ring elements distinct from zero, even when this is not expressly stated.

A prime number in the ring of integers may always be decomposed into factors, even in two ways:

$$p = p\cdot 1 = (-p)\cdot(-1).$$

However, one of these factors is always a "unit", that is, a number ε, whose inverse ε^{-1} is likewise in the ring; $+1$ and -1 are units.

If, in general, an integral domain with identity is given, then by a unit[11] we understand an element ε which possesses an inverse ε^{-1} in the domain. Then ε^{-1}, obviously, is also a unit.

If ε is a unit, then every element a admits a factorization

$$a = a\varepsilon^{-1}\cdot\varepsilon.$$

Such factorizations where one factor is a unit may be called *trivial factorizations.*

An element $p \neq 0$ which admits only trivial factorizations of the kind $p = ab$, where a or b is a unit, is called an *indecomposable element* or a *prime element.* (In case of integers we say: *prime number*; in case of polynomials: *irreducible polynomial.*)

Two quantities, such as a and $b = a\varepsilon^{-1}$, which differ only by a unit as factor, are sometimes called *associates.* Either one is a divisor of its associate, and for their respective principal ideals we have

$$(a) \subseteqq (b), \qquad (b) \subseteqq (a), \qquad \text{hence} \quad (b) = (a).$$

Thus two associates generate the same principal ideal.

If, conversely, either of the two quantities a and b divides the other one, namely,

$$a = bc, \qquad b = ad,$$

it follows that

$$b = bcd, \qquad \text{hence} \quad 1 = cd, \qquad c = d^{-1};$$

hence c and d are units, and a and b are associates.

If c is a divisor of a, but not an associate of a, that is, $a = cd$, and d is not a

[11] The word "unit" is often used as a synonym for "unit element." However, these concepts are to be clearly distinguished in discussing factorization, since, for example, -1 is also a unit.

unit, then c is called a *proper divisor* of a. In this case a is not a divisor of c, and the ideal (c) is a proper divisor of the ideal (a). For if a were a divisor of c, say $c = ab$, then we would have

$$a = cd = abd$$
$$1 = bd$$

and d would be a unit, contrary to our assumption.

A prime element may also be defined as an element distinct from zero which does not possess any proper divisors except units.

Theorem: *If, in a Euclidean ring, b is a proper divisor of a, then $g(b) < g(a)$.*

Proof: The division of b by a leaves a remainder, namely

$$b = aq+r, \qquad g(r) < g(a).$$

Equating $a = bc$, it follows that

$$r = b-aq = b(1-cq)$$
$$g(r) \geqq g(b); \qquad \text{hence} \quad g(b) \leqq g(r) < g(a).$$

In a Euclidean ring every element a distinct from zero is a product of prime elements:

$$a = p_1 p_2 \dots p_r.$$

Remark: More generally, the theorem can be proved for principal ideal rings, but we must then use the axiom of choice (Section 9.2). This part of the book is intended to be elementary, and thus the axiom choice will not be employed. The proof is therefore given only for Euclidean rings.

Proof: We apply the method of induction on $g(a)$: Let the assertion be true for all elements b with $g(b) < n$, and let $g(a) = n$. If a is prime: $a = p$, there is nothing more to be proved. However, if a factors: $a = bc$, where b and c are proper divisors of a, then

$$g(b) < g(a), \qquad g(c) < g(a).$$

By the induction hypothesis, b and c are products of prime elements. Hence $a = bc$ is also a product of prime elements.

We now investigate the uniqueness of factorization into primes $a = p_1 p_2 \dots p_r$ and consider not only Euclidean rings, but arbitrary principal ideal rings.

In a principal ideal ring a prime element, other than a unit, generates a maximal prime ideal (whose residue class ring is thus a field).

Proof: If p is prime, then it has no proper divisors except units, and therefore (since every ideal is a principal ideal) the ideal (p) has no proper ideal divisors except the unit ideal.

Remark: The solvability of the equation $\overline{ax} = \bar{b}$ in the residue class ring or

of the congruence $ax \equiv b(p)$ in the given ring may, of course, readily be seen from the fact that, for $a \not\equiv 0(p)$, we have $(a, p) = 1$. For this implies

$$1 = ar+ps$$
$$b = arb+psb$$
$$b \equiv arb(p).$$

We infer at once: *If a product is divisible by the prime element p, so is one of the factors*; for the residue class ring has no divisors of zero.

Exercises

3.25. Solve the congruence

$$6x \equiv 7(19)$$

using the Euclidean algorithm.

3.26. If in a principal ideal ring a product ab is divisible by c and a is not divisible by c, then b is divisible by c.

We are now in a position to prove the *theorem of uniqueness of prime factorization in principal ideal rings*. Let

$$a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s \tag{3.12}$$

be two factorizations of the same number a in a principal ideal ring. We shall exclude the trivial case where a is a unit and where, consequently, all p_i and q_j are units. Then we may assume that p_1 and q_1 are not units, and that all possible units among the factors p_i and q_j are combined with the factor p_1 and q_1, respectively. Thus let the p_i and q_j not be units. Now we state: $r = s$, *and the p_i and q_j are identical, except for their order and for unit factors.*

For $r = 1$ the proof is clear, for since $a = p_1$ is prime, the product $q_1 \dots q_s$ can contain only one factor $q_1 = p_1$. Thus we may proceed by induction on r. Since p_1 divides the product $q_1 \dots q_s$, p_1 must divide one of the factors q_i. With the q rearranged, p_1 will divide q_1:

$$q_1 = \varepsilon_1 p_1. \tag{3.13}$$

Here ε_1 must be a unit, or else q_1 would not be prime. Substituting (3.13) in (3.12) and dividing by p_1, we obtain

$$p_2 \dots p_r = (\varepsilon_1 q_2) q_3 \dots q_s. \tag{3.14}$$

By the induction hypothesis, the factors on the left and right side of (3.14) must be the same, except for the unit factors. Since p_1 is identical with q_1, except for the unit factor ε_1, the proof is completed.

From the theorems proved we infer: *The elements of a Euclidean ring are uniquely expressible as products of prime elements, except for units and for the* *order of the factors.* This is true in particular for the integers, for the polynomials in one variable with coefficients from a field, and for the Gaussian integers.

Exercises

3.27. The integral polynomials $f(x)$ modulo any prime number p are uniquely decomposable into factors which are irreducible modulo p.

3.28. What are the units of the Gaussian number ring? Decompose into prime factors the numbers 2, 3, 5 in this ring.

3.29. For the number 4 in the ring of the numbers $a+b\sqrt{-3}$ there are two substantially different factorizations into prime factors:

$$4 = 2\cdot 2 = (1+\sqrt{-3})\,(1-\sqrt{-3}).$$

3.30. In a principal ideal ring the residue classes modulo a consisting of elements relatively prime to a form a group under multiplication.

In Chapter 5 we shall see that there are rings other than principal ideal rings for which the unique factorization theorem holds. For all such rings we shall now prove the following theorem.

Theorem: *If in* $\mathfrak{o}$ *every element factors uniquely into prime elements, then every prime element p generates a prime ideal, and every nonprime element distinct from zero generates a nonprime ideal.*

Proof: Let p be prime. If $ab \equiv 0(p)$, then the factor p must occur, when ab is factored. This factorization, however, is obtained by combining the factorizations of a and b; therefore, the factor p must already occur in a or b, whence $a \equiv 0(p)$ or $b \equiv 0(p)$.

Now let p factor: $p = ab$, where a and b are proper divisors of p. Then it follows that $ab \equiv 0(p)$, $a \not\equiv 0(p)$, $b \not\equiv 0(p)$. Therefore the ideal (p) is not prime.

Exercise

3.31. Prove that for all rings with unique factorization every two or more elements have a "greatest common divisor" and a "least common multiple," both of them being determined except for unit factors.

Remark: For rings of the kind considered, the g.c.d. in the sense of an element is not always the same as the g.c.d. in the sense of an ideal. For example, in the polynomial domain of a variable x with integer coefficients the elements 2 and x have no common divisors except units; but the ideal $(2, x)$ is not the unit ideal. (In Chapter 5 it will be proved that there is unique factorization in this ring.)

Chapter 4

VECTOR SPACES AND TENSOR SPACES

4.1 VECTOR SPACES

Let (1) K be a skew field with elements $a, b, \ldots$ which are called *coefficients* or *scalars*, (2) $\mathfrak{M}$ be a module (that is, an additive Abelian group) with elements $x, y, \ldots$ which are called *vectors*, and (3) xa be a multiplication of vectors with scalars with the following properties:

V1. xa lies in $\mathfrak{M}$.

V2. $(x+y)a = xa+ya.$

V3. $x(a+b) = xa+xb.$

V4. $x(ab) = (xa)b.$

V5. $x1 = x.$

If these requirements are fulfilled, then $\mathfrak{M}$ is called a *vector space over* K or, more precisely, a *right K vector space*, since the coefficients a stand to the right of the vectors. The concept of a *left K vector space* is defined analogously; the associative law V4 for a left vector space reads

V4* $(ab)x = a(bx).$

If K is commutative, we may also write xa in place of ax. A right vector space thus becomes a left vector space. If, however, K is not commutative, then we must distinguish between right and left vector spaces.

We write xab rather than $x(ab)$ or $(xa)b$. The zero element of $\mathfrak{M}$ is denoted by 0 just as the zero element for K.

Examples of vector spaces are all extension fields of a field K and, more generally, of all rings R containing a skew field K as long as the unit element of K is also a unit element of R.

From V2 it follows as usual that

$$(x_1+\cdots+x_r)a = x_1a+\cdots+x_ra$$
$$(x-y)a = xa-ya$$
$$0\cdot a = 0.$$

of the columns are given. The following example ($n = 3$, $a_0 = 0$, $\Delta a_0 = 1$, $\Delta^2 a_0 = 6$, $\Delta^3 a_0 = 6$) will explain the computation:

$$\begin{array}{cccccccc}
0 & & & & & & & \lambda_0 = 0 \\
 & 1 & & & & & & \\
1 & & 6 & & & & & \lambda_1 = 1 \\
 & 7 & & 6 & & & & \\
8 & & 12 & & & & & \lambda_2 = \frac{6}{2} = 3 \\
 & 19 & & 6 & & & & \\
27 & & 18 & & & & & \lambda_3 = \frac{6}{6} = 1 \\
 & 37 & & 6 & & & & \\
64 & & 24 & & & & & \\
 & 61 & & & & & & \\
125 & & & & & & &
\end{array}$$

$$\begin{aligned} f(x) &= \lambda_0+\lambda_1 x+\lambda_2 x(x-1)+\lambda_3 x(x-1)(x-2) \\ &= x+3x(x-1)+x(x-1)(x-2) = x^3. \end{aligned}$$

By an arithmetic series of 0th order we shall mean a sequence of identical numbers $c, c, c, \ldots$, and by an arithmetic series of nth order a sequence of numbers such that its sequence of differences is an arithmetic series of $(n-1)$th order. Then it is obvious that the first column of the array (5.13) forms an arithmetic series of the nth order, provided the $(n+2)$th column consists of zeros only. Consequently, what was proved above may be formulated as follows.

The values of a polynomial $f(x)$ of degree n at the points 0, 1, 2, 3, . . . *form an arithmetic series of the nth order, and every arithmetic series of the nth order consists of the values of a polynomial of at most degree n at those points.* The polynomial $f(x)$ itself is obtained from (5.7) and (5.14). Thus the generic term a_x of an arithmetic series of order n is given by the formula

$$a_x = f(x) = a_0+(\Delta a_0)x+\frac{\Delta^2 a_0}{2}\,x(x-1)+\cdots+\frac{\Delta^n a_0}{n!}\,x(x-1)\ldots(x-n+1).$$

A practical application of the array of differences (5.13) can be found in the interpolation and integration of functions given by numerical tables (for example, by tables obtained empirically). If $a_0, a_1, a_2, \ldots$ are the values of a function $\varphi(x)$ for equidistant argument values α_0, α_0+h, $\alpha_0+2h, \ldots$, it will be seen that, for well-behaved functions and for not too great an interval h, the second, third, fourth, or in the worst case the fifth difference becomes practically zero, which shows that in some adjacent intervals the function behaves almost exactly like the polynomial of at most degree four. Thus, for numerical interpolation or integration, the function may be replaced by the polynomial which assumes the table values at two to five successive points. Interpolation is carried out by means of formula (5.7). In most cases linear or quadratic interpolation is sufficient, which means that only the first and second differences are needed, and the higher ones may be neglected. When differences $\Delta^k a_\nu$ are converted into difference quotients, powers of the length of the interval h appear besides the factors $k!$; accordingly, instead of (5.14), we must use the formula

$$\lambda_k = \frac{\Delta^k a_0}{k!\,h^k}.$$

For argument values $\alpha_0, \alpha_1, \ldots$ no longer equidistant we must form difference quotients (5.12) right at the outset instead of the differences $\Delta^k a_\nu$. Further details of the computation as well as error estimates will be found in special text books.[1]

Exercises

5.5. The partial sums $s_m = \sum_{\nu=0}^{m-1} a_\nu$ of an arithmetic series of the nth order (where $s_0 = 0$) form an arithmetic series of the $(n+1)$th order. Derive from this the formula for the sum

$$s_m = ma_0+\binom{m}{2}\Delta a_0+\cdots+\binom{m}{n+1}\Delta^n a_0.$$

5.6. Furnish formulas for the sums $\sum_{\nu=0}^{m-1}\nu$, $\sum_{\nu=0}^{m-1}\nu^2$, $\sum_{\nu=0}^{m-1}\nu^3$.

5.4 FACTORIZATION

We saw already in Section 4.1 that the theorem on unique factorization holds for the polynomial domain K[x], where K is a commutative *field.* We shall proceed to prove the following more general main theorem.

Theorem: *If $\mathfrak{S}$ is an integral domain with an identity, and if the unique factorization theorem holds in $\mathfrak{S}$, then the same theorem holds for the polynomial domain $\mathfrak{S}[x]$.*

The proof is due to Gauss.

Let $f(x) = \sum_0^n a_i x^i$ be a polynomial in $\mathfrak{S}[x]$ distinct from zero. The greatest common divisor d of $a_0, \ldots, a_n$ in $\mathfrak{S}$ (cf. Exercise 3.31) is called the *content* of $f(x)$. Factoring out d, we have

$$f(x) = d\cdot g(x),$$

where $g(x)$ has the content 1. Both $g(x)$ and d are uniquely determined, except for unit factors. Polynomials having content 1 are called *primitive polynomials* (with respect to $\mathfrak{S}$).

Lemma 1: *The product of two primitive polynomials is itself primitive.*

[1] For example, Kowalewski, *Interpolation und genäherte Quadratur* (Leipzig, 1930).

Proof: Let

$$f(x) = a_0+a_1x+\cdots$$

and

$$g(x) = b_0+b_1x+\cdots$$

be primitive polynomials. Let us suppose the coefficients of $f(x)\cdot g(x)$ have a common divisor d other than a unit. If p is a prime factor of d, then p must divide all coefficients of $f(x)g(x)$. Let a_r be the first coefficient of $f(x)$ not divisible by p (it must exist; otherwise $f(x)$ would not be a primitive polynomial); similarly, let b_s be the first coefficient of $g(x)$ not divisible by p.

The coefficient of x^{r+s} in $f(x)g(x)$ is of the form

$$a_rb_s+a_{r+1}b_{s-1}+a_{r+2}b_{s-2}+\cdots$$
$$+a_{r-1}b_{s+1}+a_{r-2}b_{s+2}+\cdots \quad .$$

The sum is supposed to be divisible by p. All terms except the first term are divisible by p. Hence, a_rb_s must be divisible by p; that is, either a_r or b_s has to be divisible by p, contrary to the assumption.

Let Σ be the quotient field of $\mathfrak{S}$ (Section 3.3). Then every polynomial in $\Sigma[x]$ can be factored uniquely (Section 3.8). In order to pass from the factorization in $\Sigma[x]$ to that in $\mathfrak{S}[x]$, we utilize the following fact: Every polynomial $\varphi(x)$ of $\Sigma[x]$ may be written in the form $[F(x)]/b$ ($F(x)$ in $\mathfrak{S}[x]$, b in $\mathfrak{S}$), where b is, say, the product of the denominators of the coefficients of $\varphi(x)$. Moreover, we may express $F(x)$ as the product of its "content by a primitive polynomial":

$$F(x) = a\cdot f(x),$$

$$\varphi(x) = \frac{a}{b}\cdot f(x). \tag{5.15}$$

Now we state the following.

Lemma 2: *The primitive polynomial $f(x)$ occurring in* (5.15) *is uniquely determined by $\varphi(x)$ up to units of $\mathfrak{S}$. Conversely, $\varphi[x]$ is by* (5.15) *uniquely determined by $f(x)$ up to units of $\Sigma[x]$. If in this manner we assign to each $\varphi(x)$ of $\Sigma[x]$ a primitive polynomial $f(x)$, then to the product of two polynomials $\varphi(x)\cdot\psi(x)$ there corresponds, up to units, the product of the respective primitive polynomials (and vice versa). If $\varphi(x)$ is irreducible in $\Sigma[x]$, then $f(x)$ is irreducible in $\mathfrak{S}[x]$ (and conversely).*

Proof: Let two different expressions for $\varphi(x)$ be given:

$$\varphi(x) = \frac{a}{b}f(x) = \frac{c}{d}g(x).$$

Then

$$adf(x) = cbg(x) \tag{5.16}$$

follows.

The content of the left side is ad, that on the right side, cb; hence

$$ad = \varepsilon cb$$

where ε is a unit in $\mathfrak{S}$. Substituting it in (5.16) and dividing by cb, we get

$$\varepsilon f(x) = g(x).$$

Thus $f(x)$ and $g(x)$ differ from one another only by a unit in $\mathfrak{S}$.

For the product of two polynomials

$$\varphi(x) = \frac{a}{b}f(x)$$

$$\psi(x) = \frac{c}{d}g(x),$$

we obtain at once

$$\varphi(x)\cdot\psi(x) = \frac{ac}{bd}f(x)g(x).$$

By Lemma 1, $f(x)g(x)$ is again a primitive polynomial. Thus the product $f(x)\cdot g(x)$ corresponds to the product $\varphi(x)\cdot\psi(x)$.

If, finally, $\varphi(x)$ is indecomposable, so is $f(x)$; for a decomposition $f(x) = g(x)h(x)$ would immediately imply a decomposition

$$\varphi(x) = \frac{a}{b}f(x) = \frac{a}{b}g(x)\cdot h(x).$$

The converse can be proved in a similar fashion.

This completes the proof of Lemma 2.

By virtue of Lemma 2, the unique factorization of the polynomials $\varphi(x)$ may readily be applied to the respective primitive polynomials. Hence: *Primitive polynomials may uniquely (up to unit factors) be decomposed into prime factors which are themselves primitive polynomials.*

Let us now turn to the factorization of arbitrary polynomials in $\mathfrak{S}[x]$. A polynomial which does not factor is necessarily either a prime constant or an irreducible primitive polynomial, for any other polynomial factors into its content times a primitive polynomial. To factor a polynomial $f(x)$, then, write it as content times a primitive polynomial, and factor these two parts into prime factors. The first part can be so factored (uniquely except for unit factors) by the hypothesis of our main theorem; so can the second, by what we have just proved. This completes the proof of the main theorem.

The following assertion is an additional result of the proof.

If a polynomial $F(x)$ in $\mathfrak{S}[x]$ factors in $\Sigma[x]$, then it factors in $\mathfrak{S}[x]$.

For if we put $F(x) = d\cdot f(x)$, we obtain a primitive polynomial $f(x)$ corresponding to the polynomial $F(x)$, and according to Lemma 2 a factorization of $F(x)$ in $\Sigma[x]$ entails one of $f(x)$ in $\mathfrak{S}[x]$. Thus, if $f(x)$ factors, so does $F(x)$.

For example, a polynomial with integer coefficients which factors when we allow rational coefficients must also factor using integer coefficients. Thus, *if a polynomial with integral coefficients cannot be factored using integral coefficients, it also cannot be factored using rational coefficients.*

By induction we obtain another result from the main theorem.

If $\mathfrak{S}$ is an integral domain with an identity element, and if the unique factorization theorem is valid in $\mathfrak{S}$, then this theorem is likewise valid in the polynomial domain $\mathfrak{S}[x_1, \ldots, x_n]$.

From this theorem follows, for example, the unique factorization for polynomials with integer coefficients (in any number of variables), for polynomials with coefficients in a field, and so on.

The concept of a "primitive polynomial," introduced in the Gaussian lemmas above, is particularly useful whenever we are dealing with polynomial domains in several variables. If K is a field, then a polynomial f of $K[x_1, \ldots, x_n]$ is called *primitive with respect to* $x_1, \ldots, x_{n-1}$ if it is primitive with respect to the integral domain $K[x_1, \ldots, x_{n-1}]$, that is, if it does not have a nonconstant factor that depends only on $x_1, \ldots, x_{n-1}$.

Exercises

5.7. The only units in $\mathfrak{S}[x]$ are those in $\mathfrak{S}$.

5.8. Prove that the factorization of a homogeneous polynomial yields only homogeneous factors.

5.9. Prove that the determinant

$$\Delta = \begin{vmatrix} x_{11} \ldots x_{1n} \\ \cdot \qquad \cdot \\ \cdot \qquad \cdot \\ \cdot \qquad \cdot \\ x_{n1} \ldots x_{nn} \end{vmatrix}$$

is irreducible in the polynomial domain $\mathfrak{S}[x_{11}, \ldots, x_{nn}]$. (Select one indeterminate, say x_{11}, and show that Δ is primitive with respect to the others.)

5.10. Establish a rule to decide whether a polynomial with integer coefficients has a factor of the first degree.

5.11. Prove the irreducibility of the polynomial

$$x^4 - x^2 + 1$$

in the polynomial domain of the indeterminate x over the ring of integers. Is the polynomial reducible when rational coefficients are allowed? Is it reducible over the ring of Gaussian integers?

5.5 IRREDUCIBILITY CRITERIA

Let $\mathfrak{S}$ be an integral domain with an identity element in which unique factorization holds. Let

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

be a polynomial in $\mathfrak{S}[x]$. The following theorem frequently supplies information as to the irreducibility of $f(x)$.

Eisenstein's Theorem: *If there exists a prime element p in $\mathfrak{S}$ such that*

$$\begin{aligned} a_n &\not\equiv 0(p) \\ a_i &\equiv 0(p) \qquad \text{for all } i<n \\ a_0 &\not\equiv 0(p^2), \end{aligned}$$

then $f(x)$ is irreducible in $\mathfrak{S}[x]$, except for constant factors; in other words, $f(x)$ is irreducible in $\Sigma[x]$, where Σ is the quotient field of $\mathfrak{S}$.

Proof: Let us suppose $f(x)$ factors:

$$f(x) = g(x) \cdot h(x),$$

$$g(x) = \sum_0^r b_\nu x^\nu,$$

$$h(x) = \sum_0^s c_\nu x^\nu,$$

$$r>0, \quad s>0, \quad r+s = n;$$

then we would have

$$a_0 = b_0 c_0 \qquad \text{and} \quad a_0 \equiv 0(p).$$

It follows that either $b_0 \equiv 0(p)$ or $c_0 \equiv 0(p)$. Let, for example, $b_0 \equiv 0(p)$. Then $c_0 \not\equiv 0(p)$, or else we would have $a_0 = b_0 c_0 \equiv 0(p^2)$.

Not all the coefficients of $g(x)$ are divisible by p, for otherwise the product $f(x) = g(x) \cdot h(x)$ would be divisible by p, and all coefficients, in particular a_n, would be divisible by p, which contradicts the hypothesis. Thus let b_i be the first coefficient of $g(x)$ not divisible by $p (0 < i \leqq r < n)$. Then

$$\begin{aligned} a_i &= b_i c_0 + b_{i-1} c_1 + \cdots + b_0 c_i \\ a_i &\equiv 0(p) \\ b_{i-1} &\equiv 0(p) \\ &\ldots \\ b_0 &= 0(p); \end{aligned}$$

hence

$$\begin{aligned} b_i c_0 &\equiv 0(p) \\ c_0 &\not\equiv 0(p) \\ b_i &\equiv 0(p), \end{aligned}$$

contrary to the hypothesis.

Hence $f(x)$ is irreducible, except for constant factors.

Example 1: $x^m - p$ (p prime) is irreducible over the ring of integers (and therefore also over the field of rational numbers). Hence $\sqrt[m]{p} (m>1,\ p \text{ prime})$ is always irrational.

Example 2: $f(x) = x^{p-1}+x^{p-2}+\cdots+1$ is the left member of a "cyclotomic equation" if p is a prime number. We again ask for irreducibility over the ring of integers. The Eisenstein criterion cannot be applied directly, but we can reason as follows: If $f(x)$ were reducible, $f(x+1)$ would be also. Now we have

$$f(x+1) = \frac{(x+1)^p-1}{(x+1)-1} = \frac{x^p+\binom{p}{1}x^{p-1}+\cdots+\binom{p}{p-1}x}{x}$$

$$= x^{p-1}+\binom{p}{1}x^{p-2}+\cdots+\binom{p}{p-1}.$$

All coefficients, except that of x^{p-1} are divisible by p; for in the formula for the binomial coefficients

$$\binom{p}{i} = \frac{p(p-1)\ldots(p-i+1)}{i!}$$

the numerator is divisible by p for $i<p$, but not the denominator. Furthermore, the constant term

$$\binom{p}{p-1} = p$$

is not divisible by p^2. Hence $f(x+1)$ is irreducible, and so is $f(x)$.

Example 3: For $f(x) = x^2+1$ the same transformation leads to a decision, since

$$f(x+1) = x^2+2x+2.$$

Exercises

5.12. Prove the irrationality of $\sqrt[m]{p_1p_2\cdots p_r}$, where $p_1,\ldots,p_r$ are different prime numbers and $m>1$.

5.13. Show that

$$x^2+y^3-1$$

is irreducible in $\mathrm{P}[x, y]$, where P is any field in which $+1 \neq -1$.

5.14. Show that the polynomials

$$x^4+1, \qquad x^6+x^3+1$$

are irreducible in the polynomial domain over the integers.

Basically, the Eisenstein theorem rests on the fact that the equation

$$f(x) = g(x)\cdot h(x)$$

is transformed into a congruence modulo p^2, namely

$$f(x) \equiv g(x)\cdot h(x),$$

which leads to an absurdity. In many other cases it is likewise possible to furnish irreducibility proofs by transforming the equations into congruences, modulo some quantity q of the domain $\mathfrak{S}$, and by investigating whether the polynomial $f(x)$ under consideration can be resolved modulo q. If, in particular, $\mathfrak{S}$ is the domain of the integers $\mathbb{Z}$, then there are only a finite number of polynomials of a given degree in the residue class domain modulo q; hence there are always but a finite number of possibilities of a resolution of $f(x)$ modulo q that have to be investigated. If it is found that $f(x)$ is irreducible modulo q, then $f(x)$ was also irreducible in $\mathbb{Z}[x]$, and even in the opposite case we might be able to draw conclusions from the decomposition modulo q. In the case where q is a prime number we may apply the unique factorization theorem of the polynomials modulo q (Exercise 3.27).

Example 4: $\mathfrak{S} = \mathbb{Z}; f(x) = x^5-x^2+1$. If $f(x)$ factors modulo 2, then one of the factors has to be linear or quadratic. Now there are but two linear polynomials modulo 2:

$$x, \qquad x+1,$$

and but one irreducible quadratic polynomial:

$$x^2+x+1.$$

On performing the division, we see that x^5-x^2+1 is not divisible by any of these polynomials (modulo 2). This can be seen directly from

$$x^5-x^2+1 = x^2(x^3-1)+1 \equiv x^2(x+1)\,(x^2+x+1)+1.$$

Hence, $f(x)$ is irreducible.

5.6 FACTORIZATION IN A FINITE NUMBER OF STEPS

Thus far we have only seen that there is a theoretical possibility to decompose into prime factors any polynomial in $\Sigma\,[x_1,\ldots,x_n]$ for a given field Σ, and in some instances we have provided the tools for actually furnishing a decomposition, or for showing the impossibility; yet we still lack a general method for performing the factorization in a finite number of steps for any case that may present itself to us. We proceed to develop such a method at least for the case in which Σ is the field of rational numbers.

According to Section 4.5, we may assume the coefficients of any rational polynomial to be integers, and we may perform its factorization in the domain of integers. In the ring $\mathbb{Z}$ of the integers itself a factorization into primes can evidently be performed by a finite trial and error method; furthermore, there are only a finite number of units ($+1$ and -1) in the ring $\mathbb{Z}$, and hence a finite number of possible factorizations. Similarly, in the polynomial domain $\mathbb{Z}[x_1,\ldots,x_n]$ there are only the units $+1$, -1. By the method of induction on the variable number n we shall now reduce everything to the following problem.

Let any factorization in $\mathfrak{S}$ be performable in a finite number of steps: moreover, let there be only a finite number of units in $\mathfrak{S}$. We wish to find a method of factoring every polynomial in $\mathfrak{S}[x]$ into prime factors.

The solution is due to Kronecker.

Let $f(x)$ be a polynomial of degree n in $\mathfrak{S}[x]$. If $f(x)$ can be factored, then one of the factors is of degree $\leqq n/2$; thus, if s is the greatest integer $\leqq n/2$, we must investigate whether $f(x)$ has a factor $g(x)$ of degree $\leqq s$.

We form the functional values $f(a_0), f(a_1), \dots, f(a_s)$ for $s+1$ integral arguments $a_0, a_1, \dots, a_s$. If $f(x)$ is to be divisible by $g(x)$, then $f(a_0)$ must be divisible by $g(a_0)$, and $f(a_1)$ by $g(a_1)$, and so on. However, every $f(a_i)$ in $\mathfrak{S}$ possesses only a finite number of factors; therefore, for every $g(a_i)$ there are only a finite number of possibilities all of which may be found explicitly. For every possible combination of values $g(a_0), g(a_1), \dots, g(a_s)$ there is, according to the theorems of Section 4.4, one and only one polynomial $g(x)$ which may be formed by Lagrange's or, more conveniently, Newton's interpolation formula. In this way a finite number of possible factors $g(x)$ are found. Employing the division algorithm, we may now find out whether each of these polynomials $g(x)$ is actually a factor of $f(x)$. If, apart from the units, none of the possible $g(x)$ is a factor of $f(x)$, then $f(x)$ is irreducible; otherwise, a factorization has been found, and we may proceed to apply the same procedure to the two factors, and so forth. In this manner we finally arrive at the irreducible factors.

In the integral case ($\mathfrak{S} = \mathbb{Z}$) the procedure may frequently be shortened considerably. By factoring the given polynomial modulo 2 and possibly modulo 3, we get an idea what degrees the possible factor polynomials $g(x)$ might have, and to what residue classes the coefficients modulo 2 and 3 might belong. This limits the number of the possible $g(x)$ considerably. Moreover, when applying Newton's interpolation formula, one should note that the last coefficient λ_s must be a factor of the highest coefficient of $f(x)$, which limits the number of possibilities still further. Finally, it is an advantage to use more than $s+1$ points a_i (preferably 0, ± 1, ± 2 and so on). For determining the possible $g(a_i)$ we use those $f(a_i)$ which contain the least number of prime factors; the other points may afterwards be used in order to limit the number of possibilities still further by examining each $g(x)$, and to see whether it assumes values which are factors of the respective $f(a_i)$ at all points a_i.

Exercises

5.15. Factor

$$f(x) = x^5+x^4+x^2+x+2$$

in $\mathbb{Z}[x]$.

5.16. Factor

$$f(x, y, z) = -x^3-y^3-z^3+x^2(y+z)+y^2(x+z)+z^2(x+y)-2xyz$$

in $\mathbb{Z}[x, y, z]$.

5.7 SYMMETRIC FUNCTIONS

Let $\mathfrak{o}$ be an arbitrary commutative ring with an identity element.

A polynomial in $\mathfrak{o}[x_1, \dots, x_n]$ which is unchanged by any permutation of the indeterminates $x_1, \dots, x_n$ is called a (rational integral) *symmetric function* of the variables $x_1, \dots, x_n$. Examples: sum, product, sum of powers $s_\varrho = \sum_{\nu=1}^{n} x_\nu^\varrho$.

Introducing a new indeterminate z, we put

$$\begin{aligned} f(z) &= (z-x_1)(z-x_2)\dots(z-x_n) \\ &= z^n-\sigma_1 z^{n-1}+\sigma_2 z^{n-2}-\dots+(-1)^n\sigma_n. \end{aligned} \tag{5.17}$$

The coefficients of the powers of z in this polynomial are

$$\begin{aligned} \sigma_1 &= x_1+x_2+\dots+x_n, \\ \sigma_2 &= x_1x_2+x_1x_3+\dots+x_2x_3+\dots+x_{n-1}x_n, \\ \sigma_3 &= x_1x_2x_3+x_1x_2x_4+\dots+x_{n-2}x_{n-1}x_n, \\ &\dots \\ \sigma_n &= x_1x_2\dots x_n. \end{aligned}$$

Obviously, they are all symmetric functions, since the left side of (5.17) remains unchanged by any permutations of the x_i. We call $\sigma_1, \dots, \sigma_n$ the *elementary symmetric functions* of $x_1, \dots, x_n$.

A polynomial $\varphi(\sigma_1, \dots, \sigma_n)$ becomes a symmetric function of the $x_1, \dots, x_n$ when the σ are written in terms of the x. Thus a term $c\sigma_1^{\mu_1}\dots\sigma_n^{\mu_n}$ of $\varphi(\sigma_1, \dots, \sigma_n)$ becomes a homogeneous polynomial in the x_i of degree $\mu_1+2\mu_2+\dots+n\mu_n$, since every σ_i is a homogeneous polynomial of the ith degree. The sum $\mu_1+2\mu_2+\dots+n\mu_n$ will be called the *weight* of the term $c\sigma_1^{\mu_1}\dots\sigma_n^{\mu_n}$. The weight of a polynomial $\varphi(\sigma_1, \dots, \sigma_n)$ is defined as the largest weight occurring among its terms. Polynomials $\varphi(\sigma_1, \dots, \sigma_n)$ of weight k, therefore, yield symmetric polynomials in the x_i of degree $\leqq k$.

The so-called Fundamental Theorem on Symmetric Functions asserts that the converse is also true:

A symmetric polynomial of degree k in $\mathfrak{o}[x_1, \dots, x_n]$ *may be written as a polynomial* $\varphi(\sigma_1, \dots, \sigma_n)$ *of weight k.*

Proof: The given symmetric polynomial is ordered *lexicographically* (as in a dictionary), that is, a term $x_1^{\alpha_1}\dots x_n^{\alpha_n}$ precedes $x_1^{\beta_1}\dots x_n^{\beta_n}$ if the first non-vanishing difference $\alpha_i-\beta_i$ is positive. Together with a term $ax_1^{\alpha_1}\dots x_n^{\alpha_n}$ occur all terms whose exponents are a permutation of the α_i. These are not all written; we rather write $a\sum x_1^{\alpha_1}\dots x_n^{\alpha_n}$, where only the lexicographically first term of the sum actually appears. For this term, $\alpha_1 \geqq \alpha_2 \geqq \dots \geqq \alpha_n$.

Let the degree of the given symmetric polynomial be k, and let the first term in the lexicographic ordering be $ax_1^{\alpha_1}\dots x_n^{\alpha_n}$. We now form a product of elementary