# The Question of Finitely Many Steps in Polynomial Ideal Theory *

**Grete Hermann** in Göttingen

In the present work, the domains in which ideals are defined are polynomial domains. An ideal will be called *given* if a *basis* of the ideal is known, and *computable* if a basis can be computed. This work deals with computing characteristic ideals and polynomials for a given ideal $\mathfrak{m}$. The computation is based on ideal theory and elimination theory as developed by E. Noether and K. Hentzelt [2,8,9][1]. I especially recommend the summary [9, §1] for the basic ideas used here. Some changes to the definitions and further corollaries will be given in §1 of this work.

The computational methods below are computations in *finitely many steps*. The claim that a computation can be carried out in finitely many steps will mean here that *an upper bound for the number of necessary operations for the computation* can be specified. Thus it is not enough, for example, to suggest a procedure, for which it can be proved theoretically that it can be executed in finitely many operations, if no upper bound for the number of operations is known [2]. In particular, the bounds appearing in the present work will depend only on the number $n$ of variables, the number $t$ of basis elements of the ideal, and the maximum degree $q$ of these basis elements; they are independent of the coefficients of the basis elements. Using these bounds, which indicate up to what degree the variables must be considered, the problems can be reduced to problems of determinant and elementary divisor theory, which can be settled in finitely many steps by known methods.

The methods provided in §§6-8, with which all of the characteristic ideals and polynomials for the ideal $\mathfrak{m}$ can be computed, must be preceded by some preparatory theorems in §§2-5. The search for the associated prime ideals of an ideal $\mathfrak{m}$ corresponds to, and reduces to, the simpler problem of factoring a polynomial into prime functions. Thus §2 deals with the factorization of a polynomial into prime functions. The methods used here were suggested by

* *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. **95** (1926), 736-788. Translation by Michael Abramson.

[1] For useful concepts from field theory, [10] is recommended.

[2] Macaulay, who indicates a way based on Lasker's work [6] to compute the associated prime ideals and the exponents of the associated primary ideals associated of an ideal, has no such upper bound [7, p. 81].

Kronecker [5]. Kronecker restricted everything to fields of characteristic zero, and then only to finite algebraic and transcendental extensions of prime fields. His methods can be extended directly to fields of arbitrary characteristic, and specifically to finite algebraic, and finite or infinite transcendental extensions of prime fields. For the case of infinite algebraic extensions, we need help from ideas of Steinitz.

The theorems in the paragraphs which follow are ideal theoretic. In §§3-5, the basics for the computation of the upper bounds are given which make the later calculations possible. It is of utmost importance to be able to carry out the simplest computational operations, the formation of products and quotients, least common multiples, and greatest common divisors in finitely many steps. As long as the methods for this are not trivial, they appear in §3 as an application of a theorem of Hilbert [3][3]. §§4-5 bring criteria for the divisibility of a polynomial by an ideal. In particular, the criterion supplied in §4 is purely formal; the divisibility depends on the solvability of a linear system of equations, which can be computed from the coefficients of the given polynomials and those of the basis elements of the ideal. It is not necessary to know the inner structure of the ideal to apply this criterion. On the other hand, *Hentzelt's Nullstellensatz* provides a criterion in §5, which also gives us substantial insight into the structure of the ideal. There is of course a bound on the degree to which a polynomial must vanish, at least at the transcendental zeros of the ideal, in order to be divisible by the ideal. Because of its theoretic formulation as opposed to the one given in §4, this criterion is itself of some interest; in the most special case, it reduces to Noether's fundamental theorem on algebraic functions. Moreover, it will be shown that the number computed here is indeed an upper bound for the smallest exponent of prime ideals which appear in a decomposition of $\mathfrak{m}$.

Now as an application of the theorems in §§2-5, the computations of the important ideals and polynomials are carried out in §§6-8. §6 provides the computation of fundamental ideals, which simultaneously yields the computation of the norm and elementary divisor form of the ideal. The polynomials essential for elimination theory are thereby computed, from whose factorization, we obtain the zeros of the ideals. In §7, methods for computing the associated prime ideals of the ideal $\mathfrak{m}$ are proposed. This is more complicated when the underlying coefficient domain for the polynomials of the ideal is an imperfect field than in the case of perfect fields. Finally, by applying Hentzelt's Nullstellensatz, we show in §8 how to find a primary ideal for each associated prime ideal of the ideal $\mathfrak{m}$ that can appear in a decomposition of $\mathfrak{m}$. Of course with these primary ideals, we also have the isolated components of the ideals.

The theorems of §§4-5, as well as Theorem 6 in §6, were taken from a manuscript of K. Hentzelt. Hentzelt gave them there using only very com-

[3]The theorem used here is a part of Theorem 3 on the termination of the syzygy chain. The same theorem can be found in König [4]. König uses the same methods as Hilbert, but starts errantly from only one equation, without noticing that the induction step actually leads to a system of equations.

plex formulas that lack conceptual meaning. I have replaced this formulation with a conceptual one, and explicitly specified the bounds, at whose computation Hentzelt only hinted. Furthermore, it was necessary to extend the claim in Hentzelt's Nullstellensatz somewhat by using the concept of transcendental zeros. Hentzelt spoke only of the set of algebraic zeros of an ideal and thus did not have the vital partitioning of zeros by dimension of the prime ideals for what followed. The method used in Hentzelt's proof of reducing the degree numbers by a regular determinant, *i.e.* by a determinant representing a regular polynomial, was taken by Hentzelt from Hilbert's proof, which is given in §3 so that the proofs of the theorems in §§3-5 are completely parallel. With his theorems, Hentzelt intended only to take care of the question of elimination theory in finitely many steps. He wanted to compute the norm and elementary divisor form of an ideal, but as the applications §§6-8 show, all of the characteristic ideals for the ideal can already be computed on the basis of his theorems.

# §1. Fundamental Concepts

The definitions of the underlying domain, transformed ideals, module representation of ideals, its isolated components, the elementary divisor form and norm, as well as the decomposition theorems valid for ideals are given in [9,§1.1-3,5-7,9][4].

1. *Notation.* The degree of a polynomial $f(x_1, \ldots, x_n)$ in all variables will be denoted by $[f]$, the degree of $f$ in $x_1, \ldots, x_\varrho$ by $[f]_\varrho$. $f^{(i)}$, $g^{(i)}$, $h^{(i)}$, etc. will denote polynomials which are dependent only on $x_i, \ldots, x_n$.

   If $\mathbb{P}$ denotes any field and $\alpha_1, \ldots, \alpha_r$ are algebraic or transcendental elements over $\mathbb{P}$ lying in any extension field of $\mathbb{P}$, then $\mathbb{P}(\alpha_1, \ldots, \alpha_r)$ is the field obtained by adjoining $\alpha_1, \ldots, \alpha_r$ to $\mathbb{P}$, and $\mathbb{P}[\alpha_1, \ldots, \alpha_r]$ is the ring of polynomials in $\alpha_1, \ldots, \alpha_r$ with coefficients in $\mathbb{P}$. If $\overline{\mathbb{P}}$ is the underlying field of the non-transformed ideals, and $\mathbb{P}$ is the one for the transformed ideals, then with the notation of [9, §1.1],

$$\mathbb{P} = \overline{\mathbb{P}}(u_{11}, \ldots, u_{nn}),$$

   where the $u_{ij}$ denote the transformation coefficients, whence the domains $\overline{\mathfrak{R}}$ and $\mathfrak{R}$ of the non-transformed and transformed ideals can be written as:

$$\begin{array}{rcl} \overline{\mathfrak{R}} & = & \overline{\mathbb{P}}[y_1, \ldots, y_n], \\ \mathfrak{R} & = & \mathbb{P}[x_1, \ldots, x_n] \quad = \quad \overline{\mathbb{P}}(u_{11}, \ldots, u_{nn})[x_1, \ldots, x_n]. \end{array}$$

[4]Translator's Note: A *transformed ideal* is the image of an ideal in the domain of a linear transformation of the variables of a polynomial ring, where the transformation coefficients are indeterminates added to the underlying field in the image. The *module representation of ideals* arises from viewing the polynomial ring $\mathbb{P}[y_1, \ldots, y_n]$ as the set of all linear combinations of power products in $y_i, \ldots, y_n$ with coefficients in the ring $\mathbb{P}[y_1, \ldots, y_{i-1}]$.

2. In contrast to [9, §1.8], the *dimension* of a prime ideal not equal to the unit ideal $\mathfrak{o}$ may now be defined in the following way: The residue class ring of $\overline{\mathfrak{R}}$ modulo a prime ideal $\overline{\mathfrak{p}}$ not equal to $\mathfrak{o}$ is, by definition, a ring without zero divisors, so it can be extended to a residue class field $\overline{\mathfrak{R}}/\overline{\mathfrak{p}}$ by adjoining pairs of elements. $\overline{\mathfrak{R}}/\overline{\mathfrak{p}}$ is an extension field of a field $(\overline{\mathbb{P}})$ isomorphic to $\overline{\mathbb{P}}$. The transcendence degree $\nu$ of $\overline{\mathfrak{R}}/\overline{\mathfrak{p}}$ over $(\overline{\mathbb{P}})$ is called the *transcendence degree* or *dimension* of $\overline{\mathfrak{p}}$, and we have $0 \leq \nu \leq n$. It follows directly from [9, Theorem 5] that this definition does in fact agree with the one from [9, §1.8].

3. The definition of *fundamental ideal* can now be properly tied to the dimension of a prime ideal. The isolated component of an ideal $\mathfrak{m}$ to which every associated prime ideal of dimension $n - \varrho$ and higher belongs, and only these belong, is called the *$\varrho$-th fundamental ideal* $\mathfrak{g}_\varrho$ of $\mathfrak{m}$. It follows immediately that $\mathfrak{g}_{\varrho-1}$ is the $(\varrho - 1)$-th fundamental ideal of $\mathfrak{g}_\varrho$ and $\mathfrak{g}_\varrho$ coincides with its $\varrho$-th fundamental ideal. Ideals, for which the first fundamental ideal not equal to $\mathfrak{o}$ equals the ideal, have only associated prime ideals of a fixed dimension. By [9, Theorems 8,10], this definition for transformed ideals agrees with the one given in [9, §1.4][5], so we may refer to that one as well.

4. In addition to transformed ideals, *transformed modules and systems of equations* will also appear. A module of linear forms[6] with coefficients in $\mathbb{P}[x_1, \ldots, x_n]$ is called *transformed* if it can be made into a module of linear forms with coefficients in $\overline{\mathbb{P}}[y_1, \ldots, y_n]$ by the transformation $y = U(x)$ and the adjoining of indeterminate transformation coefficients to the field $\overline{\mathbb{P}}$. Similarly, a system of linear equations with coefficients in $\mathbb{P}[x_1, \ldots, x_n]$ is called *transformed* if it can be made into a system of linear equations with coefficients in $\overline{\mathbb{P}}[y_1, \ldots, y_n]$ by the transformation $y = U(x)$. For transformed modules and systems of equations, the existence of a nonzero determinant, whose rank agrees with that of the module or system of equations, can always be assumed to represent a regular polynomial relative to the $x_i$, $i = 1, \ldots, n$.[7]. Such a determinant will also be called a *regular determinant*.

   By [9, Lemma 1], prime and primary ideals are mapped by the transformation $y = U(x)$ to prime and primary ideals. The converse is also true. For non-transformed ideals, transformed prime and primary ideals correspond again to prime and primary ideals. Indeed, let $\mathfrak{q}$ be a transformed prime ideal, and $\overline{\mathfrak{q}}$ the corresponding non-transformed ideal. Let $\overline{a}$ and $\overline{b}$

[5]Translator's Note: Noether defines $\mathfrak{g}_i$ as the set of all polynomials $G(x)$ for which there exists a non-zero polynomial $b^{(i)}$ such that $b^{(i)}G(x) \equiv 0\ (\mathfrak{m})$. Let $E^{(i)}$ be the greatest common divisor of all such $b^{(i)}$. Then the *elementary divisor form* is the product of these $E^{(i)}$.

[6]Translator's Note: This is a *free module* in today's terminology.

[7]Translator's Note: A polynomial of degree $d$ in variables $x_1, \ldots, x_n$ is *regular in* $x_i$ if the coefficient of $x_i^d$ is non-zero. A polynomial is *regular* if it is regular in every $x_i$.

be elements of $\overline{\mathfrak{R}}$, and $a$ and $b$ the polynomials obtained from them under the transformation. Then it follows from $\overline{a}\overline{b} \equiv 0\ (\overline{\mathfrak{q}})$, $\overline{b}^{\kappa} \not\equiv 0\ (\overline{\mathfrak{q}})$ for all $\kappa$, and also from $ab \equiv 0\ (\mathfrak{q})$, $b^{\kappa} \not\equiv 0\ (\mathfrak{q})$ for all $\kappa$, that $a \equiv 0\ (\mathfrak{q})$ and consequently $\overline{a} \equiv 0\ (\overline{\mathfrak{q}})$. Therefore, $\overline{\mathfrak{q}}$ is a primary ideal. If $\mathfrak{q}$ is a prime ideal and we replace $\kappa$ in this argument with 1 accordingly, then we obtain: $\overline{\mathfrak{q}}$ is a prime ideal. Since divisibilities are retained under forward and backward transformations, associated prime and primary ideals map to associated ones, respectively. Furthermore, the dimension of a prime ideal is not changed by the transformation (see [9, footnote 12]). By [9, Lemma 2], we can transform the individual primary components in the representation of a non-transformed ideal as the least common multiple of maximal primary ideals, and thereby obtain a representation of the transformed ideal as the least common multiple of maximal primary components. By the definition of fundamental ideals, since the dimension of these components remains unchanged, the $\varrho$-th fundamental ideal of the transformed ideal is the transformed ideal of the $\varrho$-th fundamental ideal of the non-transformed ideal, so corresponding prime ideals map to each other, and similarly the isolated components of the non-transformed ideal map to those of the transformed ideals under the transformation.

Since the mapping of transformed to non-transformed ideals can be carried out in finitely many steps - inverting the transformation, partitioning the basis elements as power products of transformation coefficients - we can restrict the computation of basis elements of associated prime, primary and fundamental ideals and the isolated components of an ideal $\mathfrak{m}$ to transformed ideals.Indeed, as long as these ideals are unique, they are also transformed in $\mathfrak{m}$. The primary ideals are the only ones which are not unique. So for their computation, there is more to prove to obtain transformed ideals.

5. *The elementary divisor form of a prime ideal in perfect and imperfect fields.* The field $\mathbb{P}$ is called *perfect* if every prime function in it factors into distinct linear factors over a suitable extension field; otherwise it is called *imperfect*. We have the theorem: *The elementary divisor form of a prime ideal is a prime function, and that of a primary ideal is a power of a prime function which is the elementary divisor form of the associated prime ideal* [9, Theorem 1][8]. In a perfect field, the converse is true: *If the elementary divisor form of an ideal is a prime function, then the ideal is a prime ideal* [9, Theorem 13]. In imperfect fields, we have only: *If the elementary divisor form of a (proper or improper) ideal is a primary function, then the (proper or improper) ideal is a primary ideal.* In imperfect fields, there are proper primary ideals whose elementary divisor form is a prime function [9, §6, Example 2].

[8]Translator's Note: A *prime function* is an irreducible polynomial over $\mathbb{P}$ and a *primary function* is a power of a prime function.

## §2 Factoring Polynomials in Finitely Many Steps

Let $f(x_1, \ldots, x_n)$ be a polynomial defined over a field $\mathbb{P}$. The factorization of $f$ into prime factors in an extension field of $\mathbb{P}$ will be considered, and in particular, a factorization in finitely many steps. By the Kronecker substitution [4, Chapter 2, §§3-4]

$$x_\lambda = \xi^{d^{n-\lambda}},$$

in which $d$ must be chosen greater than the degree of $f$, a polynomial in only one variable $\xi$ can be assigned uniquely to $f$ in such a way that every factor of $f$ corresponds to a factor of this polynomial. Because of the unique assignment of the polynomials, if the number of factors of the polynomial in $\xi$ is known, then so is the number of factors of $f$. Therefore, we can restrict ourselves to factorization of polynomials in one variable. It will become evident that the feasibility of factorization depends on the nature of the field over which we wish to factor. The simplest case is the problem where the extension field is formed by adjoining finitely many algebraic and transcendental elements to the prime field. Here Kronecker's theorem holds[9]:

**Theorem 1.** *Hypothesis: Let $K$ be a prime field, $z_k$, $k = 1, \ldots, m$, be transcendental over $K(z_1, \ldots, z_{k-1}, z_{k+1}, \ldots, z_m, \alpha_1, \ldots, \alpha_l)$, and $\alpha_i$, $i = 1, \ldots, l$, be algebraic over $K(z_1, \ldots, z_m, \alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_l)$.*
*Claim: Every polynomial $f(x)$ can be factored over $K(z_1, \ldots, z_m, \alpha_1, \ldots, \alpha_l)$ into prime factors in finitely many steps.*

*Proof* (by two applications of induction). 1. $l = 0$. The case $m = 0$ must be treated separately according to when the characteristic of $K$ has the value 0, or is a prime number $p$. The proof is very simple in the second case since then $\mathbb{P} = K$ contains only finitely many elements. In the first case, the proof of the conclusion from $n - 1$ to $n$ runs completely parallel, so that they both can be brought together.

(a) First, let $m = l = 0$. If $\mathbb{P} = K$ has characteristic $p$, then it has only $p$ elements. Now if $f(x)$ has degree $r$, then we need only consider factors of polynomials of degree $q \leq \frac{r}{2}$. Since $K$ has only $p$ elements which come into question as coefficients of these polynomials, there are only $p^{\left(\left[\frac{r}{2}\right]+1\right)}$ polynomials of degree $q \leq \frac{r}{2}$, where $\left[\frac{r}{2}\right]$ denotes the largest integer $\leq \frac{r}{2}$. These polynomials can be individually tested in finitely many steps to determine whether or not they are factors of $f$.

(b) If $\mathbb{P}$ contains infinitely many elements, then either it is the prime field of characteristic 0, or $\mathbb{P} = K(z_1, \ldots, z_m)$. If $K$ is of characteristic 0, let $[K]$ be the ring lying in $K$ which is isomorphic to the ring of integers. Otherwise, let $[K] = K$. Let $[\mathbb{P}] = [K][z_1, \ldots, z_m]$. Without loss of generality, we may assume

[9] See [5]. Kronecker proved this theorem only for the case of characteristic 0, where finitely many algebraic extensions can be combined into a single one. However, the methods used there can be carried over immediately to the general case.

$f(x)$ is an element of $[\mathbb{P}][x]$. Furthermore, by well-known theorems on primitive functions, we need only consider factors of $f$ which also lie in $[\mathbb{P}][x]$.

Let $q \leq \frac{r}{2}$. We investigate the existence of a factor $\phi(x)$ of degree $q$. Let $s_0, \ldots, s_q$ be any $q+1$ distinct elements in $[K][z_1]$. If $K$ has characteristic 0, then $K$ already contains infinitely many integers, so in this case, $s_0, \ldots, s_q$ are already elements in $[K]$. Then

$$\phi(x) = \phi(s_0)g_0(x) + \ldots + \phi(s_q)g_q(x),$$

where

$$g_i(x) = \frac{(x-s_0)\cdots(x-s_{i-1})(x-s_{i+1})\cdots(x-s_q)}{(s_i-s_0)\cdots(s_i-s_{i-1})(s_i-s_{i+1})\cdots(s_i-s_q)}.$$

If $\phi(x)$ is a factor of $f(x)$, then $\phi(s_i)$ must be a factor of $f(s_i)$. But only finitely many values for $\phi(s_i)$, which will be discussed separately, come into question. If $m = 0$, then $f(s_i)$ is an integer whose finitely many divisors can be written down. Since the theorem was already proved in (1a) for prime fields of characteristic $p$, the case $m = l = 0$ is now completely settled.

Thus we may assume that the factorization of a polynomial in $[K][z_1, \ldots, z_m]$ can be achieved in finitely many steps. As an element in $[K][z_1, \ldots, z_m]$, $f(s_i)$ may now be viewed as a polynomial in $z_m$ with coefficients in $[K][z_1, \ldots, z_{m-1}]$. Therefore, by hypothesis, it can be factored into irreducible factors in finitely many steps.

2. We assume the theorem is already proved for $l-1$ algebraic extensions. Let $\alpha_l$ be algebraic over $K(z_1, \ldots, z_m, \alpha_1, \ldots, \alpha_{l-1})$. By substituting $x = y - u \cdot \alpha_l$, where $u$ denotes an indeterminate adjoined to the field and which by (1) does not affect the factorization, we find that $f(y - u\alpha_l)$ depends explicitly on $\alpha_l$. We multiply $f(y - u\alpha_l)$ by all polynomials obtained by replacing $\alpha_l$ in $f$ by its conjugates over $K(z_1, \ldots, z_m, \alpha_1, \ldots, \alpha_{l-1})$. The product is a polynomial whose coefficients lie in $K(z_1, \ldots, z_m, \alpha_1, \ldots, \alpha_{l-1})$, which then, by hypothesis, factors over this field into irreducible factors in finitely many steps. The greatest common divisor of these factors with the polynomial $f(y - u\alpha_l)$ are the factors of $f(y - u\alpha_l)$. By substituting $y = x + u\alpha_i$, we obtain the desired factors of $f(x)$, which can therefore be computed in finitely many steps. □

The case where infinitely many transcendental elements are adjoined to the prime field can be immediately reduced to the case just considered. Indeed, the polynomial can contain only finitely many of these infinitely many elements, and if we again restrict the factorization to $[\mathbb{P}][x]$, no factor can contain any transcendental element that the polynomial itself does not contain. Thus it suffices to carry out the factorization in the field formed by adjoining to the prime field the necessary algebraic elements and the finitely many transcendental elements that appear in the polynomial.

Otherwise, infinitely many algebraic elements are adjoined to the prime field. In this case, it is not true that an algebraic element not appearing in the polynomial $f(x)$ cannot appear in a factor of $f$. The methods of Kronecker's theorem

fail here. However, there is a factorization of the polynomial into linear factors that can be carried out symbolically in the algebraic closure of $\mathbb{P}$.

In any case, it is possible to factor the polynomial into prime factors over the field specified by its own coefficients, since only finitely many algebraic elements over the prime field appear among the coefficients. By Steinitz, we can now introduce symbolically a zero $j$ of such a prime function $g(x)$, so for which $g(j) = 0$, since the domain obtained by adjoining such a symbol to the coefficient field is isomorphic to the residue class field modulo the prime function, itself a field. If we apply this procedure finitely often, then we obtain a factorization of the polynomial into linear factors, in which case it is well-known that a finite extension field is sufficient. If this itself is not isomorphic to a subfield of the given field in which the factorization occurs, then at least it holds for one of the finitely many intermediate fields corresponding to the possible combinations of finitely many factors.

## §3. Computational Operations in Ideal Theory

The theorem of §3 will show how to carry out the simplest computational operations of ideal theory in finitely many steps. It deals with the formation of the least common multiple and greatest common divisor, and of products and quotients. The set of all basis elements of two ideals forms a basis of the greatest common divisor of two ideals that can be written down immediately. Similarly, the basis of the product of two ideals is easily found. It consists of the set of all products of each basis element of one ideal with each one of the other. The construction of the basis of least common multiples and quotients is harder. Hilbert's theorem[10] will provide the additional methods.

**Theorem 2** *Hypothesis. Let $f_{ij}$ be polynomials in $x_1, \ldots, x_n$ with coefficients in $\mathbb{P}$, that is elements of $\mathbb{P}[x_1, \ldots, x_n]$.*
*Claim: A complete solution for the system of equations*

$$\begin{aligned} f_{11}z_1 + \ldots + f_{1s}z_s &= 0 \\ &\vdots \\ f_{t1}z_1 + \ldots + f_{ts}z_s &= 0, \end{aligned}$$

*also consisting of elements of $\mathbb{P}[x_1, \ldots, x_n]$, can be computed in finitely many steps. If $q$ is the maximum degree of the $f_{ij}$, then the degree of the polynomials of the complete solution set does not exceed $m(t, q, n)$, where $m$ satisfies the reduction formula $m(t, q, 0) = 0$, $m(t, q, n) = qt + m(t^2q, q, n-1)$. Thus $m(t, q, n) = \sum_{i=0}^{n-1} (qt)^{2^i}$.*

[10] Macaulay hints at the possibility of using Hilbert's theorem to obtain these results.

By a *complete solution*, we mean here a set of solutions to the system of equations, on which every other solution is linearly dependent with coefficients in $\mathbb{P}[x_1, \ldots, x_n]$.

*Proof* (by induction). 1. $n = 0$. The coefficients $f_{ij}$ and the desired solutions $z_i$ are constants, elements of the field $\mathbb{P}$. As is well-known, the system of equations can be solved in this case in finitely many steps, the problem is reduced to one in determinant theory. Since no indeterminates appear at all, the degree of all polynomials is 0.

2. Assume the theorem is already proved for $n = r - 1$ $(r > 0)$. Let $n = r$.

(a) Suppose the system of equations is transformed. Without loss of generality, we may assume that there are no other linear relations among the equations, so clearly $t \leq s$. If $t = s$, then $z_1 = \ldots = z_s = 0$ is the only solution, so it forms a complete solution, and hence the theorem is proved for this case.

Thus we may assume then that $s > t$ and $t$ is the rank of

$$\begin{pmatrix} f_{11} & \ldots & f_{1s} \\ \vdots & & \vdots \\ f_{t1} & \ldots & f_{ts} \end{pmatrix}.$$

We set

$$D_{i_1 \ldots i_t} = \begin{vmatrix} f_{1i_1} & \ldots & f_{1i_t} \\ \vdots & & \vdots \\ f_{ti_1} & \ldots & f_{ti_t} \end{vmatrix}$$

where $i_1, \ldots, i_t$ denote any $t$ distinct integers in the sequence $1, \ldots, s$. Without loss of generality, we may assume that

$$D = D_{1 \ldots t} = \begin{vmatrix} f_{11} & \ldots & f_{1t} \\ \vdots & & \vdots \\ f_{t1} & \ldots & f_{tt} \end{vmatrix} \neq 0,$$

and that $D$ has the highest degree $\mu \leq qt \leq m(t, q, r)$ among all of the $D_{i_1 \ldots i_t}$ which appear. Since the system of equations is assumed to be transformed, we may assume $D$ is regular in $x_1$, *i.e.* the coefficient of $x_1^{\mu}$ in $D$ does not vanish. Then the given system of equations has the solutions

$$\begin{gathered} z_1 = D_{t+1,2 \ldots t}, \quad \ldots, \quad z_t = D_{1 \ldots t-1,t+1}, \quad z_{t+1} = D, \quad z_{t+2} = \ldots = z_s = 0 \\ \vdots \\ z_1 = D_{s2 \ldots t}, \quad \ldots, \quad z_t = D_{1 \ldots t-1,s}, \quad z_{t+1} = \ldots = z_{s-1} = 0, \quad z_s = D, \end{gathered}$$

which may be called the *canonical solutions* of the system of equations. The degree of the polynomials of these solutions do not exceed $\mu$. Because of the regularity of $D$ in $x_1$, from each solution another $\zeta_1, \ldots, \zeta_s$ is derived, for which

$$[\zeta_{t+1}]_1 < [D]_1 = \mu, \quad \ldots, \quad [\zeta_s]_1 < \mu$$

and the equations

$$\begin{aligned} l_1 &= f_{11}\zeta_1 + \ldots + f_{1s}\zeta_s &= 0 \\ &\vdots \\ l_t &= f_{t1}\zeta_1 + \ldots + f_{ts}\zeta_s &= 0 \end{aligned}$$

hold. Now let $F_{ik}$ denote the $(t-1)$-row subdeterminant of $D$ corresponding to $f_{ik}$. Then

$$\begin{aligned} 0 &= F_{11}l_1 + \ldots + F_{t1}l_t &= D\zeta_1 + D_{t+1,2\ldots t}\,\zeta_{t+1} + \ldots + D_{s2\ldots t}\,\zeta_s \\ &\vdots &\vdots \\ 0 &= F_{t1}l_1 + \ldots + F_{tt}l_t &= D\zeta_t + D_{1\ldots(t-1)(t+1)}\,\zeta_{t+1} + \ldots + D_{1\ldots t-1,s}\,\zeta_s \end{aligned}$$

Because of

$$\begin{aligned} [D_{i_1\ldots i_t}]_1 &\leq \mu \\ [\zeta_{t+\lambda}]_1 &< \mu \qquad \text{for } \lambda = 1, \ldots, s-t \\ [D]_1 &= \mu \end{aligned}$$

it follows that

$$[\zeta_i]_1 < \mu \qquad \text{for } i = 1, \ldots, t,$$

so in general

$$[\zeta_i]_1 < \mu \qquad \text{for } i = 1, \ldots, s.$$

Therefore,

$$\begin{aligned} \zeta_1 &= \xi_{11}^{(2)} x_1^{\mu-1} + \ldots + \xi_{1\mu}^{(2)} \\ &\vdots \\ \zeta_s &= \xi_{s1}^{(2)} x_1^{\mu-1} + \ldots + \xi_{s\mu}^{(2)}, \end{aligned}$$

where $\xi_{ij}^{(2)}$ are elements of $\mathbb{P}[x_2, \ldots, r]$ in accordance with the notation in §1.6. We put these expressions in the equations $l_1 = \ldots = l_t = 0$ and arrange them by powers of $x_1$. Then each of the coefficients of these powers, which still depend on $x_2, \ldots, x_r$, must vanish. Thus we obtain equations of the form

$$\begin{aligned} \phi_{11}^{(2)}\xi_{11}^{(2)} + \ldots + \phi_{1\sigma}^{(2)}\xi_{s\mu}^{(2)} &= 0 \\ &\vdots \\ \phi_{\tau 1}^{(2)}\xi_{11}^{(2)} + \ldots + \phi_{\tau\sigma}^{(2)}\xi_{s\mu}^{(2)} &= 0, \end{aligned}$$

where $[\phi_{ij}] \leq q$ and $\mu s = \sigma > \tau = \mu t \leq qt^2$. By hypothesis, since $n = r - 1$ for this system of equations, a complete solution, whose elements have degrees not exceeding $m(qt^2, q, r-1)$, can be computed in finitely many steps.

If $\overline{\xi}_{11}^{(2)}, \ldots, \overline{\xi}_{s\mu}^{(2)}$ is a solution to this system of equations, then

$$\begin{aligned} \overline{\xi}_1 &= \overline{\xi}_{11}^{(2)} x_1^{\mu-1} + \ldots + \overline{\xi}_{1\mu}^{(2)} \\ &\vdots \\ \overline{\xi}_s &= \overline{\xi}_{s1}^{(2)} x_1^{\mu-1} + \ldots + \overline{\xi}_{s\mu}^{(2)} \end{aligned}$$

is a solution to the original system of equations, and conversely, every solution of the above system of equations can be brought into the form of the canonical solution. Therefore, a complete solution to the given system of equations is constructed from the complete solution of the system of equations independent of $x_1$ formed by the indicated combinations of powers of $x_1$, together with the canonical solutions. Hence, this complete solution can be computed in finitely many steps and the degree of its solutions does not exceed $\mu + m(qt^2, q, r-1) \leq qt + m(qt^2, q, r-1) = m(t, q, r)$

(b) Suppose the system of equations is non-transformed. We transform it by $x = U(x')$ and compute the complete solutions of the transformed system by (a). Since the coefficients of the system of equations for the inverse transformation $x' = U^{-1}(x)$ are again independent of the indeterminates $u_{\mu\nu}$, the factors resulting from similar power products of the $u_{\mu\nu}$ in the inversely transformed solutions form a complete solution of the given equations. Thus in this case, they can also be computed in finitely many steps. Since the degrees of the polynomials do not grow under transformation, the degree restrictions hold here also. □

**Corollary to Theorem 2.** *If in the case $t = 1$, the coefficients $f_i$ of the given equation are homogeneous in $x_1, \ldots, x_\varrho$ $(0 \leq \varrho \leq n)$, then the polynomials appearing in the complete solution may be assumed to be homogeneous in $x_1, \ldots, x_\varrho$, and the degree restrictions of Theorem 2 remain unchanged.*

*Proof.* Let $z_1, \ldots, z_s$ be any solution to the equation, so

$$f_1 z_1 + \ldots + f_s z_s = 0.$$

Let

$$\begin{aligned} z_{11} + \ldots + z_{1j_1} &= z_1 \\ &\vdots \\ z_{s1} + \ldots + z_{sj_s} &= z_s \end{aligned}$$

be the partitioning of these polynomials into summands that are homogeneous in $x_1, \ldots, x_\varrho$, such that any two summands have different degrees in $x_1, \ldots, x_\varrho$. Thus $f_i z_{ik}$ is homogeneous in $x_1, \ldots, x_\varrho$, but $f_i(z_{ik_1} + z_{ik_2})$ is not for $k_1 \neq k_2$. If we split up the equation

$$f_1 z_1 + \ldots + f_s z_s = 0$$

into components which are homogeneous in $x_1, \ldots, x_\varrho$, but which have different degrees from each other, so that they must each vanish individually, then we obtain equations of the form

$$f_1 z_{1k_1} + \ldots + f_s z_{sk_s} = 0,$$

where there are sufficiently many such equations that each of the summands $z_{ik}$, $k = 1, \ldots, j_i$, $i = 1 \ldots, s$, appears in exactly one equation.

Therefore, the sets $z_{1k_1}, \ldots, z_{sk_s}$ are solutions of the equation. The solution $z_1, \ldots, z_s$ is linearly dependent on these; this results from summing over these solutions. By the appropriate partitioning of the solutions appearing in a complete solution, which can be computed in finitely many steps by the procedure indicated, we obtain a complete solution of the equation, consisting of polynomials homogeneous in $x_1, \ldots, x_\varrho$ and having the same maximal degree as the original solution set. □

## Application of Theorem 2

**1. Computation of the Least Common Multiple $[\mathfrak{a}, \mathfrak{b}]$ of Two Ideals $\mathfrak{a} = (f_1, \ldots, f_t)$ and $\mathfrak{b} = (g_1, \ldots, g_s)$ in Finitely Many Steps.**

We have

$$c \equiv 0 \quad ([\mathfrak{a}, \mathfrak{b}])$$

if and only if

$$c \equiv 0 \quad (\mathfrak{a}) \quad \text{and} \quad c \equiv 0 \quad (\mathfrak{b}),$$

holds, *i.e.* if

$$c = d_1 f_1 + \ldots + d_t f_t = e_1 g_1 + \ldots + e_s g_s.$$

Thus in this case

$$d_1 f_1 + \ldots + d_t f_t - e_1 g_1 - \ldots - e_s g_s = 0.$$

By Theorem 2, a complete solution of this equation can be computed. Let

$$\begin{matrix} d_{11}, \ldots, d_{1t},\ e_{11}, \ldots, e_{1s} \\ \vdots \\ d_{k1}, \ldots, d_{kt},\ e_{k1}, \ldots, e_{ks} \end{matrix}$$

be such a solution. Then

$$\begin{array}{ccccc} c_1 & = & d_{11} f_1 + \ldots + d_{1t} f_t & = & e_{11} g_1 + \ldots + e_{1s} g_s \\ \vdots & & \vdots & & \vdots \\ c_k & = & d_{k1} f_1 + \ldots + d_{kt} f_t & = & e_{k1} g_1 + \ldots + e_{ks} g_s \end{array}$$

is a basis of $[\mathfrak{a}, \mathfrak{b}]$. Therefore $[\mathfrak{a}, \mathfrak{b}] = (c_1, \ldots, c_k)$.

**2. Computation of the Quotient $\mathfrak{a} : \mathfrak{b}$.**

It is well-known that $\mathfrak{a} : \mathfrak{b} = [\mathfrak{a} : (g_1), \ldots, \mathfrak{a} : (g_s)]$. Now

$$c \equiv 0 \quad (\mathfrak{a} : (g_j))$$

if and only if

$$cg_j = d_1 f_1 + \ldots + d_t f_t,$$

so when

$$cg_j - d_1 f_1 - \ldots - d_t f_t = 0.$$

By Theorem 2, a complete solution of this equation can be computed. Let $c_{j1}, \ldots, c_{jm_j}$ be the associated factors of $g_j$ above. Then

$$\mathfrak{a} : (g_j) = (c_{j1}, \ldots, c_{jm_j}).$$

By 1, the basis of $\mathfrak{a} : \mathfrak{b} = [\mathfrak{a} : (g_1), \ldots, \mathfrak{a} : (g_s)]$ can also be computed in finitely many steps.

# §4. Degree Restrictions in Formal Divisibility Theorems

Theorem 3 now provides a criterion to help determine in finitely many steps whether or not two ideals are divisible by each other [11].

**Theorem 3.** *Hypothesis: Let $\mathfrak{M} = (l_1, \ldots, l_t)$ be a module of linear forms in $z_1, \ldots, z_s$, whose coefficients are polynomials $f_{ij}(x_1, \ldots, x_n)$ in $\mathbb{P}[x_1, \ldots, x_n]$ which are independent of $z_1, \ldots, z_s$. Let $[f_{ij}] \leq q$ and*

$$\begin{aligned} l_1 &= f_{11} z_1 + \ldots + f_{1s} z_s \\ &\vdots \\ l_t &= f_{t1} z_1 + \ldots + f_{ts} z_s. \end{aligned}$$

*Suppose $l \equiv 0$ $(\mathfrak{M})$, so that*

$$l_1 = a_1 l_1 + \ldots + a_t l_t.$$

*Claim: This representation can be chosen so that*

$$[a_i] \leq [l] + 2m(t, q, n),$$

[11] König offered such a criterion by solving the inhomogeneous equation $f_1 z_1 + \ldots + f_s z_s = f$ using the solvability of the homogeneous equation, where the induction conclusion had to be modified according to footnote 4 [Translator's Note: This is footnote 3 in this translation]. König did not produce the degree restrictions calculated in Theorem 3, which are important for what follows.

*where $m(t,q,n)$ is defined exactly as in Theorem 2.*

*Proof* (by induction). 1. $n = 0$. In this case the theorem is clear since every polynomial in which $x$ appears has degree 0. So certainly $[a_i] = [l] + 0 = 0$.

2. Assume the theorem is already proved for $n = r - 1$. Let $n = r$. Let $p$ be the rank of

$$\begin{pmatrix} f_{11} & \dots & f_{1s} \\ \vdots & & \vdots \\ f_{t1} & \dots & f_{ts} \end{pmatrix}.$$

Clearly $p \leq t$. As in Theorem 2, we set

$$\begin{vmatrix} f_{1i_1} & \dots & f_{1i_p} \\ \vdots & & \vdots \\ f_{pi_1} & \dots & f_{pi_p} \end{vmatrix} = D_{i_1 \dots i_p}$$

and assume

$$\begin{vmatrix} f_{11} & \dots & f_{1p} \\ \vdots & & \vdots \\ f_{p1} & \dots & f_{pp} \end{vmatrix} = D_{1\dots p} = D \neq 0.$$

(a) Assume $\mathfrak{M}$ is transformed so then $D$ can be assumed to be regular in $x_1$. Then

$$[D]_1 = [D] \leq qt.$$

If $F_{ij}$ denotes the $(p-1)$-row subdeterminant of $D$ corresponding to $f_{ij}$, then $\mathfrak{M}$ contains the forms

$$\begin{aligned} m_1 = F_{11}l_1 + \ldots + F_{1p}l_p \equiv 0 \quad (\mathfrak{M}) \\ \vdots \\ m_1 = F_{p1}l_1 + \ldots + F_{pp}l_p \equiv 0 \quad (\mathfrak{M}) \end{aligned}$$

and in particular,

$$\begin{aligned} m_1 &= Dz_1 + D_{p+1,2\dots p}z_{p+1} + \ldots + D_{s2\dots p}z_s \\ &\vdots \\ m_p &= Dz_p + D_{1\dots p-1,p+1}z_{p+1} + \ldots + D_{1\dots p-1,s}z_s. \end{aligned}$$

We have $[F_{ik}] \leq (t-1)q$, $[l_i] \leq q$, so $[m_i] \leq qt$, and in fact this holds for every term of the representation by the $l$'s.

Now let $g(z) = g_1z_1 + \ldots + g_sz_s$ be a linear form in $z$ with coefficients in $\mathbb{P}[x_1, \dots, x_r]$. Because of the regularity of $D$ in $x_1$, there exist polynomials $G_i$ and $j_i$ such that

$$g_i = G_i + Dj_i$$

for $i = 1, \ldots, p$, where

$$[G_i]_1 < [D]$$

and we will show that

$$[j_i] \leq [g_i] \leq [g].$$

To prove this, suppose that $[j_i] > [g_i]$. Let $j_i = j_{i1} + \ldots + j_{ik_i}$ be the partitioning of $j_i$ into homogeneous summands of different degrees, and in particular let $[j_{i1}] = [j_i]$. Let $j_{i1}^{(2)}(x_1, \ldots, x_r) \not\equiv 0$ be the coefficient of the highest power of $x_1$ appearing in $j_{i1}$. Thus $j_{i1} = j_{i1}^{(2)} x_1^{\kappa} + \ldots$ and $\left[j_{i1}^{(2)}\right] = [j_i] - \kappa$. Because of the regularity of $D$ in $x_1$,

$$D = b x_1^{[D]} + \ldots$$

where $b \neq 0$ is an element of $\mathbb{P}$. Thus

$$j_i D = f^{(2)} x_1^{\kappa + [D]} + \ldots,$$

where

$$f^{(2)} = b j_{i1}^{(2)} + \ldots$$

is a term of smaller degree. Therefore, $f^{(2)} \neq 0$ and $\left[f^{(2)}\right] = [j_i] - \kappa$. Since $[G_i]_1 < [D]$, $f^{(2)}$ is the coefficient of $x_1^{\kappa+[D]}$ in $g_i$, and $[g_i] \geq \left[x_1^{\kappa+[D]} f^{(2)}\right] = [D] + [j_i] > [D] + [g_i] \geq [g_i]$, so the assumption $[j_i] > [g_i]$ has led to a contradiction. Therefore, $[j_i] \leq [g_i]$ as claimed.

We can set

$$g(z) = G(z) + \sum_{i=1}^{p} m_i j_i$$

where

$$G(z) = G_1 z_1 + \ldots + G_p z_p + G_{p+1} z_{p+1} + \ldots + G_s z_s$$

and

$$\left[\sum_{i=1}^{p} m_i j_i\right] \leq [g] + qt \leq [g] + m(t, q, r),$$

which indeed holds for every term of the representation by the $l$'s. If $g(z) \equiv 0\ (\mathfrak{M})$, then since $m_i \equiv 0\ (\mathfrak{M})$, $G(z) \equiv 0\ (\mathfrak{M})$ as well, so by the above, we need only to prove the theorem for $G(z)$.

It follows from

$$G(z) \equiv 0 \quad (\mathfrak{M})$$

that

$$G(z) = a_1 l_1 + \ldots + a_t l_t,$$

so

$$G_i = a_1 f_{i1} + \ldots + a_t f_{tt}.$$

Since $p$ is the rank of $\mathfrak{M}$, $l_{p+\lambda}$ is linearly dependent on $l_1, \ldots, l_p$, $0 \leq \lambda \leq t-p$, provided that $\frac{1}{D}$ is allowed as a multiplier. So

$$Dl_{p+\lambda} \equiv 0 \quad (l_1, \ldots, l_p).$$

Because of the regularity of $D$ in $x_1$, we can choose the $a$'s such that

$$[a_{p+\lambda}]_1 < [D] \qquad \text{for } 0 \leq \lambda \leq t-p.$$

Now

$$\sum_{i=1}^{p} G_i F_{ik} = Da_k + \sum_{\tau=p+1}^{t} a_\tau \sum_{\pi=1}^{p} f_{\pi\tau} F_{\pi k},$$

where

$$\begin{aligned} \left[\sum f_{\pi\tau} F_{\pi k}\right] &\leq qt, \\ [a_\tau]_1 &\leq [D] \qquad \text{for } \tau = p+1, \ldots, t, \\ [G_i]_1 &\leq [D] \qquad \text{for } i = 1, \ldots, p, \\ [F_{ik}] &\leq q(t-1), \end{aligned}$$

so

$$[a_k]_1 \leq qt \quad \text{for } k = 1, \ldots, t,$$

*i.e.*

$$[a_k]_1 \leq 2m(t, q, 1).$$

Therefore the theorem is proved for $r = 1$. Let $r > 1$. Then

$$G(z) \equiv 0 \ (\mathfrak{B}),$$

where

$$\mathfrak{B} = (l_1, x_1 l_1, \ldots, x_1^{qt} l_1,\ l_2, \ldots, x_1^{qt} l_t)$$

is a module of linear forms in $z_1, x_1 z_1, \ldots, x_1^{qt} z_1, \ldots, x_1^{qt} z_s$ with coefficients in $\mathbb{P}[x_2, \ldots, x_r]$. The number $T$ of basis elements of $\mathfrak{B}$ is $qt^2$. Since the coefficients of $\mathfrak{B}$ depend only on $r-1$ variables, there is by hypothesis a representation

$$G(z) = a_1^{(2)} l_1 + \ldots + a_T^{(2)} x_1^{qt} l_t,$$

where

$$\left[a_i^{(2)}\right] \leq [G] + 2m(qt^2, 1, r-1)$$

holds. Now since

$$g = G + \sum_{i=1}^{p} m_i j_i$$

and

$$\left[\sum_{i=1}^{p} m_i j_i\right] \leq [g] + qt,$$

we have

$$[G] \leq [g] + qt.$$

Therefore,

$$\left[a_i^{(2)}\right] \leq [g] + qt + 2m(qt^2, q, r-1).$$

If we order the representation of $G(z)$ by the $l$'s

$$G(z) = a_1 l_1 + \ldots + a_t l_t,$$

then

$$[a_i] \leq \max\left[a_k^{(2)}\right] + qt,$$

*i.e.*

$$[a_i] \leq [g] + 2qt + 2m(qt^2, q, r-1) = [g] + 2m(t, q, r).$$

(b) Suppose $\mathfrak{M}$ is non-transformed. The theorem holds for the corresponding transformed module. Since inverting the transformation does not raise the degrees, the theorem holds for non-transformed modules as well. □

## Application of Theorem 3

### Criterion for the Divisibility of Two Ideals by Each Other

If we set $s = 1$ and drop $z_1$ which appears as a factor in every element of $\mathfrak{M}$, then $\mathfrak{M}$ reduces to an ideal $\mathfrak{m} = (f_1, \ldots, f_t)$ of polynomials in $x_1, \ldots, x_n$, and the theorem reads: *If $g \equiv 0$ $(\mathfrak{m})$, then there is a representation*

$$g = g_1 f_1 + \ldots + g_t f_t,$$

*where*

$$[g_i] \leq [g] + 2m(t, q, n).$$

So if we also assume that the $g_i$ are polynomials of degree $[g] + 2m(t, q, n)$ with indeterminate coefficients, then the equations, which arise by comparing coefficients from the equation $g = \sum_{i=1}^{t} f_i g_i$, must be solvable. Conversely, if they are solvable, then $g \equiv 0$ $(\mathfrak{m})$. The system of equations in question, on whose solvability we therefore depend, is now linear in the unknowns. By determinant theory methods, the solvability can then be decided in finitely many steps. Thus we can decide in finitely many steps whether or not each individual polynomial in $\mathbb{P}[x_1, \ldots, x_n]$ is divisible by $\mathfrak{m}$. Now since for the divisibility of an ideal by another it is necessary and sufficient that the basis elements of the first be

divisible by the second, a criterion for the divisibility of an ideal by another is easily produced.

It will be important later to completely ignore exceeding the degree. Theorem 4 will show that there is in fact an ideal basis, for which this is possible.

**Theorem 4.** *For every ideal* $\mathfrak{m} = (f_1, \ldots, f_t)$*, there exists a canonical basis* $f_{\varrho 1}, \ldots, f_{\varrho t_\varrho}$*,* $\varrho = 1, \ldots, n$*, such that for every* $g \equiv 0\ (\mathfrak{m})$*, there exists a representation*

$$g = \sum_{i=1}^{t_\varrho} g_i f_{\varrho i},$$

*where*

$$[g_i]_\varrho = [g]_\varrho - [f_{\varrho i}]_\varrho$$

*for* $g_i \neq 0$*. This basis can be computed in finitely many steps, and* $[f_{pi}] \leq m(1, q, n) = \sum_{i=1}^{n-1} q^{2^i}$*.*

*Proof.* We set

$$\overline{f}_\tau(x_0, x_1, \ldots, x_n) = x_0^{[f_\tau]_\varrho} f_\tau\left(\frac{x_1}{x_0}, \ldots, \frac{x_\varrho}{x_0}, x_{\varrho+1}, \ldots, x_n\right)$$

so that $\overline{f}_\tau$ is homogeneous in $x_0, x_1, \ldots, x_\varrho$. Let $g \equiv 0\ (M)$ and

$$\overline{g}(x_0, x_1, \ldots, x_n) = x_0^{[g]_\varrho} g\left(\frac{x_1}{x_0}, \ldots, \frac{x_\varrho}{x_0}, x_{\varrho+1}, \ldots, x_n\right).$$

By Theorem 3, there exists a representation

$$g = c_1 f_1 + \ldots + c_t f_t$$

such that

$$[c_i] \leq [g] + 2m(t, q, n).$$

Consequently,

$$x_o^k \overline{g} = \sum_{i=1}^{t} x_0^{k_i} \overline{c}_i \overline{f}_i,$$

where the $\overline{c}_i$ are formed analogously to $\overline{f}_i$ and $\overline{g}_i$, and the $k_i$ can be chosen so that the exponent $k_i = 0$ for at least one $i$, and

$$k \leq q + 2m(t, q, n).$$

Therefore,

$$x_0^{2m+q} \overline{g} \equiv 0 \quad (\overline{f}_1, \ldots, \overline{f}_t) \qquad \text{in } \mathbb{P}[x_0, x_1, \ldots, x_n].$$

Conversely, if this congruence holds, then we obtain $g \equiv 0\ (M)$ by setting $x_0 = 1$.

Hence by the methods presented in Theorem 2, we form a complete solution to the equation

$$x_0^{2m+q}\mathfrak{X} - \overline{c}_1\overline{f}_1 - \ldots - \overline{c}_t\overline{f}_t = 0,$$

which may be assumed to be homogeneous in $x_0, x_1, \ldots, x_\varrho$ by the Corollary to Theorem 2, and where we let $\mathfrak{X} = \overline{f}_{\varrho 1}, \ldots, \mathfrak{X} = \overline{f}_{\varrho t_\varrho}$. Thus

$$[\overline{f}_{\varrho i}] \leq m(1, q, n) = \sum_{i=0}^{n-1} q^{2^i}.$$

Let

$$g \equiv 0 \ (M),$$

so

$$\overline{g} = \sum_{i=1}^{t_\varrho} \overline{g}_i \overline{f}_{\varrho i},$$

where, without loss of generality, we may assume that the $\overline{g}_i$ are homogeneous in $x_1, \ldots, x_\varrho$. Since all members of this equation are homogeneous in $x_0, x_1, \ldots, x_\varrho$, the $\overline{g}_i$ can be chosen such that

$$[\overline{g}_i]_\varrho = [\overline{g}]_\varrho - [\overline{f}_{\varrho i}]_\varrho$$

provided $g_i \neq 0$.

Now if we set $x_0 = 1$, and thereby derive $f_{\varrho i}$ from $\overline{f}_{\varrho i}$, then

$$\mathfrak{m} = (f_{\varrho 1}, \ldots, f_{\varrho t_\varrho})$$

with

$$[\overline{f}_{\varrho i}] \leq \sum_{i=0}^{n-1} q^{2^i},$$

and it follows from

$$g \equiv 0 \pmod{\mathfrak{m}}$$

that

$$g = \sum_{i=1}^{t_\varrho} g_i f_{\varrho i},$$

where

$$[g_i]_\varrho = [g]_\varrho - [f_{\varrho i}]_\varrho$$

provided $g_i \neq 0$. □

# §5. The Hentzelt Nullstellensatz

In contrast to the purely formal divisibility criterion of Theorem 3, Hentzelt's Nullstellensatz brings a criterion which indicates how strongly a polynomial must vanish at the zeros of an ideal in order to be divisible by the ideal. To prove this theorem, three lemmas are needed.

In the lemmas, it must be assumed that the underlying field $\overline{\mathbb{P}}$ [§1.1], in which the ideals and modules appear, have infinitely many elements. This condition is certainly satisfied if we replace $\overline{\mathbb{P}}$ with $\overline{\mathbb{P}}(s)$, where $s$ is transcendental over $\overline{\mathbb{P}}$. Therefore in the lemmas, $\overline{\mathbb{P}}$ will contain infinitely many elements. It will be shown that adjoining $s$ is not a restriction of Hentzelt's Nullstellensatz.

**Lemma 1.** *Hypothesis: Let* $\mathfrak{m} = (l_1, \ldots, l_t)$ *be a module of linear forms*

$$\begin{aligned} l_1 &= f_{11}z_1 + \ldots + f_{1s}z_s \\ &\vdots \\ l_t &= f_{t1}z_1 + \ldots + f_{ts}z_s \end{aligned}$$

*with* $[f_{ij}] \leq q$. *Let* $p$ *be the rank of* $\mathfrak{m}$.
*Claim: After a homogeneous linear transformation* $x = U'(x')$ *of* $x_1, \ldots, x_n$ *with transformation coefficients in* $\overline{\mathbb{P}}$, *and having a nonzero determinant, we have: If* $\mathfrak{G}_n$ *is the set of all linear forms* $g$ *for which there exists a polynomial* $k(x'_n) \neq 0$ *dependent only on* $x'_n$ *such that* $k(x'_n)g \equiv 0\ (\mathfrak{M})$, *then there exists a polynomial* $K(x'_n) \neq 0$ *dependent only on* $x'_n$ *such that*

1. $K(x'_n)\mathfrak{G}_n \equiv 0 \quad (\mathfrak{M})$
2. $[K(x'_n)] \leq M(t, q, n)$

*where*

$$\begin{aligned} M(t, q, 1) &= qt \\ M(t, q, n) &= M(qt^2, q, n-1). \end{aligned}$$

*Therefore,*

$$M(t, q, n) = (qt)^{2^{n-1}}.$$

*Proof* (by induction.) 1. $n = 1$. $\mathfrak{G}_1 = \mathfrak{G}$ is the fundamental module for $\mathfrak{M}$ [12]. Let

$$D = \begin{vmatrix} f_{11} & \ldots & f_{1p} \\ \vdots & & \vdots \\ f_{p1} & \ldots & f_{pp} \end{vmatrix} \neq 0.$$

[12] The definition of fundamental module is given in [9,§1.5].

By [2, Theorem 3],

$$D\mathfrak{G} \equiv 0 \quad (\mathfrak{M})$$

so

$$[D]_1 \leq [D] \leq qt = M(t, q, 1).$$

2. Suppose the theorem is already proved for $n = r - 1$. Let $n = r > 1$. Since $\overline{\mathbb{P}}$ consists of infinitely many elements, we can always cause $D$ to be regular in $x_1'$ by a transformation that satisfies the conditions specified in the claim. In order to simplify notation in what follows, the accents on $x$ will be omitted. Let

$$k(x_r)g \equiv 0 \quad (\mathfrak{M}).$$

As in Theorem 3, we set

$$g = g_1 z_1 + \ldots + g_s z_s$$

and

$$g_i = G_i + Dj_i,$$

so that

$$\begin{aligned} [G_i]_1 &\leq [D] \leq qt \\ [j_i] &\leq [g_i] \leq [g]. \end{aligned}$$

Then

$$g = G + \sum_{i=1}^{p} m_i j_i,$$

where the $m_i$ have the same meaning as in Theorem 3. Because $m_i \equiv 0$ $(\mathfrak{M})$,

$$k(x_r)G \equiv 0 \quad (\mathfrak{M}).$$

Thus

$$[k(x_r)G_i]_1 \leq qt \qquad \text{for } i = 1, \ldots, p.$$

Let

$$k(x_r)G = a_1 l_1 + \ldots + a_t l_t.$$

Then we can show, just as in Theorem 3, that

$$[a_i]_1 \leq qt \qquad \text{for } i = 1, \ldots, t.$$

Thus

$$k(x_r)G \equiv 0 \quad (\mathfrak{B}),$$

where $\mathfrak{B}$ again denotes the module of linear forms $(l_1, \ldots, l_t, \ldots, x_1^{qt} l_t)$ whose coefficients are polynomials in $x_2, \ldots, x_r$. Therefore, after a transformation of $x_2, \ldots, x_r$ which can be combined with the first, there exists, by hypothesis, a polynomial $K(x_r)$ independent from the choice of $g$, such that

$$K(x_r)G \equiv 0 \quad (\mathfrak{B})$$

and

$$[K(x_r)] \leq M(qt^2, q, r-1).$$

Furthermore,

$$K(x_r)G \equiv 0 \quad (\mathfrak{M}),$$

so

$$K(x_r)g \equiv 0 \quad (\mathfrak{M}).$$

Hence

$$K(x_r)\mathfrak{G}_r \equiv 0 \quad (\mathfrak{M}),$$

so

$$[K(x_r)] \leq M(qt^2, q, r-1) = M(t, q, r). \quad \square$$

**Corollary 1 to Lemma 1.** *If $\mathfrak{M}$ is transformed, then the claim holds without applying the specific transformation.*

*Proof.* Let $\mathfrak{M}$ be the result of $y = U(x)$ to $\overline{\mathfrak{M}}$. $\mathfrak{M}$ maps on $\mathfrak{M}'$ by $x = U'(x')$. Thus $\mathfrak{M}'$ is the result of the composite transformation $y = UU'(x') = V(x')$ on $\overline{\mathfrak{M}}$. Hence the equations

$$V = UU', \qquad U = VU'^{-1}$$

hold between the transformation matrices, so since $U'$ has a nonzero determinant, the transformation is uniquely invertible. Using these equations, the elements of $V$ and those of $U$ can be expressed linearly with coefficients in $\overline{\mathbb{P}}$ in terms of each other. So the elements of $U$, as well as the elements of $V$ are indeterminates, and the fields $\overline{\mathbb{P}}(u)$ and $\overline{\mathbb{P}}(v)$ coincide. Therefore, $\mathfrak{M}'$ is also the associated transformed module of $\overline{\mathfrak{M}}$, so $\mathfrak{M}'$ and $\mathfrak{M}$ are isomorphic and they differ only in notation. If we replace $x'$ by $x$ in $\mathfrak{M}'$ and $V$ by $U$, then $\mathfrak{M}'$ maps to $\mathfrak{M}$. Since the theorem is proved for $\mathfrak{M}'$, it is also true for $\mathfrak{M}$. $\square$

**Corollary 2 to Lemma 1.** *For transformed ideals in the special case $s = 1$, the theorem provides an upper bound on the degree of the $n$-th level elementary divisors.*[13]

*Proof.* In this case $\mathfrak{M}$ maps to an ideal $\mathfrak{m}$ because the factor $z_1$, which appears unnecessarily in every element, can be cancelled. Let $\mathfrak{M}$ and hence $\mathfrak{m}$ be transformed. Then $\mathfrak{G}_n$ maps to the $(n-1)$-th fundamental ideal $\mathfrak{g}_{n-1}$ of $\mathfrak{m}$. Now if $E(x_n)$ is an $n$-th level elementary divisor of $\mathfrak{m}$, then $E(x_n)$ is the greatest common divisor of every $K(x_n)$ for which

$$K(x_n)\mathfrak{g}_{n-1} \equiv 0 \quad (\mathfrak{m})$$

holds [9, §1.5]. Therefore, by Lemma 1 and the first corollary,

$$[E(x_n)] \leq M(t, q, n). \quad \square$$

[13]Translator's Note: This is just $E^{(n)}$ as defined in footnote 5.

**Lemma 2.** *Hypothesis: Let $\xi_{\varrho+1}, \ldots, \xi_n$ be any elements lying in an extension field of $\overline{\mathbb{P}}$, perhaps adjoined to the field $\overline{\mathbb{P}}$. Let the following ideals be defined:*

$$\begin{aligned} \mathfrak{m} &= (f_1, \ldots, f_t), \qquad q \geq [f_i] \quad \text{for } i = 1, \ldots, t \\ \mathfrak{d} &= \left((x_{\varrho+1} - \xi_{\varrho+1})^{e_{\varrho+1}}, \ldots, (x_n - \xi_n)^{e_n}\right) \\ \mathfrak{a} &= (\mathfrak{m}, \mathfrak{d}) \end{aligned}$$

*Claim: After a homogeneous linear transformation $x = U'(x')$ of the form*

$$\begin{array}{rcccccc} x_1 &=& u_{11}x'_1 + \ldots + u_{1\varrho}x'_\varrho & & & & \\ &\vdots& \vdots & & & & \\ x_\varrho &=& u_{\varrho 1}x'_1 + \ldots + u_{\varrho\varrho}x'_\varrho & & & & \\ x_{\varrho+1} &=& & x'_{\varrho+1} & & & \\ &\vdots& \vdots & & \ddots & & \\ x_n &=& & & & x'_n & \end{array}$$

*with coefficients from $\overline{\mathbb{P}}$ and a nonzero determinant: If $\mathfrak{g}_\varrho$ denotes the set of all polynomials $g$ for which there exists a polynomial $k(x'_\varrho)$ dependent only on $x'_\varrho$ such that $k(x'_\varrho)g \equiv 0\ (\mathfrak{a})$, $k \neq 0$, then there exists a polynomial $K(x'_\varrho)$ dependent only on $x'_\varrho$, such that*

1. $K(x'_\varrho)\mathfrak{g}_\varrho \equiv 0 \quad (\mathfrak{a})$
2. $[K(x'_\varrho)] \leq N\left(t, q, \varrho, \prod_{i=\varrho+1}^{n} e_i\right)$,

*where*

$$N\left(t, q, \varrho, \prod_{i=\varrho+1}^{n} e_i\right) = M\left(t \prod_{i=\varrho+1}^{n} e_i,\ \ q,\ \ \varrho\right) = \left(qt \prod_{i=\varrho+1}^{n} e_i\right)^{2^{\varrho-1}}.$$

*Proof.* Let $X_\mu$, $\mu = 1, \ldots, S$, $S = \prod e_i$, be the power products of $(x_{\varrho+1} - \xi_{\varrho+1}), \ldots, (x_n - \xi_n)$ where the exponent of $(x_i - \xi_i)$ is less than $e_i$. Set

$$f_\kappa X_\mu \equiv \sum_{\sigma=1}^{S} X_\sigma f_{\sigma\tau_{\kappa\mu}}(x_1, \ldots, x_\varrho) \quad (\mathfrak{d}) \qquad \begin{array}{rcl} \kappa &=& 1, \ldots, t \\ \mu &=& 1, \ldots, S \\ \tau_{\kappa\mu} &=& 1, \ldots, tS. \end{array}$$

If $i$ is one of the numbers $1, \ldots, tS$, then let

$$l_i = X_1 f_{1i} + \ldots + X_S f_{Si}.$$

Then $\mathfrak{M} = (l_1, \ldots, l_{tS})$ is the module of linear forms which maps to $\mathfrak{m}$ modulo $\mathfrak{d}$. $\mathfrak{M}$ will be transformed in the manner indicated by Lemma 1. The accent

on the $x$'s will again be omitted. Since the coefficients $\mathfrak{M}$ are just polynomials in $x_1, \ldots, x_\varrho$, the transformation applies only to $x_1, \ldots, x_\varrho$. Using the identity transformation on $x_{\varrho+1}, \ldots, x_n$, it can be extended to $x = U'(x')$. Then by Lemma 1, there exists a polynomial $K(x_\varrho)$ dependent only on $x_\varrho$ such that

$$K(x_\varrho)\mathfrak{G}_\varrho \equiv 0 \ (\mathfrak{M})$$

and

$$[K(x_\varrho)] \leq M(tS, q, \varrho) = N(t, q, \varrho, S).$$

If we again view the elements of $\mathfrak{G}_\varrho$ and $\mathfrak{M}$ as polynomials in $x_1, \ldots, x_n$, then

$$(\mathfrak{G}_\varrho, \mathfrak{d}) = (\mathfrak{g}_\varrho, \mathfrak{d})$$
$$(\mathfrak{M}, \mathfrak{d}) = (\mathfrak{m}, \mathfrak{d}) = \mathfrak{a}.$$

Thus

$$K(x_\varrho)(\mathfrak{g}_\varrho, \mathfrak{d}) \equiv 0 \quad (\mathfrak{a}),$$

so

$$K(x_\varrho)\mathfrak{g}_\varrho \equiv 0 \quad (\mathfrak{a})$$

all the more. □

**Corollary to Lemma 2.** *If $\mathfrak{m}$ is transformed, then the claim is true without applying the specific transformation.*

*Proof.* Let $\mathfrak{m}$ be the result of the transformation $y = U(x)$ on $\overline{\mathfrak{m}}$. Let $\mathfrak{m}'$, $\mathfrak{a}'$, and $\mathfrak{d}'$ come from $\mathfrak{m}$, $\mathfrak{a}$, and $\mathfrak{d}$ via $x = U'(x')$, $\mathfrak{a}' = (\mathfrak{m}', \mathfrak{d}')$. Now since, in the basis elements of $\mathfrak{d}'$, only $x_{\varrho+1}, \ldots, x_n$ appear , which are simply transformed by the identity, $\mathfrak{d}$ and $\mathfrak{d}'$ are isomorphic. The same is true for $\mathfrak{m}$ and $\mathfrak{m}'$ because $\mathfrak{m}$ is transformed, as was proved in the Corollary to Lemma 1. Furthermore, since the isomorphism in both cases consists of interchanging $x$ with $x'$ and the elements of $U$ with those of $UU'$, $\mathfrak{a}$ and $\mathfrak{a}'$ are also isomorphic. Since the theorem is already proved for $\mathfrak{a}'$, it holds for $\mathfrak{a}$ as well. □

**Lemma 3.** *Hypothesis: Let*

$$\mathfrak{m} = \big(f_1(x_1, \ldots, x_n, y), \ldots, f_t(x_1, \ldots, x_n, y)\big)$$

*be an ideal in $\mathbb{P}(y)[x_1, \ldots, x_n]$, where $y$ is transcendental over $\mathbb{P}[x_1, \ldots, x_n]$. Let $\mathfrak{m}_\xi = \big(f_1(x_1, \ldots, x_n, \xi), \ldots, f_t(x_1, \ldots, x_n, \xi)\big)$ be the ideal in $\mathbb{P}[x_1, \ldots, x_n]$ formed by substituting an element $\xi$ in $\mathbb{P}$ for $y$ in $\mathfrak{m}$. Let $k(x_1, \ldots, x_n, y) \not\equiv 0 \ (\mathfrak{m})$. Without loss of generality, the polynomials $f_i$, $i = 1, \ldots, t$, and $k$ may be assumed to be integral in $y$, so that for all $\xi$ in $\mathbb{P}$, the polynomials $f_i(x_1, \ldots, x_n, \xi)$ and $k(x_1, \ldots, x_n, \xi)$ are defined.*
*Claim: There exists $\xi$ in $\mathbb{P}$ such that*

$$k(x_1, \ldots, x_n, \xi) \not\equiv 0 \quad (\mathfrak{m}_\xi).$$

*Proof.* 1. *The connection between questions of divisibility and rank.*

Let

$$g(x_1, \ldots, x_n, y) \equiv 0 \quad (\mathfrak{m}).$$

By Theorem 3, there exists a representation

$$\begin{aligned} g(x_1, \ldots, x_n, y) &= \phi_1(x_1, \ldots, x_n, y) f_1(x_1, \ldots, x_n, y) + \ldots \\ &\quad + \phi_t(x_1, \ldots, x_n, y) f_t(x_1, \ldots, x_n, y) \end{aligned}$$

such that $[\phi_i] \leq [g] + 2m(t, q, n)$, where $q$ is again the maximal degree of the $f_i(x_1, \ldots, x_n, y)$ in $x_1, \ldots, x_n$.

Let $z_\sigma$, $\sigma = 1, \ldots, s$, be the distinct power products of $x_1, \ldots, x_n$ for which $[z_\sigma] \leq [g] + q + 2m(t, q, n)$. Let $\zeta_\varrho$, $\varrho = 1, \ldots, r$, be the distinct power products for which $[\zeta_\varrho] \leq [g] + 2m(t, q, n)$.

Because of the degree restrictions on the individual terms of the representation of $g$, we can bring this representation into the form

$$G(z_1, \ldots, z_s, y) = \overline{\phi}_1(y) F_1(z_1, \ldots, z_s, y) + \ldots + \overline{\phi}_{tr}(y) F_{tr}(z_1, \ldots, z_s, y),$$

where $G(z_1, \ldots, z_s, y) = g(x_1, \ldots, x_n, y)$, the $F_i(z_1, \ldots, z_s, y)$ are of the form $\zeta_\varrho f_k(x_1, \ldots, x_n, y)$, and the $F_i$ and $G$ are linear in $z_1, \ldots, z_s$. Now since $G$ depends linearly on the $F_i$, the matrices

$$A = \begin{pmatrix} g_1(y) & f_{11}(y) & \ldots & f_{1,tr}(y) \\ \vdots & \vdots & \ldots & \vdots \\ g_s(y) & f_{s1}(y) & \ldots & f_{s,tr}(y) \end{pmatrix} \text{ and } B = \begin{pmatrix} f_{11}(y) & \ldots & f_{1,tr}(y) \\ \vdots & \ldots & \vdots \\ f_{s1}(y) & \ldots & f_{s,tr}(y) \end{pmatrix}$$

have the same rank, where $g_i$ and $f_{ij}$ denote the coefficients of $z_i$ in $G$ and $F_j$, respectively.

On the other hand, if both of these matrices have the same rank, then $G$ is linearly dependent on the $F_i$. If we again replace the $z_\sigma$ in $G$ and $F_i$ by the power products of $x_1, \ldots, x_n$, then we get $g \equiv 0$ $(\mathfrak{m})$. Therefore, the two matrices have the same rank if and only if $g$ is divisible by $\mathfrak{m}$. These same observations hold if we set $y$ equal to an element $\xi$ of $\mathbb{P}$. Then polynomials $\phi_{\xi i}(x_1, \ldots, x_n)$ satisfying the same degree restrictions in $x_1, \ldots, x_n$ take the place of $\phi_i(x_1, \ldots, x_n, y)$. Therefore, it is also true that $g(x_1, \ldots, x_n, \xi)$ is divisible by $\mathfrak{m}_\xi$ if and only if the two matrices formed by the substitution $y = \xi$ in $A$ and $B$ have the same rank.

2. Because $k(x_1, \ldots, x_n, y) \not\equiv 0$ $(\mathfrak{m})$, the matrices $A'$ and $B'$, formed from $k(x_1, \ldots, x_n, y)$ analogously to the matrices $A$ and $B$ , have different rank. Thus there is a non-zero determinant in $A'$ whose rank is 1 higher than that of $B'$. Now since $\mathbb{P}$ consists of infinitely many elements, $y$ can be specialized to $\xi$ in $\mathbb{P}$ in such a way that these determinants remain nonzero. If we replace $y$ by this $\xi$ in $A'$ and $B'$, then they retain different ranks. Therefore,

$$k(x_1, \ldots, x_n, \xi) \not\equiv 0 \quad (\mathfrak{m}). \qquad \square$$

With Lemmas 2 and 3, Hentzelt's Nullstellensatz can now be proved.

**Definition 1.** By a *complete zero-set* of an ideal $\mathfrak{m}$, we mean a set of one zero of each transcendence degree from each associated prime ideal of $\mathfrak{m}$.

**Definition 2.** If $\xi_1^{(i)}, \ldots, \xi_n^{(i)}$, $i = 1, \ldots, m$, is a complete zero-set of $\mathfrak{m}$, then $\mathfrak{o}_i = \left(x_1 - \xi_1^{(i)}, \ldots, x_n - \xi_n^{(i)}\right)$ is called the associated *zero-set ideal* of $\mathfrak{m}$.

It follows from the definition that $\mathfrak{o}_i$ is a prime ideal in

$$\mathfrak{R}_i = \mathfrak{R}\left(\xi_1^{(i)}, \ldots, \xi_n^{(i)}\right) = \mathbb{P}\left(\xi_1^{(i)}, \ldots, \xi_n^{(i)}\right)[x_1, \ldots, x_n].$$

**Theorem 5 (Hentzelt's Nullstellensatz).** *Hypothesis: Let $\xi_1^{(i)}, \ldots, \xi_n^{(i)}$, $i = 1, \ldots, m$, be a complete zero set of $\mathfrak{m} = (f_1, \ldots, f_t)$. Let $\mathfrak{o}_i$, $i = 1, \ldots, m$, be the corresponding zero-set ideal. Let $q$ be the maximal degree of $f_1, \ldots, f_t$. Let*

$$\kappa(t, q, n) = q + \prod_{\lambda=1}^{n} \left[(qt)^{2^{\lambda-1} \prod_{i=1}^{n-\lambda} (2^{n-i}+1)} - 1\right] = q + v(t, q, n).$$

*Claim: It follows from*

$$g \equiv 0 \quad (\mathfrak{m}, \mathfrak{o}_i^\kappa) \quad \textit{in} \quad \mathfrak{R}_i = \mathfrak{R}\left(\xi_1^{(i)}, \ldots, \xi_n^{(i)}\right) \quad (\textit{for } i = 1, \ldots, m)$$

*that*

$$g \equiv 0 \quad (\mathfrak{m}).$$

In the following second version, Hentzelt states the theorem only for algebraic zeros.

**Theorem 5a.** *Hypothesis: Let $\xi_1, \ldots, \xi_n$ be an arbitrary set of values in the algebraic closure of $\mathbb{P}$. Let*

$$\mathfrak{a} = (x_1 - \xi_1, \ldots, x_n - \xi_n).$$

*Claim: It follows from*

$$g \equiv 0 \quad (\mathfrak{m}, \mathfrak{o}_i^\kappa)$$

*that for every such set of values,*

$$g \equiv 0 \quad (\mathfrak{m}).$$

If $\xi_1, \ldots, \xi_n$ is not an algebraic zero of $\mathfrak{m}$, then $(\mathfrak{m}, \mathfrak{a}^\kappa) = \mathfrak{o}$, so clearly $g \equiv 0$ $(\mathfrak{m}, \mathfrak{o}_i^\kappa)$. So instead of the condition "for every arbitrary set of values", we can also use "for every algebraic zero of $\mathfrak{m}$".

*Proof.* Both versions of the theorem will be proved. A few preparatory remarks are needed for the proof.

1. Without loss of generality, it may be assumed that the underlying field $\overline{\mathbb{P}}$ has infinitely many elements. The theorem will be proved for this specific case. Let $\mathfrak{m}$ be defined in $\mathfrak{R} = \mathbb{P}[x_1, \ldots, x_n] = \overline{\mathbb{P}}(u_{11}, \ldots, u_{nn})[x_1, \ldots, x_n]$, where $\overline{\mathbb{P}}$ contains only finitely many elements. Suppose $\overline{\mathbb{P}}' = \overline{\mathbb{P}}(s)$, where $s$ is transcendental over $\overline{\mathbb{P}}$. Let $\mathfrak{m}'$ be defined in $\mathfrak{R}' = \mathbb{P}'[x_1, \ldots, x_n] = \overline{\mathbb{P}}'(u_{11}, \ldots, u_{nn})[x_1, \ldots, x_n]$ with the same basis as $\mathfrak{m}$. Then the zeros of $\mathfrak{m}$ and $\mathfrak{m}'$ coincide. Thus a polynomial $g$ in $\mathfrak{R}$ that satisfies the hypothesis of Theorems 5 and 5a for $\mathfrak{m}$ satisfies it for $\mathfrak{m}'$ as well. So by hypothesis

$$g \equiv 0 \quad (\mathfrak{m}').$$

Therefore, there exists a polynomial $k(s)$ in $\mathbb{P}(s)$ whose lowest coefficient may be assumed to be the identity $E$ of $\mathbb{P}$, such that

$$k(s)g = g_1 f_1 + \ldots + g_t f_t,$$

where the $g_i$ are integral in $s$. By comparing coefficients of the smallest power of $s$ appearing in $k$, we obtain

$$g = g_1' f_1 + \ldots + g_t' f_t$$

with $g_i' \equiv 0\ (\mathfrak{R})$. But that means $g \equiv 0\ (\mathfrak{m})$.

2. We already have

$$\kappa(t, q, n) \geq \kappa(t, q, n-1).$$

In particular, if $t = q = 1$, then

$$v(1, 1, n) = v(1, 1, n-1) = 0,$$

so

$$\kappa(1, 1, n) = \kappa(1, 1, n-1) = 1.$$

Let $qt \geq 2$. If we separate the last factor of $v(t, q, n)$, then we obtain the equation

$$\begin{aligned} v(t, q, n) &= \prod_{\lambda=1}^{n} \left[ (qt)^{2^{\lambda-1} \prod_{i=1}^{n-\lambda} (2^{n-i}+1)} - 1 \right] \left[ (qt)^{2^{n-1}} - 1 \right] \\ &= v_1(t, q, n) \left[ (qt)^{2^{n-1}} - 1 \right] \geq v_1(t, q, n) \end{aligned}$$

since $qt \geq 2$. Furthermore, because

$$\prod_{i=1}^{n-\lambda} (2^{n-i} + 1) \geq \prod_{i=1}^{n-\lambda-1} (2^{n-i-1} + 1),$$

it follows that

$$v_1(t,q,n) \geq v_1(t,q,n-1).$$

Hence

$$v(t,q,n) \geq v(t,q,n-1),$$

so

$$\kappa(t,q,n) \geq \kappa(t,q,n-1).$$

3. Let $l \geq \prod_{\lambda=1}^{n}(l_\lambda - 1)$, then

$$\mathfrak{a}^l \equiv 0 \quad \big((x_1-\xi_1)^{l_1},\ldots,(x_n-\xi_n)^{l_n}\big).$$

In particular,

$$\mathfrak{a}^l = \left((x_1-\xi_1)^l, \quad \ldots, \quad \prod_{\substack{\lambda=1 \\ \varepsilon_1+\ldots+\varepsilon_n=l}}^{n} (x_\lambda-\xi_\lambda)^{\varepsilon_\lambda}, \quad \ldots, \quad (x_n-\xi_n)^l\right).$$

For $\sum_{\lambda=1}^{n}\varepsilon_\lambda = l$ in general,

$$\prod_{\lambda=1}^{n}(x_\lambda-\xi_\lambda)^{\varepsilon_\lambda} \equiv 0 \quad \big((x_1-\xi_1)^{l_1},\ldots,(x_n-\xi_n)^{l_n}\big).$$

For the proof, some further notation must be defined.

4. Let $E_n(x_n)$ be the $n$-th level elementary divisor of $\mathfrak{m}$ [9, §1.6] and $l_n$ be an integer $\geq [E_n(x_n)]$. By Corollary 2 of Lemma 1, we can set

$$l_n = (qt)^{2^{n-1}}$$

for transformed ideals, to which we first restrict the proof. Furthermore, let

$$l_\lambda = N\left(t,q,\lambda,\prod_{i=\lambda+1}^{n} l_i\right) = \left(tq\prod_{i=\lambda+1}^{n} l_i\right)^{2^{\lambda-1}}.$$

Then

$$\prod_{\lambda=1}^{n}(l_\lambda - 1) = v(t,q,n) < \kappa(t,q,n).$$

By the third remark, the representation of $v$ leads to the conclusion: It follows from

$$g \equiv 0 \quad (\mathfrak{m},\mathfrak{a}^\kappa)$$

that

$$g \equiv 0 \quad \left(\mathfrak{m}, (x_1 - \xi_1)^{l_1}, \ldots, (x_n - \xi_n)^{l_n}\right).$$

For brevity, set

$$\mathfrak{d}_i = \left((x_i - \xi_i)^{l_i}, \ldots, (x_n - \xi_n)^{l_n}\right) \qquad \text{for } i = 1, \ldots, n.$$

Thus it follows from

$$g \equiv 0 \quad (\mathfrak{m}, \mathfrak{a}^\kappa)$$

that

$$g \equiv 0 \quad (\mathfrak{m}, \mathfrak{d}_1).$$

5. Let $\left\{ \begin{array}{ccc} \xi_1^1 & \ldots & \xi_n^1 \\ & \vdots & \\ \xi_1^p & \ldots & \xi_n^p \end{array} \right\}$ be the zeros of the associated 0-dimensional prime ideal of $\mathfrak{m}$. The roots of $E_n(x_n)$ belong to the row $\xi_1^p, \ldots, \xi_n^p$ [9, §1.9].

The proof of the theorem can now be carried out by induction.

1. $n = 1$. $\mathfrak{m} = (f(x))$ is a principal ideal. Both formulations of the theorem assert precisely the same thing, that every zero has transcendence degree 0, and is therefore algebraic. Let

$$f(x) = (x - \xi^1)^{c_1} \cdots (x - \xi^m)^{c_m}.$$

Then $\xi^1, \ldots, \xi^m$ are the only zeros of $\mathfrak{m}$ and

$$\kappa(1, q, 1) \geq q \geq \max_{i=1,\ldots,m} c_i.$$

Let

$$g \equiv 0 \quad \left(\mathfrak{m}, (x - \xi^i)^\kappa\right) \qquad \text{for } i = 1, \ldots, m.$$

Then

$$g = h_{i1} + h_{i2}(x - \xi^i)^\kappa \qquad \text{for } i = 1, \ldots, m.$$

Therefore,

$$g \equiv 0 \quad \left(\prod_{i=1}^{n} (x - \xi^i)^{c_i}\right),$$

*i.e.*

$$g \equiv 0 \quad (\mathfrak{m}).$$

2. Assume the theorem is already proved for $n = r - 1$. Let $n = r$.

(a) Assume $\mathfrak{m}$ is transformed. Now according to the hypotheses of the second formulation of the theorem, let

$$g \equiv 0 \quad (\mathfrak{m}, \mathfrak{a}^\kappa)$$

for every set of values $\xi_1, \ldots, \xi_r$. By the substitution $x_r = \xi_r$, $\mathfrak{m}$ is mapped to $\overline{\mathfrak{m}}$, $g$ to $\overline{g}$, $\mathfrak{a}$ to $\overline{\mathfrak{a}} = (x_1 - \xi_1, \ldots, x_{r-1} - \xi_{r-1})$, and

$$g \equiv 0 \quad (\overline{\mathfrak{m}}, \overline{\mathfrak{a}}^{\kappa}).$$

By hypothesis, this congruence holds for every $\xi_r$ lying in $\mathbb{P}$. Therefore by Lemma 3, it also holds if $\xi_r$ is replaced by a transcendental element over $\mathbb{P}$, *e.g.* by $x_r$, adjoined to $\mathbb{P}$. But then $\overline{g} = g$, and $\overline{\mathfrak{m}}$ is formed from $\mathfrak{m}$ by adjoining $x_r$ to $\mathbb{P}$. The polynomials of $\overline{\mathfrak{m}}$ that are integral in $x_r$ form then the $(r-1)$-th fundamental ideal $\mathfrak{g}_{r-1}$ of $\mathfrak{m}$ because $\mathfrak{m}$ is transformed. Therefore,

$$g \equiv 0 \quad \left(\overline{\mathfrak{m}}, \overline{\mathfrak{a}}^{\kappa(t,q,r)}\right).$$

Since $\kappa(t,q,r) \geq \kappa(t,q,r-1)$, it follows that

$$g \equiv 0 \quad \left(\overline{\mathfrak{m}}, \overline{\mathfrak{a}}^{\kappa(t,q,r-1)}\right)$$

for every set of values $\xi_1, \ldots, \xi_{r-1}$. Since $t$ is the number of basis elements in $\overline{\mathfrak{m}}$ and $q$ is an upper bound for its degree, it follows by hypothesis that

$$g \equiv 0 \quad (\mathfrak{m}).$$

Since $g$ is integral in $x_r$,

$$g \equiv 0 \quad (\mathfrak{g}_{r-1}).$$

The same holds under the hypothesis of the first version of this theorem. Let $g \equiv 0$ $(\mathfrak{m}, \mathfrak{o}_i^{\kappa})$ for $i = 1, \ldots, m$ accordingly. By adjoining $x_r$ to the field $\mathbb{P}$, the zero-set ideals $\mathfrak{o}_i$ corresponding to the zeros of transcendence degree 0 map into the unit ideal $\mathfrak{o}$. The other zero-set ideals, in which $\xi_r$ is a parameter that can be set equal to $x_r$, consist of ideals $\overline{\mathfrak{o}}_i$ formed by deleting the last basis element from $\mathfrak{o}_i$. Since the zeros of $\mathfrak{g}_{r-1}$ are formed by deleting the zeros of transcendence degree 0 from $\mathfrak{m}$, these $\overline{\mathfrak{o}}_i$ are the associated zero-set ideals of the ideal $\overline{\mathfrak{m}}$. As above, it follows therefore from

$$g \equiv 0 \quad (\mathfrak{m}, \mathfrak{o}_i^{\kappa}) \quad \text{for} \quad i = 1, \ldots, m$$

that

$$g \equiv 0 \quad (\mathfrak{g}_{r-1}).$$

If $\mathfrak{m}$ contains *no 0-dimensional prime ideal*, then $\mathfrak{g}_{r-1} = \mathfrak{m}$, so $g \equiv 0$ $(\mathfrak{m})$, and *the theorem is proved.*

It may be assumed therefore that $\mathfrak{m}$ has a 0-dimensional prime ideal with zeros $\xi_1^j, \ldots, \xi_r^j$, $j = 1, \ldots, p$. Instead of entire sets of values, it suffices for the additional proof of the *second version* of the theorem that we consider only sets $\xi_1^{i_1}, \ldots, \xi_r^{i_r}$, where $i_1, \ldots, i_r$ are any $r$ identical or distinct numbers of the sequence $1, \ldots, p$.

Up to now, we have:

1. $g \equiv 0\ (\mathfrak{g}_{r-1})$. Thus $E_r(x_r)g \equiv 0\ (\mathfrak{m})$, where the roots of $E_r(x_r)$ belong to the sequence $\xi_r^1, \ldots, \xi_r^p$. Since $\mathfrak{m}$ is transformed, there exists, by reasons of symmetry, polynomials $E_i(x_i)$, $i = 1, \ldots, r$, such that $E_i(x_i)g_{r-1} \equiv 0\ (\mathfrak{m})$, so $E_i g \equiv 0\ (\mathfrak{m})$. The roots of $E_i(x_i)$ belong to the sequence $\xi_i^1, \ldots, \xi_i^p$.

2. $g \equiv 0\ (\mathfrak{m}, \mathfrak{d}_1)$. It will be shown that the divisibility of $g$ by $\mathfrak{m}$ follows easily. Assume it has already been shown that

$$g \equiv 0 \quad (\mathfrak{m}, \mathfrak{d}_\nu),$$

*i.e.*

$$g \equiv 0 \quad (\mathfrak{m}, (x_\nu - \xi_\nu^{i_\nu})^{l_\nu}, \mathfrak{d}_{\nu+1}),$$

so

$$g \equiv h(x_1, \ldots, x_r)(x_\nu - \xi_\nu^{i_\nu})^{l_\nu} \qquad (\mathfrak{m}, \mathfrak{d}_{\nu+1}).$$

By 1,

$$E_\nu(x_\nu)g \equiv 0 \quad (\mathfrak{m}).$$

Therefore,

$$E_\nu h(x_\nu - \xi_\nu^{i_\nu})^{l_\nu} \equiv 0 \qquad (\mathfrak{m}, \mathfrak{d}_{\nu+1}).$$

By the Corollary to Lemma 2, there exists a polynomial $K^{i_{\nu+1}\cdots i_r}(x_\nu)$ such that

$$K^{i_{\nu+1}\cdots i_r}(x_\nu)h \equiv 0 \qquad (\mathfrak{m}, \mathfrak{d}_{\nu+1})$$

and

$$[K^{i_{\nu+1}\cdots i_r}(x_\nu)] \leq N\left(t, q, \nu, \prod_{i=\nu+1}^{r} l_i\right) = l_\nu.$$

Both $(x_\nu - \xi_\nu^{i_\nu})^{l_\nu} E_\nu(x_\nu)$ and $K^{i_{\nu+1}\cdots i_r}(x_\nu)$ have the property that their product with $h$ is divisible by $(\mathfrak{m}, \mathfrak{d}_{\nu+1})$. Thus the same is true for their greatest common divisor, whose roots are clearly all those which are also roots of both of these polynomials, and which does not have higher degree than them. Thus for

$$E^{i_\nu i_{\nu+1}\cdots i_r}(x_\nu) = \left(K^{i_{\nu+1}\cdots i_r}(x_\nu), E_\nu(x_\nu)(x_\nu - \xi_\nu^{i_\nu})^{l_\nu}\right),$$

1. $E^{i_\nu \cdots i_r}(x_\nu)h(x_1, \ldots, x_r) \equiv 0 \quad (\mathfrak{m}, \mathfrak{d}_{\nu+1})$.
2. $[E^{i_\nu \cdots i_r}(x_\nu)] \leq l_\nu$, since the same is true for $K^{i_{\nu+1}\cdots i_r}(x_\nu)$.
3. The roots of $E^{i_\nu \cdots i_r}(x_\nu)$ belong to the sequence $\xi_\nu^1, \ldots, \xi_\nu^p$, since the same is true for $E_\nu(x_\nu)(x_\nu - \xi_\nu^{i_\nu})^{l_\nu}$.

Let

$$E^{i_\nu \cdots i_r}(x_\nu) = (x_\nu - \xi_\nu^{i_\nu})^{d_{i_\nu \cdots i_r}} D^{i_\nu \cdots i_r}(x_\nu),$$

where $\xi_\nu^{i_\nu}$ are not roots of $D^{i_\nu \cdots i_r}(x_\nu)$ and

$$d_{i_\nu \cdots i_r} \leq l_\nu.$$

Since all of the polynomials $E^{1i_\nu\cdots i_r}(x_\nu),\ldots,E^{pi_\nu\cdots i_r}(x_\nu)$ have only roots in the sequence $\xi_\nu^1,\ldots,\xi_\nu^p$, the polynomials $D^{1i_\nu\cdots i_r}(x_\nu),\ldots,D^{pi_\nu\cdots i_r}(x_\nu)$ are relatively prime. Thus

$$\mathfrak{d} = \left(D^{1i_\nu\cdots i_r}(x_\nu),\ldots,D^{pi_\nu\cdots i_r}(x_\nu)\right) = \mathfrak{o}.$$

Now

$$\begin{aligned} D^{i_\nu\cdots i_r}(x_\nu)g &\equiv (x_\nu-\xi_\nu^{i_\nu})^{l_\nu}h(x_1,\ldots,x_r)D^{i_\nu\cdots i_r}(x_\nu) \\ &= (x_\nu-\xi_\nu^{i_\nu})^{l_\nu-d_{i_\nu\cdots i_r}}E^{i_\nu\cdots i_r}(x_\nu)h(x_1,\ldots,x_r)\equiv 0 \quad (\mathfrak{m},\mathfrak{d}_{\nu+1}). \end{aligned}$$

This holds for $i_\nu = 1,\ldots,p$, so

$$\mathfrak{d}g \equiv 0 \quad (\mathfrak{m},\mathfrak{d}_{\nu+1}).$$

Now since $\mathfrak{d}=\mathfrak{o}$ contains the identity element,

$$g \equiv 0 \quad (\mathfrak{m},\mathfrak{d}_{\nu+1}).$$

If we set $\nu$ to the values $1,\ldots,r$ successively, then we obtain

$$g \equiv 0 \quad (\mathfrak{m}).$$

Therefore, the *second version of the theorem* is proved for transformed ideals. For the full proof of the first version, it suffices to show that

$$g \equiv 0 \quad (\mathfrak{m},\mathfrak{o}^\kappa)$$

for every zero-set ideal of $\mathfrak{m}$ implies

$$g \equiv 0 \quad (\mathfrak{m},\mathfrak{a}^\kappa)$$

for every

$$\mathfrak{a} = (x_1-\xi_1,\ldots,x_r-\xi_r).$$

Therefore, let

$$g \equiv 0 \quad (\mathfrak{m},\mathfrak{o}^\kappa)$$

for every zero-set ideal of $\mathfrak{m}$, and $\xi_1,\ldots,\xi_r$ be an arbitrary set of values with

$$\mathfrak{a} = (x_1-\xi_1,\ldots,x_r-\xi_r).$$

It must be shown that $g\equiv 0\ (\mathfrak{m},\mathfrak{a}^\kappa)$. There are three cases to consider.

1. $\xi_1,\ldots,\xi_r$ is not an algebraic zero of $\mathfrak{m}$. Then $(\mathfrak{m},\mathfrak{a}^\kappa)=\mathfrak{o}$, so clearly
$$g \equiv 0 \quad (\mathfrak{m},\mathfrak{a}^\kappa).$$

2. $\xi_1,\ldots,\xi_r$ is a zero of one of the associated 0-dimensional prime ideals of $\mathfrak{m}$. Then $\mathfrak{a}$ belongs to the set of zero set ideals, so again
$$g \equiv 0 \quad (\mathfrak{m},\mathfrak{a}^\kappa).$$

3. $\xi_1, \ldots, \xi_r$ is an algebraic zero of $\mathfrak{m}$, but not a zero of an associated 0-dimensional prime ideal of $\mathfrak{m}$.

Now $(\mathfrak{m}, \mathfrak{a}^\kappa)$ is a 0-dimensional prime ideal, so $(\mathfrak{m}, \mathfrak{a}^\kappa) \equiv 0\ (\mathfrak{a})$ because $\mathfrak{m} \equiv 0\ (\mathfrak{a})$. On the other hand $\mathfrak{a}^\kappa \equiv 0\ (\mathfrak{m}, \mathfrak{a}^\kappa)$. Therefore, all of the associated prime ideals of $(\mathfrak{m}, \mathfrak{a}^\kappa)$ are divisors of the prime ideal $\mathfrak{a}$, and this itself is an associated prime ideal of $(\mathfrak{m}, \mathfrak{a}^\kappa)$. However, as a 0-dimensional prime ideal, $\mathfrak{a}$ has no proper divisor except for $\mathfrak{o}$, so it is the only associated prime ideal of $(\mathfrak{m}, \mathfrak{a}^\kappa)$. Therefore, $(\mathfrak{m}, \mathfrak{a}^\kappa)$ is a primary ideal and is associated to $\mathfrak{a}$. Now let $\mathfrak{t}$ be the least common multiple of the 0-dimensional primary ideals which appear in a decomposition of $\mathfrak{m}$. Then

$$\mathfrak{m} = [\mathfrak{g}_{r-1}, \mathfrak{t}].$$

By hypothesis

$$\mathfrak{t} \not\equiv 0 \quad (\mathfrak{a}).$$

Since $\mathfrak{a}$ is a prime ideal,

$$\mathfrak{t}^\lambda \not\equiv 0 \quad (\mathfrak{a})$$

for all $\lambda$. Because $(\mathfrak{m}, \mathfrak{a}^\kappa) \equiv 0\ (\mathfrak{a})$, it follows that

$$\mathfrak{t}^\lambda \not\equiv 0 \quad (\mathfrak{m}, \mathfrak{a}^\kappa)$$

for all $\lambda$. On the other hand,

$$\mathfrak{m} = [\mathfrak{g}_{r-1}, \mathfrak{t}] \equiv 0 \quad (\mathfrak{m}, \mathfrak{a}^\kappa),$$

so

$$\mathfrak{g}_{r-1}\mathfrak{t} \equiv 0 \quad (\mathfrak{m}, \mathfrak{a}^\kappa).$$

Since $(\mathfrak{m}, \mathfrak{a}^\kappa)$ is a primary ideal it follows that

$$\mathfrak{g}_{r-1} \equiv 0 \quad (\mathfrak{m}, \mathfrak{a}^\kappa).$$

But as already proved in the inductive conclusion, it now follows by the hypothesis $g \equiv 0\ (\mathfrak{m}, \mathfrak{o}_i^\kappa)$ for every zero-set ideal and by the assumption that the theorem is already proved for $r-1$ variables, that

$$g \equiv 0 \quad (\mathfrak{g}_{r-1}).$$

Therefore,

$$g \equiv 0 \quad (\mathfrak{m}, \mathfrak{a}^\kappa)$$

for every $\mathfrak{a}$. Since the second version of the theorem is already proved, it follows that

$$g \equiv 0 \quad (\mathfrak{m}).$$

The *first version* of the theorem is now proved for transformed ideals.

2. Suppose $\mathfrak{m}$ is not transformed. The theorem is true for the associated transformed ideal $\mathfrak{m}'$ of $\mathfrak{m}$. The transcendental zeros of $\mathfrak{m}$ map to those in $\mathfrak{m}'$ under the transformation. Thus the zero-set ideals $\mathfrak{o}_i$ map to zero-set ideals $\mathfrak{o}_i'$ of $\mathfrak{m}'$. The polynomial $g$ maps to $g'$. Let

$$g \equiv 0 \quad (\mathfrak{m}, \mathfrak{o}_i^{\kappa}) \qquad \text{for } i = 1, \ldots, m.$$

Consequently,

$$g' \equiv 0 \quad (\mathfrak{m}', \mathfrak{o}_i^{'\kappa}) \qquad \text{for } i = 1, \ldots, m.$$

Therefore,

$$g' \equiv 0 \quad (\mathfrak{m}').$$

Since $g'$ is transformed, it can be be inversely transformed:

$$g \equiv 0 \quad (\mathfrak{m}).$$

The same is true if we consider the ideals $\mathfrak{a}$ from the second version instead of the $\mathfrak{o}_i$, for then the algebraic zeros of the non-transformed ideals, as well as those of the transformed ideals, map to each other under the transformation. Both versions of the theorem are now completely proved. □

# §6. Fundamental Ideals

In the next paragraphs, the characteristic ideals and polynomials for an ideal will be computed. This deals mainly with the formation of the fundamental ideal as well as the norm and elementary divisor form. To do this, it will be necessary to pass to the module $\mathfrak{M}_{\varrho-1}^{*}$ defined in [9, §1.5] which consists precisely of the polynomials of $\mathfrak{m}$ whose degree in $x_1, \ldots, x_{\varrho-1}$ does not exceed a fixed degree $n_{\varrho-1}$ when viewed as linear forms in the power products of $x_1, \ldots, x_{\varrho-1}$. The computation of the number $n_{\varrho-1}$ is given in Theorem 6.

**Theorem 6.** *Hypothesis: Let $\mathfrak{m}$ be a transformed ideal in $\mathbb{P}[x_1, \ldots, x_n] = \overline{\mathbb{P}}(u_{11}, \ldots, u_{nn})[x_1, \ldots, x_n]$ and $q$ the maximal degree of the given basis of $\mathfrak{m}$. Claim: For the set of residue classes $\mathfrak{g}_{\varrho}/\mathfrak{m}$, there are residue class representatives which do not exceed a fixed degree $n_{\varrho}$ in the power products of $x_1, \ldots, x_{\varrho}$, where $n_{\varrho}$ is given by the recursive formula*

$$n_0 = 0; \qquad n_{\varrho} = n_{\varrho-1} + \left[1 + \binom{n_{\varrho-1} + \varrho - 1}{\varrho - 1}\right] \sum_{i=0}^{n-1} q^{2^i}.$$

*Proof* (by induction). 1. $\varrho = 0$. The theorem places absolutely no restrictions on the representatives of the set of residue classes, so this is clear.

2. Assume the theorem is already proved for $\varrho = 0, \ldots, \lambda - 1$.

(a) Assume that $\overline{\mathbb{P}}$ has infinitely many elements. Let

$$\mathfrak{m} = (f_{\lambda-1,1}, \ldots, f_{\lambda-1,t_{\lambda-1}})$$

be the $(\lambda-1)$-th canonical ideal basis for $\mathfrak{m}$ which exists and is computable by Theorem 4, and whose basis elements do not exceed the degree $\overline{q} = \sum_{i=0}^{n-1} q^{2^i}$ by Theorem 4. For simplicity, the index $\lambda-1$ in this basis will be omitted in the proof that follows. Thus we write

$$\mathfrak{m} = (f_1, \ldots, f_{t_{\lambda-1}}).$$

Let $z_\sigma$, $\sigma = 1, \ldots, s$, be the power products of $x_1, \ldots, x_{\lambda-1}$ whose degrees do not exceed $n_{\lambda-1}$. Hence $s = \begin{pmatrix} n_{\lambda-1}+\lambda-1 \\ \lambda-1 \end{pmatrix}$. Let $\zeta_{\mu_\kappa}$, $\mu_\kappa = 1, \ldots, m_\kappa$, be the power products of $x_1, \ldots, x_{\lambda-1}$ whose degrees do not exceed $n_{\lambda-1} - [f]_{\lambda-1}$. Hence $m_\kappa \leq s$.

Let $\mathfrak{M}^*_{\lambda-1} = \left(f_1, \ldots, f_{t_{\lambda-1}}, \zeta_1 f_1, \ldots, \zeta_{m_{t_{\lambda-1}}} f_{t_{\lambda-1}}\right) = (l_1, \ldots, l_{\overline{t}})$. Then $\overline{t} < t_{\lambda-1}s$, and $\mathfrak{M}^*_{\lambda-1}$ can be viewed as a module of linear forms in the $z_\sigma$ with coefficients in $\mathbb{P}[x_\lambda, \ldots, x_n]$. Since it is formed from the canonical ideal basis defined in Theorem 4, it consists precisely of those elements of $\mathfrak{m}$ whose degree does not exceed $n_{\lambda-1}$.

The methods of Theorem 3 will be applied to the module $\mathfrak{M}^*_{\lambda-1}$, so the existence of a regular determinant of the rank of the module must be verified. Since $\overline{\mathbb{P}}$ has infinitely many elements, the transformation $x = V(y)$

$$\begin{array}{lcl} x_1 & = & y_1 \\ & \vdots & \\ x_{\lambda-1} & = & y_{\lambda-1} \\ x_\lambda & = & v_{\lambda\lambda}y_\lambda + \ldots + v_{\lambda n}y_n \\ & \vdots & \\ x_n & = & v_{n\lambda}y_\lambda + \ldots + v_{nn}y_n \end{array}$$

maps $\mathfrak{M}^*_{\lambda-1}$ to a module $\mathfrak{M}^{*'}_{\lambda-1}$ which has a regular determinant in $y_\lambda$, where $v_{ij}$ are elements of $\overline{\mathbb{P}}$ and $V$ has a nonzero determinant. Since the transformation leaves the $z_\sigma$ unchanged, that is nothing changes in the construction of the module, $\mathfrak{M}^{*'}_{\lambda-1}$ can also be formed by first applying the transformation $x = V(y)$ and then constructing the module in the way indicated. $\mathfrak{m}$ is transformed, hence is formed from an ideal $\overline{m}$ in $\overline{\mathbb{P}}[\overline{x}_1, \ldots, \overline{x}_n]$ under the transformation $\overline{x} = U(x)$ and the adjoining of the elements $u_{ij}$ of $U$ to the field $\overline{\mathbb{P}}$. $\mathfrak{m}$ maps to $\mathfrak{m}'$ under $x = V(y)$. Now $\overline{x} = UV(y) = W(y)$. The elements $w_{ij}$ of the matrix $W$ are therefore linear combinations of the $u_{ij}$ with coefficients in $\overline{\mathbb{P}}$. Furthermore, since $V$ has a nonzero determinant, $U = WV^{-1}$, so conversely, the elements of $U$ can be expressed as linear combinations of the $w_{ij}$ with coefficients in $\overline{\mathbb{P}}$.

Like the $u_{ij}$, the $w_{ij}$ are also indeterminates, and the fields $\overline{\mathbb{P}}(u_{ij})$ and $\overline{\mathbb{P}}(w_{ij})$ are identical. Thus the correspondence $u_{ij} \sim w_{ij}$ and $x_k \sim y_k$ establishes an isomorphism between $\mathfrak{m}$ and $\mathfrak{m}'$ as well as between $\mathfrak{M}^*_{\lambda-1}$ and $\mathfrak{M}^{*'}_{\lambda-1}$, since both of these modules are formed from isomorphic ideals in entirely analogous ways. Since the existence of the regular determinant for $\mathfrak{M}^{*'}_{\lambda-1}$ was verified, it is also true therefore for $\mathfrak{M}^*_{\lambda-1}$.

Let

$$\begin{aligned} l_1 &= f_{11}z_1 + \ldots + f_{1s}z_s \\ &\vdots \\ l_{\bar{t}} &= f_{\bar{t}1}z_1 + \ldots + f_{\bar{t}s}z_s. \end{aligned}$$

Let $p \leq s$ be the rank of $\mathfrak{M}^*_{\lambda-1}$. The polynomials $D_{i_1 \ldots i_p}$, specifically $D_{1 \ldots p} = D$, $F_{ij}$ and $m_i$ are defined relative to $\mathfrak{M}^*_{\lambda-1}$ exactly as in Theorem 3. This is possible since $\mathfrak{M}^*_{\lambda-1}$ has a regular determinant.

Now let

$$k \equiv 0 \quad (\mathfrak{g}_\lambda).$$

Then since $\mathfrak{m}$ is transformed, there exists only one polynomial $K^{(\lambda+1)} \neq 0$ dependent on $x_{\lambda+1}, \ldots, x_n$ such that

$$K^{(\lambda+1)}k \equiv 0 \quad (\mathfrak{m}).$$

Furthermore since $y_\lambda \equiv 0$ $(\mathfrak{g}_\lambda)$,

$$k \equiv 0 \quad (\mathfrak{g}_{\lambda-1}).$$

Then by hypothesis,

$$k \equiv g \quad (\mathfrak{m}),$$

so

$$K^{(\lambda+1)}g \equiv 0 \quad (\mathfrak{m}),$$

where

$$[g]_{\lambda-1} \leq n_{\lambda-1}.$$

Thus

$$\left[K^{(\lambda+1)}g\right]_{\lambda-1} \leq n_{\lambda-1},$$

so therefore

$$K^{(\lambda+1)}g \equiv 0 \quad (\mathfrak{M}^*_{\lambda-1}).$$

As in Theorem 3, we set

$$g = g_1^{(\lambda)}z_1 + \ldots + g_s^{(\lambda)}z_s$$

$$g_i^{(\lambda)} = G_i^{(\lambda)} + Dj_i^{(\lambda)} \qquad \text{for } i = 1, \ldots, p,$$

so that

$$\left[G_i^{(\lambda)}\right]_\lambda < [D]_\lambda = [D] \qquad \text{for } i = 1, \ldots, p$$

and

$$\left[j_i^{(\lambda)}\right] < [g] \qquad \text{for } i = 1, \ldots, p.$$

Then as in Theorem 3,

$$\begin{aligned} g &= G + \sum_{i=1}^{p} m_i j_i^{(\lambda)} \\ G &= G_1^{(\lambda)} z_1 + \ldots + G_p^{(\lambda)} z_p + G_{p+1}^{(\lambda)} z_{p+1} + \ldots + G_s^{(\lambda)} z_s. \end{aligned}$$

Since $K^{(\lambda+1)}$ is independent of $x_\lambda$, we obtain the corresponding factorizations of $K^{(\lambda+1)}g$ by multiplying $g$, $g_i^{(\lambda)}$, $G_i^{(\lambda)}$ and $j_i^{(\lambda)}$ by $K^{(\lambda+1)}$ in these equations and inequalities. So it remains that

$$\left[K^{(\lambda+1)} G_i^{(\lambda)}\right]_\lambda < [D].$$

Because $g \equiv G\ (\mathfrak{M}_{\lambda-1}^*)$,

$$K^{(\lambda+1)} G \equiv 0\ (\mathfrak{M}_{\lambda-1}^*),$$

*i.e.*

$$\begin{aligned} K^{(\lambda+1)} G &= a_1 l_1 + \ldots + a_{\bar{t}} l_{\bar{t}} \\ K^{(\lambda+1)} G_i &= a_1 f_{i1} + \ldots + a_{\bar{t}} f_{i\bar{t}} \end{aligned}$$

Here, as in Theorem 3, we can set

$$[a_i]_\lambda \leq [D] \qquad \text{for } i = 1, \ldots, p,$$

and can easily show,[14] as we did there, that

$$[a_i]_\lambda \leq \overline{q} p \qquad \text{for } i = 1, \ldots, \bar{t},$$

*i.e.*

$$[a_i]_\lambda < \overline{q} \begin{pmatrix} n_{\lambda-1} + \lambda - 1 \\ \lambda - 1 \end{pmatrix} \qquad \text{for } i = 1, \ldots, \bar{t}.$$

Hence it follows that

$$\begin{aligned} [G_i]_\lambda &\leq \overline{q} + \overline{q} \begin{pmatrix} n_{\lambda-1} + \lambda - 1 \\ \lambda - 1 \end{pmatrix} && \text{for } i = 1, \ldots, \bar{t}, \\ [G]_\lambda &\leq n_{\lambda-1} + \overline{q} \left[1 + \begin{pmatrix} n_{\lambda-1} + \lambda - 1 \\ \lambda - 1 \end{pmatrix}\right] = n_\lambda. \end{aligned}$$

Moreover, since $k \equiv g\ (\mathfrak{m})$ and $g \equiv G\ (\mathfrak{m})$,

$$k \equiv G\ (\mathfrak{m})$$

[14] In Theorem 3, the number $t$ of basis elements of the module is used instead of $p$. But we only needed this number to be no smaller than the rank of the module. Hence the rank $p$ does the same thing in this inequality.

as well. Therefore, $G$ is a representative of the residue class $k$ in $\mathfrak{g}_\lambda/\mathfrak{m}$ that is bounded in $x_1, \ldots, x_\lambda$.

(b) Suppose $\overline{\mathbb{P}}$ contains only finitely many elements. Let $s$ be transcendental over $\overline{\mathbb{P}}$. Then clearly $\overline{\mathbb{P}}(s)$ contains infinitely many elements. Let $\mathfrak{m}'$ be the ideal in $\overline{\mathbb{P}}(u_{11}, \ldots, u_{nn}, s)[x_1, \ldots, x_n]$, whose basis coincides with that of $\mathfrak{m}$. The theorem holds for $\mathfrak{m}'$ by (a). Then the $\varrho$-th fundamental ideal $\mathfrak{g}'_\varrho$ of $\mathfrak{m}'$ is the ideal formed by adjoining $s$ in $\mathfrak{g}_\varrho$ to the $\varrho$-th fundamental ideal of $\mathfrak{m}$.[15]

Let $g \equiv 0\ (\mathfrak{g}_\varrho)$. Then $g \equiv 0\ (\mathfrak{g}'_\varrho)$ as well, so there exists $k'(s)$ such that

$$g \equiv k' \quad (\mathfrak{m}') \qquad \text{and} \qquad [k']_\varrho \leq n_\varrho.$$

Therefore,

$$g = k' + c'_1 f_1 + \ldots + c'_t f_t.$$

By multiplying by a polynomial $\kappa(s)$ in $\overline{\mathbb{P}}(u_{11}, \ldots, u_{nn})[s]$, this equation can be made integral in $s$. Hence, without loss of generality, we may assume that the identity $E$ of $\overline{\mathbb{P}}$ is the smallest coefficient in $\kappa(s)$ appearing in $\kappa(s)$. If we split up the equation

$$\kappa g = k'' + c''_1 f_1 + \ldots + c''_t f_t$$

by powers of $s$ and set the coefficients of the lowest power appearing in $\kappa(s)$ equal, then we obtain on the right and left

$$g = k + c_1 f_1 + \ldots + c_t f_t.$$

Thus $k, c_1, \ldots, c_t$ are the corresponding coefficients of $k'', c''_1, \ldots, c''_t$. Therefore

$$g \equiv k \quad (\mathfrak{m}) \qquad \text{and} \qquad [k]_\varrho \leq n_\varrho. \quad \square$$

**Lemma 4.** *Hypothesis: Let $\mathfrak{M}$ be a module of linear forms in $z_1, \ldots, z_s$ with coefficients in $\mathbb{P}[x_\varrho, \ldots, n]$. Let $\mathfrak{G}$ be the corresponding fundamental module. Let $\mathfrak{M}'$ and $\mathfrak{G}'$ be modules of linear forms in $z_1, \ldots, z_s$ with coefficients in $\mathbb{P}[x_\varrho](x_{\varrho+1}, \ldots, n)$, whose basis elements coincide with those of $\mathfrak{M}$ and $\mathfrak{G}$, respectively.*
*Claim: $\mathfrak{G}'$ is the fundamental module of $\mathfrak{M}'$.*

*Proof.* Let $c'g'(z) \equiv 0\ (\mathfrak{M}')$, where $c' \neq 0$ is an element of $\mathbb{P}[x_\varrho](x_{\varrho+1}, \ldots, n)$ and $g'(z)$ is a linear form in $z_1, \ldots, z_s$ with coefficients in $\mathbb{P}[x_\varrho](x_{\varrho+1}, \ldots, n)$. Then there exists a polynomial $d^{(\varrho+1)} \neq 0$ in $\mathbb{P}[x_{\varrho+1}, \ldots, n]$ such that

$$d^{(\varrho+1)} c'g'(z) \equiv 0 \quad (\mathfrak{M}),$$

and

$$d^{(\varrho+1)} = e^{(\varrho+1)} f^{(\varrho+1)},$$

[15] See §1.4: Adjoining indeterminates to the field does not change the property of an ideal being a fundamental ideal of another.

where

$$e^{(\varrho+1)}c' = c \qquad \text{and} \qquad f^{(\varrho+1)}g'(z) = g(z)$$

are integral in $x_{\varrho+1}, \ldots, x_n$. Therefore,

$$cg(z) \equiv 0 \quad (\mathfrak{M}) \qquad c \neq 0,$$

so

$$g(z) \equiv 0 \quad (\mathfrak{G}).$$

Hence

$$g'(z) = \frac{g(z)}{f^{(\varrho+1)}} \equiv 0 \quad (\mathfrak{G}').$$

Thus the fundamental ideal of $\mathfrak{M}'$ is divisible by $\mathfrak{G}'$. On the other hand,

$$g'(z) \equiv 0 \quad (\mathfrak{G}'),$$

so there exists a polynomial $f^{(\varrho+1)} \neq 0$ such that

$$f^{(\varrho+1)}g' = g \equiv 0 \quad (\mathfrak{G}).$$

Thus there exists a $c$ in $\mathbb{P}[x_\varrho, \ldots, x_n]$ such that

$$cg \equiv 0 \quad (\mathfrak{M})$$

and consequently

$$cg' \equiv 0 \quad (\mathfrak{M}').$$

Therefore, $g'$, and hence $\mathfrak{G}'$ as well, are divisible by the fundamental module of $\mathfrak{M}'$. So $\mathfrak{G}'$ is the fundamental ideal of $\mathfrak{M}'$. □

**Corollary to Theorem 6.** $\mathfrak{g}_\varrho$ has a basis mod $\mathfrak{m}$ consisting of elements whose degree in $x_1, \ldots, x_\varrho$ does not exceed $n_\varrho$. Now since the degree in $x_1, \ldots, x_\varrho$ of the basis elements of $\mathfrak{m}$ does not exceed $q$ already, and since $n_\varrho \geq q$ for $\varrho > 0$, $\mathfrak{g}_\varrho$ has a basis for $\varrho > 0$ consisting of elements whose degree in $x_1, \ldots, x_\varrho$ does not exceed $n_\varrho$.

As noted in the proof of Theorem 6, the module $\mathfrak{M}^*_\varrho$ consists of all elements of $\mathfrak{m}$ whose degree in $x_1, \ldots, x_\varrho$ does not exceed $n_\varrho$. We now stipulate accordingly:

**Definition.**

1. Let $\mathfrak{G}^*_\varrho$ be the module of linear forms in the power products $z_\sigma$ of $x_1, \ldots, x_\varrho$ consisting of all elements of $\mathfrak{g}_\varrho$ whose degree in $x_1, \ldots, x_\varrho$ does not exceed $n_\varrho$. Then by the Corollary to Theorem 6, $\mathfrak{G}^*_\varrho$ contains a basis of $\mathfrak{g}_\varrho$.

2. Let $\mathfrak{M}_\varrho$ and $\mathfrak{G}_\varrho$ be modules of linear forms in the power products $z_\sigma$ of $x_1, \ldots, x_\varrho$ consisting of all elements contained in $\mathfrak{m}$ and $\mathfrak{g}_\varrho$. So infinitely many $z_\sigma$ appear in $\mathfrak{M}_\varrho$ and $\mathfrak{G}_\varrho$, even though each individual linear form contains only finitely many $z_\sigma$.

For what follows, assume $\mathfrak{m}$, and hence $\mathfrak{g}_\varrho$ as well, are transformed [§1.4]. Then clearly $\mathfrak{G}_\varrho$ is the fundamental ideal of $\mathfrak{M}$. For the modules $\mathfrak{M}^*_{\varrho-1}$, $\mathfrak{G}^*_{\varrho-1}$, $\mathfrak{M}_{\varrho-1}$, and $\mathfrak{G}_{\varrho-1}$, we have:

**Theorem 7.**

1. *$\mathfrak{G}^*_{\varrho-1}$ is the fundamental ideal of $\mathfrak{M}^*_{\varrho-1}$.*
2. *The set of residue classes $\mathfrak{G}^*_{\varrho-1}/\mathfrak{M}^*_{\varrho-1}$ of $\mathfrak{G}^*_{\varrho-1}$ modulo $\mathfrak{M}^*_{\varrho-1}$ is isomorphic to that of $\mathfrak{G}_{\varrho-1}$ modulo $\mathfrak{M}_{\varrho-1}$. Notationally,*

$$\mathfrak{G}^*_{\varrho-1}/\mathfrak{M}^*_{\varrho-1} \sim \mathfrak{G}_{\varrho-1}/\mathfrak{M}_{\varrho-1}.$$

3. *$\mathfrak{M}_{\varrho-1}$ has only finitely many elementary divisors not equal to the identity $E$, namely those in $\mathfrak{M}^*_{\varrho-1}$.*

*Proof.* 1. Let $\overline{\mathfrak{G}}^*_{\varrho-1}$ be the fundamental ideal of $\mathfrak{M}^*_{\varrho-1}$. Let $g \equiv 0\ (\mathfrak{G}^*_{\varrho-1})$. Then $g \equiv 0\ (\mathfrak{g}_{\varrho-1})$ and $[g]_{\varrho-1} \leq n_{\varrho-1}$. Consequently, there exists a polynomial $f^{(\varrho)} \neq 0$ such that $f^{(\varrho)}g \equiv 0\ (\mathfrak{m})$. $[f^{(\varrho)}g]_{\varrho-1} \leq n_{\varrho-1}$, so $f^{(\varrho)}g \equiv 0\ (\mathfrak{M}^*_{\varrho-1})$, and hence $g \equiv 0\ (\overline{\mathfrak{G}}^*_{\varrho-1})$.

On the other hand, if $g \equiv 0\ (\mathfrak{G}^*_{\varrho-1})$, then there exists a $f^{(\varrho)} \neq 0$ such that $f^{(\varrho)}g \equiv 0\ (\mathfrak{M}^*_{\varrho-1})$. Hence, $[f^{(\varrho)}g]_{\varrho-1} \leq n_{\varrho-1}$, so $[g]_{\varrho-1} \leq n_{\varrho-1}$ also. Moreover, $g \equiv 0\ (\mathfrak{g}_{\varrho-1})$. Therefore, $g \equiv 0\ (\mathfrak{G}^*_{\varrho-1})$, and thus

$$\mathfrak{G}^*_{\varrho-1} = \overline{\mathfrak{G}}^*_{\varrho-1}.$$

2. Let $\{g\}$ be a residue class of $\mathfrak{G}_{\varrho-1}/\mathfrak{M}_{\varrho-1}$. By Theorem 6, $g$ may be chosen so that $[g]_{\varrho-1} \leq n_{\varrho-1}$, hence $g \equiv 0\ (\mathfrak{G}^*_{\varrho-1})$. Therefore,

$$\mathfrak{G}_{\varrho-1}/\mathfrak{M}_{\varrho-1} \sim \mathfrak{G}^*_{\varrho-1}/\mathfrak{M}_{\varrho-1}.$$

Now let $\{g\}$ be the residue class of zero in $\mathfrak{G}^*_{\varrho-1}/\mathfrak{M}_{\varrho-1}$, *i.e.*

$$g \equiv 0\ (\mathfrak{G}^*_{\varrho-1}) \qquad \text{and} \qquad g \equiv 0\ (\mathfrak{M}_{\varrho-1}),$$

so

$$[g]_{\varrho-1} \leq n_{\varrho-1} \qquad \text{and} \qquad g \equiv 0\ (\mathfrak{m}).$$

Hence it follows that

$$g \equiv 0\ (\mathfrak{M}^*_{\varrho-1}).$$

Thus $\{g\}$ is also the residue class of zero in $\mathfrak{G}^*_{\varrho-1}/\mathfrak{M}^*_{\varrho-1}$. On the other hand, if $\{g\}$ is the residue class of zero in $\mathfrak{G}^*_{\varrho-1}/\mathfrak{M}^*_{\varrho-1}$, then since $M^*_{\varrho-1} \equiv 0\ (\mathfrak{M}_{\varrho-1})$, the residue class $\{g\}$ is also the residue class of zero in $\mathfrak{G}^*_{\varrho-1}/\mathfrak{M}^*_{\varrho-1}$.Therefore,

$$\mathfrak{G}^*_{\varrho-1}/\mathfrak{M}_{\varrho-1} \sim \mathfrak{G}^*_{\varrho-1}/\mathfrak{M}^*_{\varrho-1}.$$

So then

$$\mathfrak{G}_{\varrho-1}/\mathfrak{M}_{\varrho-1} \sim \mathfrak{G}^*_{\varrho-1}/\mathfrak{M}^*_{\varrho-1}.$$

3. For the proof of the third claim, let $x_{\varrho+1}, \ldots, x_n$ be adjoined to the underlying field. By Lemma 4, the property of $G^*_{\varrho-1}$ and $G_{\varrho-1}$ being fundamental modules of $M^*_{\varrho-1}$ and $M_{\varrho-1}$, respectively, remains valid. Therefore, the coefficient domain of these modules is now the ring $\mathbb{P}[x_\varrho](x_{\varrho+1}, \ldots, x_n)$, in which every ideal is a principal ideal. The modules can then be viewed as generalized abelian groups under addition whose operator domain is the coefficient ring of the module. The theorem on the unique representation up to isomorphism of an abelian group of finite order as a direct sum of finitely many cyclic groups, whose orders are divisible by each other, is also valid here, since for its proof, we need only assume that every ideal in the operator domain is a principal ideal. The *order* of a group $\Gamma$ is defined here as an element $a$ of the operator domain such that $a\Gamma$ vanishes, and that $a$ is the greatest common divisor of all elements having this property.

Now there exists a representation

$$\begin{array}{ll} \mathfrak{M}^*_{\varrho-1} = (e_1\eta_1, \ldots, e_r\eta_r) & \mathfrak{G}^*_{\varrho-1} = (\eta_1, \ldots, \eta_r) \\ \mathfrak{M}_{\varrho-1} = (e'_1\eta'_1, \ldots, e'_{r'}\eta'_{r'}, \zeta_1, \ldots) & \mathfrak{G}_{\varrho-1} = (\eta'_1, \ldots, \eta'_{r'}, \zeta_1, \ldots) \quad [9,\ \S 1.5] \end{array}$$

where

$$\begin{array}{ll} e_1 \neq E, \ldots, e_s \neq E, & e_{s+1} = \ldots = e_r = E, \\ e'_1 \neq E, \ldots, e'_{s'} \neq E, & e'_{s'+1} = \ldots = e'_{r'} = E, \end{array}$$

$E$ is the identity of the field, and $\eta_i$, $\eta'_j$, and $\zeta_k$ are linearly independent from each other. Group theoretically, it follows then that

$$\mathfrak{G}^*_{\varrho-1}/\mathfrak{M}^*_{\varrho-1} = \{\eta_1\} + \ldots + \{\eta_s\} \qquad \mathfrak{G}_{\varrho-1}/\mathfrak{M}_{\varrho-1} = \{\eta'_1\} + \ldots + \{\eta'_{s'}\}.$$

These sums are direct, $\{\eta_i\}$ and $\{\eta'_j\}$ are cyclic groups of order $e_i$ and $e'_j$. Since this representation is unique up to isomorphism and since $\mathfrak{G}^*_{\varrho-1}/\mathfrak{M}^*_{\varrho-1} \sim \mathfrak{G}_{\varrho-1}/\mathfrak{M}_{\varrho-1}$, it follows that $r = r'$ and $e_i = e'_i$. Therefore, the elementary divisors of $\mathfrak{M}^*_{\varrho-1}$ and $\mathfrak{M}_{\varrho-1}$ not equal to the identity $E$ coincide. □

**Theorem 8.** *The basis of the $\varrho$-th fundamental ideal $\mathfrak{g}_\varrho$ of $\mathfrak{m} = (f_1, \ldots, f_t)$ can be computed in finitely many steps.*

*Proof* (by induction). 1. $\varrho = n$. Then $\mathfrak{g}_\varrho = \mathfrak{m} = (f_1, \ldots, f_t)$.

2. Assume the theorem is already proved for $\varrho \geq \lambda$. Let $\varrho = \lambda - 1$. The proof is composed of two parts.

(a) *Module computations.*

In these paragraphs, define $\mathfrak{M}^*_{\lambda-1}$ and $\mathfrak{G}^*_{\lambda-1}$ to be the modules of linear forms in the power products $z$ of $x_1, \ldots, x_{\lambda-1}$ with coefficients in $\mathbb{P}[x_\lambda, \ldots, x_n]$. As shown in Theorem 6, a basis for $\mathfrak{M}^*_{\lambda-1}$ can be computed in finitely many steps. Let $\mathfrak{M}^{*'}_{\lambda-1}$ and $\mathfrak{G}^{*'}_{\lambda-1}$ be the modules of linear forms in the power products $z$ in with coefficients in $\mathbb{P}[x_\lambda](x_{\lambda+1}, \ldots, x_n)$, which have the same basis as $\mathfrak{M}^*_{\lambda-1}$

and $\mathfrak{G}^*_{\lambda-1}$, respectively. Thus they are formed by adjoining $x_{\lambda+1}, \ldots, x_n$ to the field $\mathbb{P}$. By Theorem 7.1 and Lemma 4, $\mathfrak{G}^{*'}_{\lambda-1}$ is the fundamental ideal of $\mathfrak{M}^{*'}_{\lambda-1}$. We first consider the computation of a basis for $\mathfrak{G}^{*'}_{\lambda-1}$.

Let $A$ be the matrix of the computed module basis of $\mathfrak{M}^{*'}_{\lambda-1}$. Let $p$ be the rank of this module. Then by elementary divisor theory, there exists two matrices $R$ and $S$ of rank $t$, which have a nonzero $t$-row determinant independent of $x_\lambda$, such that

$$RAS = \begin{pmatrix} e_{\lambda-1,1} & 0 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & e_{\lambda-1,p} \end{pmatrix}.$$

$R$ and $S$ can be computed in finitely many steps (*e.g.* using Bôcher's method [1, Chap. 20]). If we set $l' = R(l)$, then the $l'$ form a new basis for $\mathfrak{M}^{*'}_{\lambda-1}$, since, due to the nonzero $t$-row determinant of $R$ independent of $x_\lambda$, the transformation is invertible. This new module basis has the matrix $RA$. Moreover, if we transform the variables $z_\sigma$ of the linear forms by $S$, that is set $z = S(z')$, then the matrix of $\mathfrak{M}^{*'}_{\lambda-1}$ achieves the form $RAS$, *i.e.*

$$\mathfrak{M}^{*'}_{\lambda-1} = (e_{\lambda-1,1}\, z'_1, \ldots, e_{\lambda-1,p}\, z'_p).$$

Thus we obtain immediately a basis of the corresponding fundamental ideal

$$\mathfrak{G}^{*'}_{\lambda-1} = (z'_1, \ldots, z'_p).$$

By back-substitution of the transformation, which is permitted because $S$ has a nonzero determinant independent of $x_\lambda$, we obtain a basis for $\mathfrak{G}^{*'}_{\lambda-1}$ in the primal variable $z$

$$\mathfrak{G}^{*'}_{\lambda-1} = (k_1, \ldots, k_p),$$

where the $k_i$ can be viewed as linear forms in the $z$'s with coefficients in $\mathbb{P}[x_\lambda, \ldots, x_n]$.

(b) *Computation of* $\mathfrak{g}_{\lambda-1}$ *in* $\mathfrak{G}^{*'}_{\lambda-1}$.

Since $\mathfrak{G}^{*'}_{\lambda-1}$ and $\mathfrak{G}^*_{\lambda-1}$ were formed by adjoining $x_{\lambda-1}, \ldots, x_n$, the linear forms in $\mathfrak{G}^{*'}_{\lambda-1}$, whose coefficients belong to $\mathbb{P}[x_\lambda, \ldots, x_n]$, are divisible by the $\lambda$-th fundamental ideal of $\mathfrak{g}_{\lambda-1}$, which is identical to $\mathfrak{g}_{\lambda-1}$. Thus they consist of all $g$ for which

$$1. \quad g \equiv 0 \ (\mathfrak{g}_{\lambda-1}) \qquad\qquad 2. \quad [g] \leq n_{\lambda-1}.$$

Therefore, $k_i \equiv 0 \ (\mathfrak{g}_{\lambda-1})$ and $[k_i] \leq n_{\lambda-1}$, where $k_i$ may still be assumed to be integral in the transformation coefficients. Let

$$|U|^\gamma k_i = U_p k_{i1} + \ldots + U_n k_{in},$$

where the $U_j$ are power products of the transformation coefficients $u_{\mu\nu}$, while the $k_{ij}$ will be independent of the $u_{\mu\nu}$ after the inverse transformation. Since $\mathfrak{g}_{\lambda-1}$ is transformed, $k_{ij} \equiv 0\ (\mathfrak{g}_{\lambda-1})$ and $[k_{ij}] \leq n_{\lambda-1}$. Therefore,

$$(k_{11}, \ldots, k_{pn}) \equiv 0 \quad (\mathfrak{G}_{\lambda-1}^{*'}).$$

On the other hand,

$$(\mathfrak{G}_{\lambda-1}^{*'}) \equiv 0 \quad (k_{11}, \ldots, k_{pn}),$$

so

$$(\mathfrak{G}_{\lambda-1}^{*'}) = (k_{11}, \ldots, k_{pn}).$$

Now we again set the power products $x_1, \ldots, x_{\lambda-1}$ equal to the $z_\sigma$ and view $\mathfrak{k} = (k_{11}, \ldots, k_{pn})$ as the ideal in $\mathbb{P}[x_1, \ldots, x_n]$ which is transformed after construction of its basis.

Let

$$g \equiv 0 \quad (\mathfrak{g}_{\lambda-1}).$$

Since by the Corollary to Theorem 6, $\mathfrak{G}_{\lambda-1}^{*}$, and hence $(\mathfrak{G}_{\lambda-1}^{*'})$ as well, already contains a basis for $\mathfrak{g}_{\lambda-1}$, there exists $a^{(\lambda+1)} \neq 0$ such that

$$a^{(\lambda+1)} g \equiv 0 \quad (\mathfrak{k}).$$

Conversely, if

$$a^{(\lambda+1)} g \equiv 0 \quad (\mathfrak{k}),$$

then

$$g \equiv 0 \quad (\mathfrak{g}_{\lambda-1}).$$

This means therefore that since $\mathfrak{k}$ is transformed, $\mathfrak{g}_{\lambda-1}$ is the $\lambda$-th fundamental ideal of $\mathfrak{k}$. Now by hypothesis, the $\lambda$-th fundamental ideal can be computed in finitely many steps. Therefore, $\mathfrak{g}_{\lambda-1}$, and hence every fundamental ideal of $\mathfrak{m}$ as well, can be computed in finitely many steps. □

**Corollary to Theorem 8.** *Set*

$$E_{\varrho-1}^{(\varrho)} = e_{\varrho-1,p}, \qquad R_{\varrho-1}^{(\varrho)} = \prod_{i=1}^{p} e_{\varrho-1,i}.$$

*Without loss of generality, we may assume that $E_{\varrho-1}^{(\varrho)}$ and $R_{\varrho-1}^{(\varrho)}$ are integral and primitive*[16] *in $x_{\varrho-1}, \ldots, x_n$. Then*

$$E = \prod_{i=1}^{n} E_{\varrho-1}^{(\varrho)}$$

[16]Translator's Note: The coefficients are relatively prime.

*is the elementary divisor form of* $\mathfrak{m}$ *and*

$$R = \prod_{i=1}^{n} R_{\varrho-1}^{(\varrho)}$$

*is the norm of* $\mathfrak{m}$.

These are both important polynomials to recover for characterizing ideals by their zeros.

By [9, Theorem 11], the norm of $\mathfrak{m}$ can be factored

$$\begin{aligned} R &= \prod_{i,v} (x_i - t_{1i}\overline{y}_{1v} - \ldots - t_{ni}\overline{y}_{nv})^{\delta} \\ &= \prod_{i,v} \left[t_{1i}(y_1 - \overline{y}_{1v}) + \ldots + t_{ni}(y_n - \overline{y}_{nv})\right]^{\delta}, \end{aligned}$$

where the $t_{ij}$ denote coefficients of the inverse transformation $U^{-1}$, and the $\overline{y}_{1v}, \ldots, \overline{y}_{nv}$ run through a complete zero-set of the non-transformed ideal $\overline{m}$ that is independent of the $t_{ij}$. By §2, the above factorization of the norm, and hence the computation of the complete set of zeros, can be carried out in finitely many steps.

# §7. Prime Ideals

Although the methods up to now, with the exception of the factoring of polynomials in §2, have required absolutely no consideration of the special properties of the original field, whether the field is perfect or imperfect is essential for computing the associated prime ideals of $\mathfrak{m}$. The reason for this lies in the theorems cited in §1.5, by which we can conclude from the fact that if the original field is perfect then the elementary divisor form is a prime function, that the ideal is prime, whereas this conclusion is not permissible in imperfect fields. Now since by previous computations, the elementary divisor forms of the desired prime ideals are known to be prime factors of the norm [9, Theorem 10], but we know nothing else about these prime ideals, the computation of their basis must originate from their elementary divisor form, and here a distinction will be made in the computation of prime ideals between perfect and imperfect fields. Theorem 9 gives the methods which will be applied in both cases. For perfect fields, this takes care of everything, but for imperfect fields, one further calculation that is given in Theorem 10 will be necessary. Theorem 11 then ties both together and applies the discovered methods to specific prime ideals of the given ideal.

**Theorem 9.** *Hypothesis: Let the prime function* $P^{(\varrho)}$ *be the elementary divisor form of the transformed prime ideal* $\mathfrak{p}$ *of dimension* $n - \varrho$ *in* $\mathbb{P}[x_1, \ldots, x_n] = \overline{\mathbb{P}}(u)[x_1, \ldots, x_n]$. *Let* $P$ *be the polynomial obtained by the inverse transformation*

*$x = U^{-1}(y)$ and multiplication by $|U|^\gamma = |u_{\mu\nu}|^\gamma$, which is integral in the $u_{\mu\nu}$. Let*

$$P = \sum_{\lambda=1}^{l} U_\lambda P_\lambda,$$

*where $U_\lambda$ are power products of the transformation coefficients $u_{\mu\nu}$ and the $P_\lambda$ are elements of $\overline{\mathbb{P}}[y_1, \ldots, y_n]$. Then*

$$\bar{\mathfrak{r}} = (P_1, \ldots, P_l)$$

*is an ideal in $\overline{\mathbb{P}}[y_1, \ldots, y_n]$. Let $\mathfrak{r}$ be its transformed ideal resulting from the transformation, and $\mathfrak{p}'$ the $\varrho$-th fundamental ideal of $\mathfrak{r}$.*
*Claim: $\mathfrak{p} = \mathfrak{p}'$ if $\overline{\mathbb{P}}$ is a perfect field. Otherwise, $\mathfrak{p}'$ is only an associated primary ideal of $\mathfrak{p}$.*

*Proof.* Since $P^{(\varrho)} \equiv 0\ (\mathfrak{r})$, the 1st to $(\varrho - 1)$-th fundamental ideal of $\mathfrak{r}$ are equal to the unit ideal $\mathfrak{o}$. The same is true for $\mathfrak{p}'$ because $\mathfrak{r} \equiv 0(\mathfrak{p}')$. But since $\mathfrak{p}'$ is the $\varrho$-th fundamental ideal of $\mathfrak{r}$, it is identical to its $\varrho$-th fundamental ideal. Therefore, only one of the highest level elementary divisors of $\mathfrak{p}'$ is not the identity, and all of the associated prime ideals of $\mathfrak{p}'$ have dimension $n - \varrho$.

Now since $P^{(\varrho)} \equiv 0\ (\mathfrak{p}')$, $P^{(\varrho)}$ is a multiple of the elementary divisor form of $\mathfrak{p}'$, which is either $P^{(\varrho)}$ or the identity $E$ because $P^{(\varrho)}$ is a prime function.

Suppose the elementary divisor form of $\mathfrak{p}'$ were $E$. Then $\mathfrak{p}' = \mathfrak{o}$;, *i.e.* there exists a polynomial

$$G^{(\varrho+1)} \neq 0$$

such that

$$G^{(\varrho+1)} \equiv 0\ (\mathfrak{r}).$$

By definition of $\bar{\mathfrak{r}}$, it follows clearly from $P^{(\varrho)} \equiv 0\ (\mathfrak{p})$ that $\bar{\mathfrak{r}} \equiv 0\ (\overline{\mathfrak{p}})$, where $\overline{\mathfrak{p}}$ is the associated non-transformed ideal of $\mathfrak{p}$. Thus, $\bar{\mathfrak{r}} \equiv 0\ (\mathfrak{p})$ as well. Therefore,

$$G^{(\varrho+1)} \equiv 0\ (\mathfrak{p}).$$

Thus $\mathfrak{p}$ would have dimension at most $n - \varrho - 1$, contradicting the hypothesis. Hence the assumption was false and $P^{(\varrho)}$ is the elementary divisor form of $\mathfrak{p}'$.

Now if $\overline{\mathbb{P}}$ is a perfect field, then by [9, Theorem 13], $\mathfrak{p}'$ is a prime ideal whose elementary divisor form coincides with $\mathfrak{p}$. Since the zeros of the ideal are determined from the elementary divisor form, both prime ideals have the same zeros, so they are identical. If $\overline{\mathbb{P}}$ is imperfect, then we can conclude that $\mathfrak{p}'$ is a primary ideal. Since $\mathfrak{p}'$ has the same zeros as $\mathfrak{p}$, $\mathfrak{p}$ is the associated prime ideal of $\mathfrak{p}'$. □

**Example.** The example at the end of [9, §6] shows that $\mathfrak{p}'$ can be a proper primary ideal in the case of imperfect fields.

Let $\overline{\mathbb{P}}$ be the residue class field mod 2, to which the indeterminate $\lambda$ is adjoined. $n = 2$. Let $\overline{\mathfrak{p}} = (y_1^2 + \lambda, y_1 + y_2)$ be the non-transformed ideal.

Then $\mathfrak{p} = ((u_{11}x_1 + u_{12}x_2)^2 + \lambda, x_1(u_{11} + u_{21}) + x_2(u_{12} + u_{22}))$. The resulting elementary divisor form is

$$P^{(2)} = x_2^2 + \lambda(t_{12}^2 + t_{22}^2),$$

where $t_{ij}$ are the coefficients of the inverse transformation $U^{-1}$. Since $n = 2$, ideals which have $P^{(2)}$ as the first elementary divisor not equal to the identity have $P^{(2)}$ as the only elementary divisor. Since $P^{(2)}$ is a prime function, these ideals are primary ideals. Thus in the notation of Theorem 9, $\mathfrak{r} = \mathfrak{p}'$. Using $x = U^{-1}y$, we obtain from $P^{(2)}$

$$P = t_{12}^2(y_1^2 + \lambda) + t_{22}^2(y_2^2 + \lambda).$$

Therefore using $y = U(x)$, $\mathfrak{p}'$ corresponds to the ideal

$$(y_1^2 + \lambda,\ y_2^2 + \lambda) = \left(y_1^2 + \lambda,\ (y_1 + y_2)^2\right).$$

But this is easily seen to be a proper, associated primary ideal of $\bar{\mathfrak{p}}$, since it contains $(y_1 + y_2)^2$, but not $(y_1 + y_2)$. Of course, the corresponding result holds for the transformed ideal.

Now to prove Theorem 10, two lemmas are necessary.

**Lemma 5.** *Hypothesis: Suppose* $\mathfrak{q}$ *is an ideal in* $\mathfrak{R} = \mathbb{P}[x_1, \ldots, x_n]$*, where* $x_i$ *is algebraic or transcendental over* $\mathbb{P}[x_1, \ldots, x_{i-1}]$*. Let* $\mathfrak{q}'$ *be the ideal in* $\mathbb{P}(x_n)[x_1, \ldots, x_{i-1}]$ *whose basis elements agree with those of* $\mathfrak{q}$*. The elements of* $\mathbb{P}[x_1, \ldots, x_n]$ *belonging to* $\mathfrak{q}'$ *are divisible by* $\mathfrak{q}$*. Then* $\mathfrak{q}$ *and* $\mathfrak{q}'$ *are uniquely determined from each other.*
*Claim: If* $\mathfrak{q}$ *is a prime or primary ideal, then so is* $\mathfrak{q}'$*, and conversely.*

*Proof.*

1. *Suppose* $\mathfrak{q}$ *is a primary ideal.*

Suppose $a'b' \equiv 0\ (\mathfrak{q}')$, but $b'^{\kappa} \not\equiv 0\ (\mathfrak{q}')$ for every $\kappa$. Then there exist polynomials $f(x_n)$ and $g(x_n)$ such that

$$fa' \equiv 0 \quad (\mathbb{P}[x_1, \ldots, x_n]) \qquad \text{and} \qquad gb' \equiv 0 \quad (\mathbb{P}[x_1, \ldots, x_n]).$$

Thus

$$fa'gb' \equiv 0 \quad (\mathfrak{q}).$$

But since it follows directly from

$$g^{\kappa}b'^{\kappa} \equiv 0 \quad (\mathfrak{q})$$

that $b'^{\kappa} \equiv 0\ (\mathfrak{q}')$,

$$(gb')^{\kappa} \not\equiv 0 \quad (\mathfrak{q})$$

for every $\kappa$. Since $\mathfrak{q}$ is primary, it follows that

$$fa' \equiv 0\ (\mathfrak{q}),$$

and thereby

$$a' \equiv 0 \ (\mathfrak{q}'),$$

*i.e.* $\mathfrak{q}'$ is primary.

2. *Suppose* $\mathfrak{q}'$ *is a primary ideal.*

It follows from

$$ab \equiv 0 \quad (\mathfrak{q}) \qquad b^\kappa \not\equiv 0 \quad (\mathfrak{q})$$

for every $\kappa$ that

$$ab \equiv 0 \quad (\mathfrak{q}') \qquad b^\kappa \not\equiv 0 \quad (\mathfrak{q}')$$

for every $\kappa$. Thus by hypothesis,

$$a \equiv 0 \quad (\mathfrak{q}'),$$

and hence

$$a \equiv 0 \quad (\mathfrak{q})$$

as well, *i.e.* $\mathfrak{q}$ is a primary ideal.

If we set $\kappa$ equal to 1 in this proof, we obtain: if $\mathfrak{q}$ is a prime ideal, then so is $\mathfrak{q}'$, and conversely. □

**Lemma 6.** *Hypothesis: Let* $\mathfrak{q}$ *be an ideal in* $\mathbb{P}[x_1, \ldots, x_n]$*, where* $x_i$*,* $i = 1, \ldots, n$*, are transcendental over* $\mathbb{P}[x_1, \ldots, x_{i-1}]$*. Let* $P^{(n)}(x_n)$ *be a prime function such that*

$$P^{(n)}(x_n) \equiv 0 \quad (\mathfrak{q}).$$

*Let* $\xi_n$ *be algebraic over* $\mathbb{P}$*, and in particular, let*

$$P^{(n)}(\xi_n) = 0.$$

*Then* $\mathbb{P}[x_1, \ldots, x_n, \xi_n]$ *is a ring without zero divisors. Let* $\mathfrak{q}'$ *be the ideal in* $\mathbb{P}[x_1, \ldots, x_n, \xi_n]$ *whose basis elements are formed from those of* $\mathfrak{q}$ *by substituting* $\xi_n$ *for* $x_n$*. Then conversely, the basis elements of* $\mathfrak{q}$ *are formed from those of* $\mathfrak{q}'$ *by substituting* $x_n$ *for* $\xi_n$ *and adding* $P^{(n)}(x_n)$ *to the basis.*
*Claim: If* $\mathfrak{q}$ *is a prime or primary ideal, then so is* $\mathfrak{q}'$*, and conversely.*

*Proof.* The proof is carried out exactly like the proof of Lemma 5. However, it results from the following additional consideration: $\mathfrak{q}$ is prime or primary if and only if the same is true for the ring $\mathfrak{o}/\mathfrak{q}$, *i.e.* if it has no zero divisors, or if a power of every zero divisor vanishes, respectively. The substitution of $\xi_n$ for $x_n$ means passage to the residue class mod $\left(P^{(n)}(x_n)\right)$. Therefore

$$\mathfrak{o} \Big/ \left(P^{(n)}(x_n)\right) = \mathfrak{o}' \qquad \mathfrak{q} \Big/ \left(P^{(n)}(x_n)\right) = \mathfrak{q}'.$$

Now it is known that $\mathfrak{o}/\mathfrak{q}$ and $\mathfrak{o}'/\mathfrak{q}'$ are isomorphic. (Both residue classes of zero contain the same elements when reduced by elements in $\mathfrak{o}$.) Therefore, if $\mathfrak{o}/\mathfrak{q}$ is

prime or primary, then so is $\mathfrak{o}'/\mathfrak{q}'$, *i.e.* if $\mathfrak{q}$ is a prime or primary ideal, then so is $\mathfrak{q}'$, and conversely. □

**Theorem 10.** *Hypothesis: Let* $\mathfrak{q}$ *be a prime ideal in* $\mathbb{P}[x_1, \ldots, x_n]$ *whose elementary divisor form is a prime function* $P^{(\varrho)}$. *Thus* $\mathfrak{q}$ *is a prime ideal if* $\mathbb{P}$ *is perfect.*
*Claim: A basis of the associated prime ideals* $\mathfrak{p}$ *of* $\mathfrak{q}$ *can be computed in finitely many steps.*

*Proof* (by induction). 1. $n = 1$. $\mathfrak{q}$ is a principal ideal, $\mathfrak{q} = (Q)$. It follows from $P^{(\varrho)} \equiv 0\ (\mathfrak{q})$ that $P^{(\varrho)} \equiv 0\ (Q)$. Then since $P^{(\varrho)}$ is a prime function, either $Q = P^{(\varrho)}$ or $Q = E$. But $Q \neq E$, since otherwise $\mathfrak{q} = \mathfrak{o}$, contradicting the hypothesis that $P^{(\varrho)} \neq E$ is the elementary divisor form. Thus $\mathfrak{q} = \left(P^{(\varrho)}\right)$. Therefore, since $P^{(\varrho)}$ is a prime function, $\mathfrak{q}$ is also a prime ideal.

2. Assume the theorem is already proved for $n = r - 1$. Let $n = r$. As shown in §1, it suffices to prove the theorem for transformed ideals, because the unique calculation of prime ideals for non-transformed ideals is given with it. So in what follows, let $\mathfrak{q}$ be transformed.

(a) Suppose $\mathfrak{q}$ has dimension greater than 0. $\varrho \neq r$. Let $\mathfrak{q}'$ be the ideal in $\mathbb{P}(x_r)[x_1, \ldots, x_{r-1}]$ formed by adjoining $x_r$ to $\mathfrak{q}$. Then the polynomials in $\mathfrak{q}'$ belonging to $\mathbb{P}[x_1, \ldots, x_r]$ form the $(r-1)$-th fundamental ideal of $\mathfrak{q}$, which coincides with $\mathfrak{q}$ since $\mathfrak{q}$ has dimension at least 1. By Lemma 5, $\mathfrak{q}'$ is a prime ideal in $\mathbb{P}(x_r)[x_1, \ldots, x_{r-1}]$. Since the zeros of $\mathfrak{q}$ agree with those of $\mathfrak{q}'$, the elementary divisor form of $\mathfrak{q}'$ is a primary function corresponding to $P^{(\varrho)}$, which is identical to $P^{(\varrho)}$ because $P^{(\varrho)} \equiv 0\ (\mathfrak{q}')$. Then by hypothesis, the basis elements of the associated prime ideals of $\mathfrak{q}$ can be computed in finitely many steps. Let $\mathfrak{p}' = (p_1, \ldots, p_v)$, where the $p_i$, $i = 1, \ldots, v$, may be assumed to be elements of $\mathbb{P}[x_1, \ldots, x_r]$.

$\mathfrak{p}$ contains precisely the polynomials in $\mathfrak{p}'$ belonging to $\mathbb{P}[x_1, \ldots, x_r]$. By Lemma 5, $\mathfrak{p}$ is a prime ideal. It follows from

$$\mathfrak{q}' \equiv 0 \quad (\mathfrak{p}') \qquad \text{and} \qquad \mathfrak{p}'^{\kappa} \equiv 0 \quad (\mathfrak{p}')$$

that

$$\mathfrak{q} \equiv 0 \quad (\mathfrak{p}) \qquad \text{and} \qquad \mathfrak{p}^{\kappa} \equiv 0 \quad (\mathfrak{p}).$$

Then divisibility remains unchanged when $x_r$ is adjoined, and if the ideal $\mathfrak{t}$ consists of all polynomials of $\mathfrak{p}'^{\kappa}$ lying in $\mathbb{P}[x_1, \ldots, x_r]$, then certainly $\mathfrak{p}^{\kappa} \equiv 0\ (\mathfrak{t})$ since every polynomial divisible by $\mathfrak{p}$ is also divisible by $\mathfrak{p}'$.

Thus $\mathfrak{p}$ is the associated prime ideal of $\mathfrak{q}$, so $\mathfrak{p}$ is transformed. Now a basis for $\mathfrak{p}$ can be computed from the basis elements of $\mathfrak{p}'$. If $p \equiv 0\ (\mathfrak{p})$, and $|U|^{\gamma} p = U_1 p_1 + \ldots + U_\mu p_\mu$ is a decomposition of $p$ into transformed components $p_i$ such that the $U_i$ are power products of the transformation coefficients and the $p_i$ will be independent of these after the inverse transformation, then since $\mathfrak{p}$ is transformed, $p_i \equiv 0\ (\mathfrak{p})$, and hence $p_i \equiv 0\ (\mathfrak{p}')$ as well. Then the basis elements $(p_1, \ldots, p_v)$ of $\mathfrak{p}'$ can be chosen so that they will be independent from the

transformation coefficients after the inverse transformation. Thus $(p_1, \ldots, p_v)$ is a transformed ideal in $\mathbb{P}[x_1, \ldots, x_r]$ consisting of all polynomials in $\mathfrak{p}'$ belonging to $\mathbb{P}[x_1, \ldots, x_r]$. Thus the elements of $\mathfrak{p}$ form the $(r-1)$-th fundamental ideal of $(p_1, \ldots, p_v)$, which can be computed in finitely many steps by Theorem 8.

(b) Suppose $\mathfrak{q}$ has dimension 0. Then the prime function $P^{(r)}(x_r)$ is a function of $x_r$ alone. Let $\xi_r$ be an element algebraically dependent on $\mathbb{P}$ by the equation $P^{(r)}(\xi_r) = 0$. Let $\mathfrak{q}'$ be the ideal in $\mathbb{P}[x_1, \ldots, x_{r-1}, \xi_r]$ formed from $\mathfrak{q}$ by passing to the set of residue classes modulo $P^{(r)}(x_r)$, in which $\xi_r$ and $x_r$ are interchanged in $\mathfrak{q}$. By Lemma 6, $\mathfrak{q}'$ is a primary ideal. By adjoining $\xi_r$ to the field $\mathbb{P}$, $\mathfrak{q}'$ is mapped to an ideal $\mathfrak{q}''$. The set of all polynomials in $\mathfrak{q}''$ which are integral in $\xi_r$ is divisible by $\mathfrak{q}'$. In particular, if

$$g(x_1, \ldots, x_{r-1}, \xi_r) \equiv 0 \quad (\mathfrak{q}''),$$

then it follows that

$$F(\xi_r) g(x_1, \ldots, x_{r-1}, \xi_r) \equiv 0 \quad (\mathfrak{q}'),$$

where

$$F(\xi_r) \neq 0.$$

Hence it follows that

$$F(x_r) g(x_1, \ldots, x_{r-1}, x_r) \equiv 0 \quad (\mathfrak{q})$$

and

$$F(x_r) \not\equiv 0 \quad \left(P^{(r)}(x_r)\right).$$

Since $P^{(r)}(x_r)$ is a prime function, it follows that $F^\kappa(x_r) \not\equiv 0 \ \left(P^{(r)}(x_r)\right)$ for every $\kappa$. Since $P^{(r)}(x_r)$ is, as the elementary divisor form of $\mathfrak{q}$, the greatest common divisor of all polynomials in $\mathfrak{q}$ dependent only on $x_r$, it follows that $F^\kappa(x_r) \not\equiv 0 \ (\mathfrak{q})$ for every $\kappa$. Thus $g(x_1, \ldots, x_{r-1}, x_r) \equiv 0 \ (\mathfrak{q})$, and hence $g(x_1, \ldots, x_{r-1}, \xi_r) \equiv 0 \ (\mathfrak{q}')$ as well. Thus by Lemma 5, $\mathfrak{q}''$ is a primary ideal.

The elementary divisor form of $\mathfrak{q}''$ is a power of a prime function, and in fact not always the first power. By Theorem 1, the corresponding prime function can be computed in finitely many steps, and by Theorem 9, we can find the basis of a primary ideal $\mathfrak{q}'''$ whose elementary divisor form is this prime function, which therefore belongs to the same prime ideal as $\mathfrak{q}''$. By hypothesis, the associated prime ideal $\mathfrak{p}''$ of $\mathfrak{q}'''$ , and hence of $\mathfrak{q}''$, can be computed in finitely many steps.

Let $\mathfrak{p}'' = (p_1(x_1, \ldots, x_{r-1}, \xi_r), \ldots, p_v(x_1, \ldots, x_{r-1}, \xi_r))$. Without loss of generality, the $p_i$ can be assumed to be integral in $\xi_r$. Let

$$\begin{aligned} |U|^{\gamma_i} p_i(x_1, \ldots, x_{r-1}, x_r) &= U_1 p_{i1}(x_1, \ldots, x_r) + \ldots + U_\mu p_{i\mu}(x_1, \ldots, x_r) \\ |U|^{\gamma} P^{(r)}(x_r) &= U_1 P_1(x_1, \ldots, x_r) + \ldots + U_\mu P_\mu(x_1, \ldots, x_r) \end{aligned}$$

be the decomposition of these polynomials into transformed components. Let $\mathfrak{p}' = (p_{11}(x_1, \ldots, x_r), \ldots, p_{v\mu}(x_1, \ldots, x_r), P_1(x_1, \ldots, x_r), \ldots, P_\mu(x_1, \ldots, x_r))$ be an ideal in $\mathbb{P}[x_1, \ldots, x_r]$. By construction, $\mathfrak{p}'$ is clearly a transformed ideal. We must still show that $\mathfrak{p}'$ is the desired associated prime ideal $\mathfrak{p}$ of $\mathfrak{q}$. In particular:

1. $\mathfrak{p}' \equiv 0\ (\mathfrak{p})$, for it follows from
$$p_i(x_1, \ldots, x_{r-1}, \xi_r) \equiv 0 \quad (\mathfrak{p}'')$$
that
$$p_i^{\kappa}(x_1, \ldots, x_{r-1}, \xi_r) \equiv 0 \quad (\mathfrak{q}'').$$
By what was proved about $\mathfrak{q}''$, it follows from
$$p_i^{\kappa}(x_1, \ldots, x_{r-1}, x_r) \equiv 0 \quad (\mathfrak{q})$$
that
$$p_i(x_1, \ldots, x_{r-1}, x_r) \equiv 0 \quad (\mathfrak{p}).$$
Furthermore, since $P^{(r)}(x_r) \equiv 0\ (\mathfrak{p})$, and since as a transformed ideal, $\mathfrak{p}$ contains a polynomial and also its transformed components, $\mathfrak{p} \equiv 0\ (\mathfrak{p}')$.

2. $\mathfrak{p}'$ is a primary ideal. Indeed, since $\mathfrak{p}'$ is transformed, it follows from $P^{(r)}(x_r) \equiv 0\ (\mathfrak{p}')$ that $\mathfrak{p}'$ has dimension at most 0, and from $\mathfrak{p} \neq \mathfrak{o}$ and $\mathfrak{p}' \equiv 0\ (\mathfrak{p})$ that it has dimension exactly equal to 0. So since $P^{(r)}(x_r)$ is a prime function, it is the elementary divisor form of $\mathfrak{p}'$. Thus $\mathfrak{p}'$ is a primary ideal, and $P^{(r)}(x_r)$ is the greatest common divisor of all polynomials in $\mathfrak{p}'$ dependent only on $x_r$.

3. $\mathfrak{p} \equiv 0\ (\mathfrak{p}')$. In particular, suppose $p(x_1, \ldots, x_{r-1}, x_r) \equiv 0\ (\mathfrak{p})$. Then either $p(x_1, \ldots, x_{r-1}, x_r) \equiv 0\ \big(P^{(r)}(x_r)\big)$, so then clearly $p_i(x_1, \ldots, x_{r-1}, x_r) \equiv 0\ (\mathfrak{p}')$; or $p(x_1, \ldots, x_{r-1}, x_r) \not\equiv 0\ \big(P^{(r)}(x_r)\big)$, so $p(x_1, \ldots, x_{r-1}, \xi_r) \equiv 0\ (\mathfrak{p}'')$. But then there exists an $F(x_r)$ such that $F(x)p(x_1, \ldots, x_{r-1}, x_r) \equiv 0\ (\mathfrak{p}')$ and $F(x_r) \not\equiv 0\ \big(P^{(r)}(x_r)\big)$. Therefore, $F^{\kappa}(x_r) \not\equiv 0\ (P^{(r)}(x_r))$ for every $\kappa$, and as remarked in 2, $P^{(r)}(x_r) \not\equiv 0\ (\mathfrak{p}')$ for every $\kappa$. Since $\mathfrak{p}'$ is a primary ideal, it follows that $p(x_1, \ldots, x_{r-1}, x_r) \equiv 0\ (\mathfrak{p}')$, and therefore $\mathfrak{p} \equiv 0\ (\mathfrak{p}')$.

1 and 3 yield $\mathfrak{p} = \mathfrak{p}'$. Therefore, since the basis of $\mathfrak{p}'$ is known, so is the basis of $\mathfrak{p}$. □

**Theorem 11.** *The associated prime ideals of an ideal* $\mathfrak{m}$ *can be computed in finitely many steps.*

*Proof.* By [9, Theorem 10], the elementary divisor forms of the associated prime ideals of $\mathfrak{m}$ are the prime functions which belong to the primary factors of the individual norms $\mathfrak{N}^{(i)}$ of $\mathfrak{m}$. Theorem 8 permits the computation of the $\mathfrak{N}^{(i)}$ in finitely many steps and §2 gives methods for calculating the corresponding prime factors. By Theorem 9, an ideal can be computed for each such prime function, which is an associated prime ideal of $\mathfrak{m}$ in perfect fields, and is, at the very least, an associated primary ideal of this prime ideal in imperfect fields, whose elementary divisor form is a prime function. By Theorem 10, the corresponding prime ideal can also be computed in the latter case. Thus Theorems 9 and 10 produce the methods by which we can find the prime ideals in finitely many steps. □

# §8. Primary Ideals and Isolated Components

The primary ideals, which appear in a representation of $\mathfrak{m}$ as the least common multiple of the largest primary components, are not unique. So we can deal only with the computation of any one possible set of primary ideals in such a representation.

Let $\mathfrak{p}_{\varrho\sigma}$ be an associated $(n-\varrho)$-dimensional prime ideal of $\mathfrak{m}$. If $\lambda$ is greater than the exponent of any associated primary ideal $\mathfrak{q}$ of $\mathfrak{p}_{\varrho\sigma}$ that can appear in a representation of $\mathfrak{m}$, then the $\varrho$-th fundamental ideal of $(\mathfrak{m}, \mathfrak{p}_{\varrho\sigma}^{\lambda})$ is also such an ideal. Thus to compute the primary ideal, it suffices to find an upper bound for $\lambda$. It will be shown that the number $\kappa(t, q, n)$ computed in Hentzelt's Nullstellensatz is such a bound.

This bound certainly reaches much higher than is necessary. This is shown in the simple example

$$\mathfrak{m} = (x^2, xy) = [(x), (x^2, y)].$$

The associated prime ideals of $\mathfrak{m}$ are $(x)$, and $(x, y)$. Hence the exponents of the primary ideal that can appear are all at most 2. Thus $\lambda = 2$ suffices for the present case, whereas Theorem 5 produces $\kappa(2, 2, 2) = 256$.

**Theorem 12** *Hypothesis: Let $\mathfrak{p}_{\varrho 1}, \ldots, \mathfrak{p}_{\varrho m_\varrho}$, $\varrho = 1, \ldots, n$, be the associated $(n-\varrho)$-dimensional prime ideals of $\mathfrak{m}$. Let $\kappa = \kappa(t, q, n)$ be the number computed in Theorem 5. Let $\mathfrak{q}_{\varrho\sigma}$ be the $\varrho$-th fundamental ideal of $(\mathfrak{m}, \mathfrak{p}_{\varrho\sigma}^{\kappa})$. Thus $\mathfrak{q}_{\varrho\sigma}$ is an associated prime ideal of $\mathfrak{p}_{\varrho\sigma}$. As a fundamental ideal of a transformed ideal, it is itself transformed.*
*Claim:* $\mathfrak{m} = [\mathfrak{q}_{11}, \ldots, \mathfrak{q}_{nm_n}]$.

*Proof.* Let $\xi_{\varrho\sigma}^1, \ldots, \xi_{\varrho\sigma}^n$ be zeros of the prime ideal $\mathfrak{p}_{\varrho\sigma}$ of transcendence degree $n - \varrho$. So $\xi_{\varrho\sigma}^{\varrho+1}, \ldots, \xi_{\varrho\sigma}^n$ are transcendental over $\mathbb{P}$.

Then $\mathfrak{o}_{\varrho\sigma} = (x_1 - \xi_{\varrho\sigma}^1, \ldots, x_n - \xi_{\varrho\sigma}^n)$ is the associated zero-set ideal of these zeros. It is a 0-dimensional prime ideal in $\mathbb{P}(\xi_{\varrho\sigma}^1, \ldots, \xi_{\varrho\sigma}^n)[x_1, \ldots, x_n]$, and

$$\mathfrak{p}_{\varrho\sigma} \equiv 0 \quad (\mathfrak{o}_{\varrho\sigma}),$$

so

$$(\mathfrak{m}, \mathfrak{p}_{\varrho\sigma}^{\kappa}) \equiv 0 \quad (\mathfrak{m}, \mathfrak{o}_{\varrho\sigma}^{\kappa}).$$

In order to apply Theorem 5, we need only show that the fundamental ideal $\mathfrak{q}_{\varrho\sigma}$ is divisible by $(\mathfrak{m}, \mathfrak{o}_{\varrho\sigma}^{\kappa})$.

Since $(\mathfrak{m}, \mathfrak{o}_{\varrho\sigma}^{\kappa}) \equiv 0$ $(\mathfrak{o}_{\varrho\sigma})$ and $\mathfrak{o}_{\varrho\sigma}^{\kappa} \equiv 0$ $(\mathfrak{m}, \mathfrak{o}_{\varrho\sigma}^{\kappa})$, and since $\mathfrak{o}_{\varrho\sigma}$ has dimension 0, $(\mathfrak{m}, \mathfrak{o}_{\varrho\sigma}^{\kappa})$ is an associated primary ideal of $\mathfrak{o}_{\varrho\sigma}$.

$(\mathfrak{m}, \mathfrak{o}_{\varrho\sigma}^{\kappa})$ contains no nonzero polynomials free of $x_1, \ldots, x_\varrho$. In particular, if $G^{(\varrho+1)}(x_{\varrho+1}, \ldots, x_n) \not\equiv 0$, then since $\xi_{\varrho\sigma}^{\varrho+1}, \ldots, \xi_{\varrho\sigma}^n$are transcendental over $\mathbb{P}$, $G^{(\varrho+1)}(\xi_{\varrho\sigma}^{\varrho+1}, \ldots, \xi_{\varrho\sigma}^n) \neq 0$, *i.e.* $G^{(\varrho+1)}(x_{\varrho+1}, \ldots, x_n) \not\equiv 0$ $(\mathfrak{o}_{\varrho\sigma})$, so $G^{(\varrho+1)}(x_{\varrho+1}, \ldots, x_n) \not\equiv 0$ $(\mathfrak{m}, \mathfrak{o}_{\varrho\sigma}^{\kappa})$.

Now let $g \equiv 0\ (\mathfrak{q}_{\varrho\sigma})$. Then there exists an $f^{(\varrho+1)} \neq 0$ such that $f^{(\varrho+1)}g \equiv 0\ (\mathfrak{m}, \mathfrak{p}^{\kappa}_{\varrho\sigma})$. Then $f^{(\varrho+1)}g \equiv 0\ (\mathfrak{m}, \mathfrak{o}^{\kappa}_{\varrho\sigma})$. But now since every power of $f^{(\varrho+1)}$ is independent of $x_1, \ldots, x_\varrho$ and therefore not divisible by the primary ideal $(\mathfrak{m}, \mathfrak{o}^{\kappa}_{\varrho\sigma})$, $g \equiv 0\ (\mathfrak{m}, \mathfrak{o}^{\kappa}_{\varrho\sigma})$ and hence

$$\mathfrak{q}_{\varrho\sigma} \equiv 0 \quad (\mathfrak{m}, \mathfrak{o}^{\kappa}_{\varrho\sigma}).$$

Therefore,

$$[\mathfrak{q}_{11}, \ldots, \mathfrak{q}_{nm_n}] \equiv 0 \quad (\mathfrak{m}, \mathfrak{o}^{\kappa}_{ij}),$$

where $\mathfrak{o}_{ij}$ denotes an arbitrary associated zero-set ideal of $\mathfrak{m}$. Then by Theorem 5,

$$[\mathfrak{q}_{11}, \ldots, \mathfrak{q}_{nm_n}] \equiv 0 \quad (\mathfrak{m}).$$

On the other hand,

$$\mathfrak{m} \equiv 0 \quad (\mathfrak{q}_{\varrho\sigma}).$$

Hence it follows that

$$\mathfrak{m} \equiv 0 \quad ([q_{11}, \ldots, \mathfrak{q}_{nm_n}]).$$

Therefore,

$$\mathfrak{m} = [\mathfrak{q}_{11}, \ldots, \mathfrak{q}_{nm_n}]. \quad \square$$

The *isolated components* of $\mathfrak{m}$ are now found by combining associated primary ideals of isolated groups under the prime ideals, where an *isolated group* consists of associated prime ideals of $\mathfrak{m}$, and for any associated prime ideal $\mathfrak{p}$ of $\mathfrak{m}$, contains all associated prime ideals of $\mathfrak{m}$ that are also multiples of $\mathfrak{p}$. Since by Theorem 3, we can determine in finitely many steps whether an ideal is divisible by another, we can compute these isolated groups in finitely many steps. If we divide the ideal $\mathfrak{m}$ by the product of $\kappa$-th powers of prime ideals of the complementary group, then we obtain the corresponding isolated components also, since by Theorem 12, $\kappa$ is indeed an upper bound for the exponent of the primary ideals which appear.

# References


[1] Bôcher. *Einführung in die hohere Algebra* [*Introduction to Higher Algebra*].

[2] K. Hentzelt, E. Noether. *Zur Theorie der Polynomideale und Resultanten* [*On the Theory of Polynomial Ideals and Resultants*]. Math. Ann. **88** (1922): 53-79.

[3] D. Hilbert. *Über die Theorie der algebraischen Formen* [*On the Theory of Algebraic Forms*]. Math. Ann. **36** (1890): 476-534.

[4] J. König. *Einleitung in die allgemeine Theorie der algebraischen Grössen* [*Introduction to the General Theory of Algebraic Elements*]. Leipzig, 1903.

[5] L. Kronecker. *Grundzüge einer arithmetischen Theorie der algebraischen Grössen* [*Basic Characteristics of an Arithmetic Theory of Algebraic Elements*], §4. J. f. Math. **92** (1882): 1-122.

[6] E. Lasker. *Zur Theorie der Moduln und Ideale* [*On the Theory of Modules and Ideals*]. Math. Ann. **60** (1905): 20-116.

[7] F. S. Macaulay. *On the Resolution of a Given Modular System into Primary Systems Including Some Properties of Hilbert Numbers*. Math. Ann. **74** (1913): 66-121.

[8] E. Noether. *Idealtheorie in Ringbereichen* [*Ideal Theory in Domains*]. Math. Ann. **83** (1921): 24-66.

[9] E. Noether. *Eliminationstheorie und allgemeine Idealtheorie* [*Elimination Theory and General Ideal Theory*]. Math. Ann. **90** (1923): 229-261.

[10] E. Steinitz. *Algebraische Theorie der Körper* [*Algebraic Theory of Fields*]. J. f. Math. **137** (1910): 167-309.

(Received 29 May 1925)