# Contributions to Constructive Polynomial Ideal Theory XVII: On Henzelt-Noether-Hermann Theory of Finitely Many Steps*

Bodo Renschuch et al.†

Dedicated in friendship to Professor Wolfgang Vogel on his 40th birthday

**Abstract**

To supplement a paper by Seidenberg [29], more errors in Hermann's classical paper [6] are listed in §1. A review of the literature that followed Hermann's paper is given in §2, and §3 describes the connection with papers to be published in this series.

## Contents



*Beiträge zur konstruktiven Theorie der Polynomideale XVII. Zur Hentzelt/Noether/Herrmannschen Theorie der endliche vielen Schritte. *Wissentschaftliche Zeitschrift der Pädagogische Hochschule "Karl Liebknecht" Potsdam* [*Scientific Journal of the "Karl Liebknecht" Teachers College in Potsdam*] **24** (1980), 87-99, **25** (1981): 125-136. Translated by Michael Abramson. Page and line numbers referring to the original German version of [6] have been changed to refer to the English language version published in Volume 32, Number 3 of this publication, where the number after the slash indicates the column.

†Author's address [in 1980]: *Dr. sc. B. Renschuch*, 1532 Kleinmachnow, Wolfswerder 40

# 1 Corrections and Comments on Hentzelt-Noether-Hermann Theory

## 1.1 On the Goals of Hentzelt-Noether-Hermann Theory

In the 16 parts of this series of articles so far (appearing since volume 17 (1973) of this journal and subsequently denoted by I, ..., XVI) and in the book [26], the author has given practical algorithms and results for various operations in polynomial ideal theory. In discussing this, the question has often been raised about how much Emmy Noether and her students already knew about approaches to such ideas, particularly when a critical examination of Grete Hermann's 1926 paper [6] was missing.

This dissertation, supervised and refereed by Emmy Noether, (Department of Mathematics and Natural Science, University of Göttingen, 4 May 1926, second reviewer: E. Landau) goes back to a dissertation by Kurt Hentzelt who died during World War I, that was proposed by E. Fischer in Erlangen (see [5, footnote 1, page53]). Thus Hentzelt's dissertation was never published. The only copy was no longer in Erlangen department records, after it was handed over to Noether to edit (see [25, remarks on p. 63]). This editing and extrapolation resulted in three papers by Hentzelt [5] from 1923, Noether [24] from 1923, and Hermann's just mentioned 1926 dissertation [6] on "the question of finitely many steps". Thus it seems reasonable to speak of Hentzelt-Noether-Hermann theory. The deep aversion to explicit computation held by Noether's contemporaries (see [35, p. 511]; confirmed in discussions with H. Grell and W. Hauser) did not hinder her in recognizing the importance of such ideas, but at the same time, explains why she assigned these parts to a graduate student and missed the errors that occurred there.

Now in what follows, if the discussion must be about the many errors and defects of different types in [6] (Samuel speaks in [29R] of [in translation] "... some minor but troublesome errors"), then it is not clear to what extent they go back to Hentzelt. From Hermann's hint in [6, p. 9] that §§4-6 of Hentzelt's manuscript were removed, we cannot be sure that the contents of §§2-3, 7-8 do not deal with [5], since she refers in other places, for example, to degree bounds (if not explicitly), which had already appeared in [5].

The sign error on [6, p. 746] actually goes back to Hilbert's famous 1890 paper [7, p. 493] and was probably carried over by Hentzelt. But here we must also take into account the situation of a quickly conferred doctorate in August 1914. Nevertheless, it would have been better had greater care been given by all those involved during the editing.

Henzelt-Noether-Hermann theory [6] does not deal with producing practical procedures (as in this series of articles), but rather with the proof that such algorithms exist. The existence of these algorithms remained open for Hermann and was first proved by Reufel in [28] (see also §2.4). By passing to transformed ideals, practical computation was made impossible, which is considered essential for computing fundamental ideals and from that the normal primary decomposition. The previously mentioned degree bounds for this are much to high and wrong as well. So it is certainly understandable if we also hope to suggest new methods for the question of normal primary decomposition and the computation of prime ideals by irrational generic zeros that would make reference to [6] unnecessary.

However, this goal is still open (see also Lazard's papers [21, 22]). The whole problem has been raised again in A. Seidenberg's highly publicized paper from 1974, and in discussions, Seidenberg alluded again to the "famous" mistake in [6, §2] which van der Waerden discovered in [32] and which he wrote about in [29, pp. 273-274]: "Van der Waerden did not go on to examine the repercussions in Hermann's paper of the error mentioned, and since (hopefully) there is no further error ($^2$), one might .... " The footnote ($^2$) contains an error G. Stolzenberg found in [6, Theorem 4], one which we also found in 1957. Since this error is only one of many, and furthermore since Seidenberg had also adopted the wrong degree bounds from [6], it seems reasonable here that we publish Christa Krause's 1958 critical analysis [31] (authored under her maiden name Veltzke) in §1, and its relation to this series of articles in §3. The latter also represents an excerpt of the author's dissertation B (Department of Natural Science, Martin Luther University, Halle, 1977). In §2, subsequent papers by Kneser, Krull, Reufel, Seidenberg, and Lazard are discussed, in which, out of consideration for the interested reader, smaller overlaps with §1 were not been intentionally avoided.

The 203-page diploma thesis [31] was supervised at the time by the author and was suggested by Grell, to whom Krull had sent a copy. In 1965, the subsequent revision [28] of Henzelt-Noether-Hermann theory by Krull's student Reufel referred to [31] on [28, p. 232] and in the bibliography, but Seidenberg did not even cite [28] in [29]. Given the scope of [31], which goes into the errors and ambiguities of [6] in the greatest detail, we give only the essential points, arranged by the sections in [6], and a list of errors in §1.9.

As already stated, the Henzelt-Noether-Hermann theory does not deal with practical algorithms. In [6, p. 8], Hermann formulates the goal as follows [in translation]:

> The computational methods below are computations *in finitely many steps*. The claim that a computation can be found 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 [italicized as in the original].

About this, Seidenberg expressed in [29, p. 275], "This is obscure, really, since one has to construct the bounds, ...,". As stated above, Reufel showed in [28] that we are dealing with algorithms. The first satisfactory treatment of the degree bounds was given by Daniel Lazard in [22] (see §3.1 and §3.4). In [13, p. 18], Krull writes about the limitations of that goal [in translation]:

> Above all, regardless of the necessary restrictions of the corresponding ground field, we must not overlook the fact that, in general, the computations may not be practical because of the many large numbers of individual steps that are needed. Thus, strictly speaking, our treatment of the "problem of finitely many steps" has an entirely theoretical character.

To a large extent, abandoning practical algorithms (called *computing in tolerably many steps* by O.H. Keller in [8, 9]) results in abandoning concrete examples. This implies not only a methodological deficiency (when illustrating the theory using examples), but also a lack of momentum for learning the theory itself. Daniel Lazard also came to this conclusion in [22, p. 165]. This may also be the reason for the hesitant editing of [6], even though we show in §3, that certain basic concepts in [6] also include practical algorithms in their definitions.

## 1.2 On §§1, 2 of Hermann's Paper

In [6, §1: *Fundamental Concepts*], various earlier notations and terms are cited from [5] and [24], from which we will only comment on the less familiar ones.

$[f]$ := degree of $f(x_1, \ldots, x_n)$ in all variables $x_1, \ldots, x_n$, analogous for forms $F(x_0, x_1, \ldots, x_n)$,
$[f]_\varrho$ := degree of $f(x_1, \ldots, x_n)$ in all variables $x_1, \ldots, x_\varrho$, $\varrho \leq n$, analogous for forms $F(x_0, x_1, \ldots, x_n)$.

The notation

$$f^{(i)} := f^{(i)}(x_i, x_{i+1}, \ldots, x_n), \tag{1}$$

and similarly for $F^{(i)} := F^{(i)}(x_i, x_{i+1}, \ldots, x_n)$, means that $f^{(i)}$ depends only on $x_i, x_{i+1}, \ldots, x_n$. Krull moved this notation to the first variables in [14, 15], but there are no clear advantages for doing this.

If $u_{11}, \ldots, u_{nn}$ are independent indeterminates that can be adjoined to a ground field, then the input variables $x_1, \ldots, x_n$ are mapped to the output variables $y_1, \ldots, y_n$ using the transformation

$$y_i = u_{i1}x_1 + \ldots + u_{1n}x_n \qquad (i = 1, 2, \ldots, n), \tag{2}$$

(similarly for $x_0, x_1, \ldots, x_n$ using $u_{00}, \ldots, u_{nn}$), whereby *transformed ideals*, *transformed modules* and *transformed equations* arise.

As already stated, passing over to transformed ideals makes practical computation impossible. Adjoining the indeterminates to the ground field also creates problems for polynomial factorization, which we will now address.

One reason for introducing transformed ideals using (2) lies in Noether's realization in [24, pp. 232-233] that all variable numberings in transformed ideals are equally adequate (see [26, §3.2, Definition 13]), thus an expression of the form (2) is indispensable. Secondly, the *regularity* of transformed polynomials is ensured by (2), which Hilbert needed in [7]. The third motivation, identified in [6, pp. 9-10], concerns the definition of the fundamental ideal, which we give as Krull introduced it in [14].

**Definition 1.** By the Lasker-Noether Theorem, given an ideal $\mathfrak{a}$ in a Noetherian ring, every irreducible representation of $\mathfrak{a}$ by largest primary components (and which is unique up to embedded primary component) is called a *normal primary decomposition*. Let $\mathfrak{a} \subset K[x_0, x_1, \ldots, x_n]$ be an H-ideal and the primary components be ordered by decreasing dimensions, hence by increasing codimension $r, r+1, \ldots, n, n+1$:

$$\mathfrak{a} = (\mathfrak{q}_{r1} \cap \ldots \cap \mathfrak{q}_{r,s_r}) \cap \left(\mathfrak{q}_{r+1,1} \cap \ldots \cap \mathfrak{q}_{r+1,s_{r+1}}\right) \cap \ldots \cap (\mathfrak{q}_{n1} \cap \ldots \cap \mathfrak{q}_{n,s_n}) \cap \quad \mathfrak{q}_T \tag{3}$$

where $\dim \mathfrak{q}_{\varrho\sigma} = \varrho$ $(\sigma = 1, \ldots, s_\varrho)$ and $\dim \mathfrak{q}_T = n+1$. Then the *i-th fundamental ideal* is defined by

$$\left.\begin{array}{ll} \mathfrak{g}_i(\mathfrak{a}) & := \mathfrak{q}_{r1} \cap \ldots \cap \mathfrak{q}_{i,s_i} \qquad i = r, \ldots, n \\ \mathfrak{g}_{i+1}(\mathfrak{a}) & := \mathfrak{a}. \end{array}\right\} \tag{4}$$

Similarly, $\mathfrak{g}_n((\mathfrak{a})) = (\mathfrak{a})$ for homogeneous P-ideals $(\mathfrak{a})$. Here again, Krull changes the order of indices in [14], but there are no advantages in doing this. Fundamental ideals are defined via (4) by Hermann in [6, pp. 9-10], Reufel in [27, p. 18] and the author in [25, p. 64 (Definition A)]. However in most cases, (4) already consists precisely of elements of the normal primary decomposition (3). Therefore, computing fundamental ideals will have to come from a different definition of fundamental ideals equivalent to (4). One such definition *only for transformed ideals* was given by Emmy Noether [24, p. 233]: If $(\mathfrak{a})$ is a transformed P-ideal, then $\mathfrak{g}_{i-1}((\mathfrak{a}))$ contains all polynomials $g(x_1, \ldots, g_n)$ for which there exists a polynomial $b^{(i)} := b^{(i)}(x_i, x_{i+1}, \ldots, x_n)$ (in general, distinct from $g(x_1, \ldots, x_n)$) such that $b^{(i)}g \in ((\mathfrak{a}))$. From the existence of ideal bases, also follows the existence of a *fixed* $b^{(i)}$ such that $b^{(i)}g \in ((\mathfrak{a}))$ for *all* $g \in \mathfrak{g}_{i-1}((\mathfrak{a}))$, so that

$$\mathfrak{g}_{i-1}((\mathfrak{a})) := (\mathfrak{a}) : \left(b^{(i)}\right) \tag{5}$$

holds (see [5, p. 62]). In $K[x_0, x_1, \ldots, x_n]$, the analogous relation

$$\left.\begin{array}{ll} \mathfrak{g}_i(\mathfrak{a}) & := \mathfrak{a} : \left(B^{(i)}\right) \\ \mathfrak{g}_{n+1}(\mathfrak{a}) & = \mathfrak{a} \end{array}\right\} \tag{6}$$

holds for transformed ideals $\mathfrak{a}$ and was given by the author in [25, p. 64, Definition B]. The first named reason for introducing transformed ideals no longer applies for (5) and (6), thus (5) and (6) hold only for transformed ideals. Hence, fundamental modules $\mathfrak{G}_{i-1}$ are also defined by (5) and (6).

Now every polynomial $f(x_1, \ldots, f_n)$ is regarded as a linear form in the monomials $\xi$ of $x_1, \ldots, x_{i-1}$ with polynomials $a^{(i)}(x_i, x_{i+1}, \ldots, x_n)$. In this way, the ideal $(\mathfrak{m})$ is mapped to a *module* $\mathfrak{M}_{i-1}$ *of linear forms*, and in particular, the fundamental ideal $\mathfrak{g}_{i-1}((\mathfrak{m}))$ is mapped to the *fundamental module* $\mathfrak{G}_{i-1}$. Then

$$\begin{array}{lll} \mathfrak{M}_{i-1} = ( & E^{(i)}\xi_0,\ E_1^{(i)}\xi_1,\ \ldots,\ E_\sigma^{(i)}\xi_\sigma,\ \xi_{\sigma+1},\ \ldots,\ \xi_{\sigma+\nu},\ \ldots\ ) & \text{and} \\ \mathfrak{G}_{i-1} = ( & \xi_0, \quad \xi_1, \ldots, \quad \xi_\sigma, \xi_{\sigma+1}, \ldots, \xi_{\sigma+\nu}, \ldots\ ) & \end{array}$$

hold for only finitely many *elementary divisors* $E^{(i)}, E_1^{(i)}, \ldots, E_\sigma^{(i)}$ such that $E_{k+1}^{(i)} \mid E_k^{(i)}$ and $E^{(i)}$ is the largest elementary divisor. Furthermore, the products $R^{(i)} := E^{(i)}E_1^{(i)} \cdots E_\sigma^{(i)}$ will be called *individual norms* and

$$E_{\mathfrak{m}} := E^{(1)}E^{(2)} \cdots E^{(n)} \tag{7}$$

the *elementary divisor form*. In more recent papers, the terms *fundamental polynomial* [15] and *fundamental form* [29, Propositions 30, 31, 32] are used for (7). Van der Waerden shows this agrees with his definition of *associated form* in [34].

The prime ideal associated with an ideal $\mathfrak{m}$ and its zeros can be obtained via the decomposition (7). This important property explains attempts by previous authors to introduce and determine $E_{\mathfrak{m}}$ using simpler means than (7) (see §1.7 and §2.2).

In [6, §2: *Polynomial Factorization in Finitely Many Steps*, Theorem 1], it is falsely claimed that it is always possible to factor a polynomial into irreducible factors over a finite extension of the prime field in finitely many steps. Since necessary and sufficient conditions for the validity of this statement are not known, it seems advisable to assume the above statement as an additional condition, "this represents a probably unavoidable but essential constraint" [13, p. 17]. As van der Waerden showed in [32], the separability of the algebraic extension must be assumed in [6, Theorem 1], otherwise the theorem can be false (see Kneser's counterexample in [11]). Krull in [16, 17, 18] continued Kneser's study by considering special fields with the desired property.

As van der Waerden showed in [32], the claim in [6, p. 11] that polynomial factorization in finitely many steps could be carried over to infinite field extensions is false. This "famous" error was found by Fröhlich and Shepherdson [2], Reufel [28] and Seidenberg [29]. Thus for these authors, the question of feasibility of polynomial factorization has a different meaning because certain ideal theoretic operations are algorithmically practical only under such assumptions (see §2.4).

### 1.3 On §3 of Hermann's Paper

In [6, §3: *Computational Operations in Ideal Theory*, Theorem 2], important for ideas that follow, is formulated:

**Theorem.** *If $f_{ij} \in K[x_1, \ldots, x_n]$, then a complete solution to the system of equations*

$$f_{i1}z_1 + \ldots + f_{is}z_s = 0 \qquad (i = 1, 2, \ldots, t) \tag{8}$$

*with quantities in $K[x_1, \ldots, x_n]$ can be computed in finitely many steps. If $q$ is the maximal degree of the $f_{ij}$, then the degree of the complete solution of the system of equations does not exceed $m(t, q, n)$; ....*

Then for $m(t, q, n)$, an incorrect recursion formula and consequently an incorrect explicit formula is given. Seidenberg calls this theorem Proposition 1 in [29]. For H-ideals and H-matrices, this theorem represents a connection to syzygy theory and is actually formulated inhomogeneously.

To prove this, we refer to Hilbert's classic induction proof [7] on $n$, in which the usual determinant methods and regularity in $x_1$ guaranteed by transformability are used. In [6, p. 12/1], each $D$ should be replaced by $-D$. As already mentioned, this mistake originated with Hilbert. The progression by powers of $x_1$ leads to a system of equations in $x_2, \ldots, x_n$ in which the induction hypothesis is applied. But we must take into account here that $f_{11}, \ldots, f_{ts}$ still depend on $x_1$ in (8). This is where the recursive formula and the explicit formula in [6] are wrong (see error 5 in the list of errors §1.9). The correct recursive formula for $m(t, q, n)$ should read

$$m(t, q, 0) = 0 \qquad \text{and} \qquad m(t, q, n) = qt + m(qt^2 + qt, q, n - 1). \tag{9}$$

An explicit formula is obtained from this only by majorization (this was confirmed in letters between the author and Ralf Fröberg in Stockholm). We set for example $\overline{m}(t, q, n) = qt + \overline{m}(2qt^2, q, n - 1)$, then with

$$2\overline{m}(t, q, n) = 2qt + (2qt)^2 + (2qt)^4 + \ldots + (2qt)^{2^{n-1}},$$

we obtain a still higher and completely impractical degree bound.

The correct recursion formula (9) was given by Reufel in [28, p. 232] with reference to [31] and before that in [27, p. 21]. Unfortunately, Seidenberg made no reference to it in [29], but rather adopted Hermann's incorrect degree bounds [29, p. 296ff]. Thus incorrect degree bounds exist in [29, Propositions 55-60, 62-63]. Consequently, the wrong degree bounds from [6] are propagated throughout the [29]. The recursion formula (9) can still be improved somewhat for the term $-1$, as Daniel Lazard showed in [20, Theorem 1], who also assumed the wrong degree bounds of Hermann and Seidenberg in [22, last theorem].

If $t = 1$ and if the $f_i$ are homogeneous in $x_1, \ldots, x_\varrho$ ($\varrho \leq n$) in (8), then [6, Corollary to Theorem 2] shows that the solution polynomials are also homogeneous in $x_1, \ldots, x_\varrho$. An important consequence is the computability of ideal intersections $(\mathfrak{a}) \cap (\mathfrak{b})$ and ideal quotients $(\mathfrak{a}) : (\mathfrak{f})$ and $(\mathfrak{a}) : (\mathfrak{b})$ for arbitrary P-ideals. This is the very first reference in the literature on computing ideal intersections and ideal quotients!

### 1.4 On §4 of Hermann's Paper

Hidden behind the [6, §4] heading *Degree Restrictions in Formal Divisibility Theorems* is the task of obtaining degree bounds for H-bases. In [6, Theorem 3], it states:

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

$$l_i = f_{i1} z_1 + \ldots + f_{is} z_s \qquad (i = 1, 2, \ldots, t).$$

*Now if $l \in \mathfrak{M}$, i.e. $l = a_1 l_1 + \ldots + a_t l_t$, then this representation can be chosen so that the $a_i$ stay below a degree bound.*

This degree bound is again wrong, because in the proof, the number of terms

$$l_1,\ x_1 l_1,\ \ldots,\ x_1^{qt} l_1,\ \ldots,\ l_t, x_1 l_t,\ \ldots,\ x_1^{qt} l_t$$

should have been counted as $(qt + 1)t = qt^2 + t$ instead of $qt^2$. Thus the estimate

$$\begin{aligned} &[a_i] \leq [l] + 2m^*(t, q, n), \qquad \text{where} \\ &m^*(t, q, 0) = 0, \quad m^*(t, q, n) = qt + m^*(qt^2 + t, q, n - 1) \end{aligned} \tag{10}$$

is correct. Then the special case $s = 1$ is considered as an application of Theorem 3. If we omit the $z_1$ that appear as a factor in all the elements of $\mathfrak{M}$, then $\mathfrak{M}$ is mapped to an ideal

$$(\mathfrak{a}) = (f_1, \ldots, f_t) \subset K[x_1, \ldots, x_n].$$

Then the existence of a representation

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

with the corrected degree bounds $[g_i] \leq [g] + 2m^*(t, q, n)$ follows from $g \in (\mathfrak{a})$.

We can now define equivalent H-ideals relative to a subset of variables, say $x_1, \ldots, x_\varrho$ ($\varrho \leq n$), and compute ideal quotients $\mathfrak{a}_1 : (x_0)^k$. Then it follows for $k$ that $k \leq q + 2m^*(t, q, n)$. Since we still must add $x_0$, [6, Theorem 4] reads correctly as:

**Theorem.** *For every P-ideal $(\mathfrak{a}) = (f_1, \ldots, f_t)$, there is a distinguished ideal basis $f_{\varrho 1}, \ldots, f_{\varrho t_\varrho}$ such that for every $g \in (\mathfrak{a})$, there exists a representation*

$$g = g_1 f_{\varrho 1} + \ldots, + g_{t_\varrho} f_{\varrho t_\varrho} \qquad \textit{where } [g_i]_\varrho = [g]_\varrho - [f_{\varrho i}]_\varrho.$$

*This basis can be computed in finitely many steps, and*

$$[f_{\varrho i}] \leq m\left(1, 2m^*(t, q, n) + q, n + 1\right).$$

Error 30 in §1.9 should also be noted on account of Seidenberg mentioning it in [29, footnote 2]. Moreover, comparing (9) and (10) yields $m^*(t, q, n) \leq m(t, q, n)$.

## 1.5 On §5 of Hermann's Paper

This chapter of [6, pp. 16-18] deals with *Hentzelt's Nullstellensatz*, in which the ideal exponents that appear are estimated by an integral function $\kappa(t,q,n)$. $\kappa$ is introduced using the recursively defined integral functions $M(t,q,n)$, $N(t,q,\varrho,e_{\varrho+1},\ldots,e_n)$, $l_\lambda(t,q,\lambda)$, and $v(t,q,\lambda)$. Wrong representations for all of these integral functions appear in [6, pp. 16-19] because the number of elements $l_1,\ldots,x_1^{qt}l_t$ are again counted incorrectly using $qt^2$ instead of $qt^2+t$. For the correct formulae, we refer to items 47 to 54 in the list of errors §1.9. As a result, since the explicit representations in [6, pp. 19-20] are wrong, the derivation

$$\kappa(t,q,n) \geq \kappa(t,q,n-1) \tag{11}$$

is also wrong; however, the validity of (11) does follow without computation from the monotonicity in $t$ and $n$ of $M(t,q,n)$.

In [6, p. 29], a single example $\kappa(2,2,2)=256$ is given. But using the formula in [6] produces 947, while the correct formula yields 1503.

Finally, let us consider the deceptive notation in [6, pp. 16-18]: $\mathfrak{G}_n$, $\mathfrak{G}_\varrho$ and $\mathfrak{g}_\varrho$ do not denote fundamental modules or fundamental ideals, respectively, according to (5), and the $e_i$ do not denote elementary divisors of $N$, but rather exponents. Finally, in [6, p. 17], the specific transformation coefficients would be better denoted $u'_{ik}$ for determining (2). To formulate Hentzelt's Nullstellensatz, we combine two definitions from [6, Definitions 1-2]:

**Definition 2.** A *complete set of zero places* of a P-ideal $(\mathfrak{a})$ will mean a set of generic zeros, one for each prime ideal associated to $(\mathfrak{a})$. If $\left(\xi_1^{(i)},\ldots,\xi_n^{(i)}\right)$, for $i=1,\ldots,h$, is a complete set of zero places of $(\mathfrak{a})$, then

$$(\mathfrak{o}_i) := \left(x_1-\xi_1^{(i)},\ \ldots,\ x_n-\xi_n^{(i)}\right) \tag{12}$$

is called the *zero place ideal belonging to* $\mathfrak{a}$.

In contrast with [6], $m$ was replaced by $h$ here in order to avoid confusion with the integral function $m(t,q,n)$. Then we have

**Theorem 1** (Hentzelt's Nullstellensatz [6, Theorem 5])**.** *If* $\left(\xi_1^{(i)},\ldots,\xi_n^{(i)}\right)$, $i=1,\ldots,h$, *is a complete set of zero places of the P-ideal* $(\mathfrak{a})=(f_1,\ldots,f_t)$ *with* $q=\max[f_j]$ *and if* $\mathfrak{o}_i$ *is the corresponding zero place ideal for* $i=1,\ldots,h$, *then in the ring extension* $K\left(\xi_1^{(i)},\ldots,\xi_n^{(i)}\right)[x_1,\ldots,x_n]$, *we have*

$$g\in((\mathfrak{a}),(\mathfrak{o}_i)^\kappa) \quad \textit{for } i=1,2,\ldots,h \quad\Longrightarrow\quad g\in(\mathfrak{a}), \tag{13}$$

*where* $\kappa(t,q,n)$ *is given by item* 51 *in the list of errors* §1.9, *and* $(\mathfrak{o}_i)$ *by* (12).

Instead of complete sets of zero places consisting of $h$ generic zeros, we can of course base them on the infinitely many specialized zeros. This second version of Hentzelt's Nullstellensatz [6, Theorem 5a] is "of no practical importance" [13, footnote 68]. In any case, these ideas lose all practical computational value for higher values of $\kappa$.

## 1.6 On §6 of Hermann's Paper

To treat [6, §5: *Fundamental Ideals*, pp. 22-26], we return to representations (5) and (6). Since ideal quotients can be computed in principle, computing transformed H-ideals reduces by (6) to constructing $B^{(i)}$, which by [28, Theorem 2] can be done theoretically, i.e. by proving the existence of an algorithm using induction.

According to [5], the ideals in the illustration on the applicability of elementary divisor theory in [6] can be viewed as modules of linear forms in the monomials. The *rank* of a module $\mathfrak{M}$ of linear forms is the maximal number of linearly independent linear forms in $\mathfrak{M}$. A module $\mathfrak{G}$ is called a *fundamental module* if it has no proper divisors of the same rank. For every $\mathfrak{M}$, there is exactly one fundamental module $\mathfrak{G}$ of the same rank [5, Theorem 1]. By §1.2, $\mathfrak{M}_{\lambda-1}$ is the module of monomials in $x_1, \ldots, x_{\lambda-1}$ with coefficients in $K(x_\lambda, \ldots, x_n)$, $\mathfrak{M}^*_{\lambda-1}$ is the corresponding H-basis relative to $x_1, \ldots, x_{\lambda-1}$ (see the end of §1.4), and the fundamental module $\mathfrak{G}_{\lambda-1}$ is defined similarly. Then the ideas in [6] can be connected as follows: [6, Theorem 6] states that for a transformed ideal $(\mathfrak{a})$ with maximal degree $q$ in the basis polynomials, there are representatives in the set of residue classes $\mathfrak{g}_\varrho((\mathfrak{a}))/(\mathfrak{a})$ whose degree $n$ does not exceed

$$n_0 := 0, \qquad n_\varrho := n_{\varrho-1} + m(1, 2m^*(t, q, n) + q, n+1)\left[1 + \binom{n_{\varrho-1} + \varrho - 1}{\varrho - 1}\right],$$

where the corrected degree bounds have been inserted. The module of linear forms in the monomials $x_1, \ldots, x_\varrho$ will be denoted by $\mathfrak{G}^*_\varrho$, which consists of the set of all elements in $\mathfrak{g}_\varrho((\mathfrak{a}))$ that do not exceed the degree $n_\varrho$ relative to $x_1, \ldots, x_\varrho$ [6, Definition 1]. Then by [6, Theorem 7], $\mathfrak{G}^*_{\varrho-1}$ is the fundamental module of $\mathfrak{M}^*_{\varrho-1}$, and furthermore, $\mathfrak{G}^*_{\varrho-1}/\mathfrak{M}^*_{\varrho-1} \cong \mathfrak{G}_{\varrho-1}/\mathfrak{M}_{\varrho-1}$. Finally, $\mathfrak{M}_{\varrho-1}$ has only finitely many nontrivial elementary divisors, namely those of $\mathfrak{M}^*_{\varrho-1}$ (see also §1.2). By the decomposition principle given by (3) and (6) respectively, which is only recognizable in the proof [6, p. 26/1] with difficulty, the inductive proof of [6, Theorem 8] is possible using these tools, whereby the basis of $\mathfrak{g}_\varrho((\mathfrak{a}))$ can be computed in finitely many steps. Krull summarizes the developments of [6] described here in [12, p. 52ff] and in [13, p. 17ff], which contain some new ideas, such as Theorem 4 (see §2.1).

### 1.7 On §7 of Hermann's Paper

In [6, §7: *Prime Ideals*, Theorem 11], it is falsely claimed that it is always possible to compute prime ideals belonging to a P-ideal $(\mathfrak{a})$. The basic idea is found in [24, Theorem X]. Then the prime ideals are obtained from the prime functions of the elementary divisor form defined by (7) using inverse transformations of (2). If the inversely transformed prime function is given in terms of the old variables $y_1, \ldots, y_n$ by $P = U_1P_1 + \ldots + U_lP_l$, where $U_1, \ldots, U_l$ are monomials in the transformation coefficients, then under certain field-theoretic conditions, the prime ideal is given by $(P_1, \ldots, P_l)$ [6, Theorem 9].

In order to obtain all prime ideals in this way, decomposing the elementary divisor forms (7) must be possible, which by itself will not guarantee that we can obtain the prime ideals using this method. Thus here, the problem of polynomial factorization plays a role, which Reufel [28] and Seidenberg [29] discuss in great detail (see §2 of this paper).

### 1.8 On §8 of Hermann's Paper

In the concluding [6, §8: *Primary Ideals*], a *normal primary decomposition*

$$\mathfrak{a} = \bigcap_{i=1}^{h} \mathfrak{g}_\varrho\left(\mathfrak{a}, \mathfrak{p}_i^\kappa\right) \tag{14}$$

for $\mathfrak{a}$ is derived with $\dim \mathfrak{p}_i = n - \varrho$ [6, Theorem 12]. In [6, p. 29/2], it is stated without proof that $\mathfrak{g}_\varrho\left(\mathfrak{a}, \mathfrak{p}_i^\kappa\right)$ is a primary ideal belonging to $\mathfrak{p}_i$, resulting in $\mathrm{Rad}\left(\mathfrak{a}, \mathfrak{p}_i^\kappa\right) = \mathrm{Rad}(\mathfrak{a}, \mathfrak{p}_i) = \mathfrak{p}_i$, $\dim\left(\mathfrak{a}, \mathfrak{p}_i^\kappa\right) = \dim \mathfrak{p}_i = n - \varrho$, and hence the unmixedness of $\mathfrak{g}_\varrho\left(\mathfrak{a}, \mathfrak{p}_i^\kappa\right)$ by (4).

For the proof, $\mathfrak{a} \subseteq \bigcap_{i=1}^h \mathfrak{g}_\varrho\left(\mathfrak{a}, \mathfrak{p}_i^\kappa\right)$ can be inferred from $\mathfrak{a} \subseteq \left(\mathfrak{a}, \mathfrak{p}_i^\kappa\right) \subseteq \mathfrak{g}_\varrho\left(\mathfrak{a}, \mathfrak{p}_i^\kappa\right)$ by (14), while the very complicated proof of $\supseteq$ requires Hentzelt's Nullstellensatz. The proof in [6] for this is terse, but complete. We make the following comment here: If we dispense with the fundamental ideal construction, then using the same methods produces a decomposition of $\mathfrak{a}$ as the intersection of quasi-primary ideals. We found the statement below as a theorem in [23] without using Hentzelt's Nullstellensatz or specifying the degree bound $\kappa$. Thus for H-ideals we have

**Theorem 2** (McCarthy [23]). *If $\mathfrak{a} \subset K[x_0, x_1, \ldots, x_n]$ is an H-ideal for which the normal primary decomposition of radicals is given by* $\operatorname{Rad}\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \ldots \cap \mathfrak{p}_m$, *then*

$$\mathfrak{a} = (\mathfrak{a}, \mathfrak{p}_1^\kappa) \cap (\mathfrak{a}, \mathfrak{p}_2^\kappa) \cap \ldots \cap (\mathfrak{a}, \mathfrak{p}_m^\kappa) \tag{15}$$

*is a decomposition of $\mathfrak{a}$ as an intersection of quasi-primary H-ideals.*

Particularly important for our task is a corollary to Theorem 2:

**Theorem 3.** *The problem of practically constructing a normal primary decomposition of an H-ideal can be reduced to the problem of constructing such a decomposition for quasi-primary H-ideals.*

## 1.9 Veltzke's List of Errors

1. p. 11/1, l. 1: "Algebraic" should read "separable algebraic" (see error 3).
2. p. 10, footnote 9: Should be omitted because the theorem on primitive elements holds (for arbitrary characteristic) due to the assumed separability.
3. p. 11/2, ll. 3-4: This claim is only correct if separability of $\alpha_l$ is assumed (see error 1, proof in [33, pp. 130-131]).
4. p. 11/2, ll. 35-39: Here it is left open how to decide whether there exists a subfield of the infinite extension field isomorphic to the finite extension field being considered (these are the splitting field or intermediate field). But by [32], this is not possible.
5. p. 12/1, ll. 9-10: Instead of $m(t,q,n) = qt + m(t^2q, q, n-1)$, it should read $m(t,q,n) = qt + m(t^2q + qt, q, n-1)$. "Thus $m(t,q,n) = \ldots$" should be omitted; the explicit formula is incorrect.
6. p. 12/1, ll. 41-45: $z_{t+1} = D$ should read $z_{t+1} = -D$ and $z_s = D$ should read $z_s = -D$.
7. p. 12/2, ll. 10-14: For $t = 1$, this identity is correct even if we define $F_{11} = 1$.
8. p. 12/2, l. 13: $F_{t1}$ should read $F_{1t}$.
9. p. 12/2, l. 26 [already corrected]: $\xi_{1\mu}^{(2)}$ should read $\xi_{s\mu}^{(2)}$.
10. p. 12/2, l. 36: $\tau = \mu t \leq qt^2$ should read $\tau = t(q+\mu) \leq qt^2 + qt$. Now $\mu s = \sigma > \tau$ can no longer follow from $s > t$, but can, without loss of generality, be assumed (this follows from the eventual reduction of the system of equations).
11. p. 12/2, l. 39: $m(qt^2, q, r-1)$ should read $m(qt^2 + qt, q, r-1)$.
12. p. 12/2, ll. 42-44 [already corrected]: $\xi_{1\mu}^{(2)}$ and $\xi_{s\mu}^{(2)}$ should read $\overline{\xi}_{1\mu}^{(2)}$ and $\overline{\xi}_{s\mu}^{(2)}$, respectively.
13. p. 13/1, l. 10: $\mu + m(qt^2, q, r-1) \leq \ldots$ should read $\mu + m(qt^2+qt, q, r-1) \leq qt + m(qt^2+qt, q, r-1) = m(t,q,r)$.
14. p. 14/1, ll. 11-12: "$[a_i] \leq [l] + 2m(t,q,n)$ where $\ldots$ is defined"] should read "$[a_i] \leq [l] + 2m^*(t,q,n)$ where $m^*(t,q,0) = 0$ and $m^*(t,q,n) = qt + m^*(qt^2 + qt, q, n-1)$." As it happens, since $m^*(t,q,n) \leq m(t,q,n)$, the formulation in [6] is also correct.
15. p. 14/1, ll. 28-30: $F_{1p}$ should read $F_{p1}$ and vice versa.
16. p. 14/1, ll. 28-34: For $t = 1$ or $s = 1$, identities are correct, even if we define $F_{1k} = 1$ or $F_{i1} = 1$, respectively.
17. p. 14/1, l. 21: $f^{(2)}$ is defined somewhat vaguely; the claim on l. 21 is only correct if $f^{(2)}$ is defined as follows: $M = [j_i]_1 + [D]$, $j_1 D = \phi_{i0}^{(2)} + \phi_{i1}^{(2)} x_1 + \ldots + \phi_{iM}^{(2)} x_1^M$, $\phi_{i,\kappa+[D]} = f^{(2)}$.
18. p. 14/2, l. 30: $m(t,q,r)$ should read $m^*(t,q,r)$.
19. p. 14/2, l. 40: $G_1 = \ldots$ should read $G_1 = a_1 f_{1i} + \ldots + a_t f_{ti}$.
20. p. 15/1, l. 5: $F_{ik}$ should read $F_{ki}$ and $F_{\pi k}$ should read $F_{k\pi}$.
21. p. 15/1, l. 7: $F_{\pi k}$ should read $F_{k\pi}$.
22. p. 15/1, l. 14: $2m(t,q,1)$ should read $2m^*(t,q,1)$.
23. p. 15/1, l. 22: $qt^2$ should read $qt^2 + qt$.
24. p. 15/1, l. 26: $2m(qt^2, q, r-1)$ should read $2m^*(qt^2 + qt, q, r-1)$.
25. p. 15/1, l. 34: Same as error 24.
26. p. 15/1, l. 40: $[a_i] \leq \ldots = \ldots$ should read $[a_l] \leq [g] + 2qt + 2m^*(qt^2 + qt, q, r-1) = [g] = 2m^*(t,q,r)$.
27. p. 15/2, l. 10: $2m(t,q,n)$ should read $2m^*(t,q,n)$.
28. p. 15/2, l. 12: $[g] + m(t,q,n)$ should read $[g] + 2m^*(t,q,n)$.

29. p. 15/2, l. 35: $[f_{pi}] \leq m(1,q,n) = \ldots$ should read $[f_{\varrho i}] \leq m(1, 2m^*(q,t,q,n)+q, n+1)$. The explicit formula is incorrect (see error 5).
30. p. 15/2, l. 44: $[c_i] \leq [g] + 2m(t,q,n)$ should read $[c_i]_\varrho \leq [g]_\varrho + 2m^*(t,q,n)$. This general version of Theorem 3 is needed for estimating $k$ in [6, p. 16/1, l. 4] and its proof is entirely analogous to Theorem 3.
31. p. 16/1, l. 1: $\overline{g}_i$ should read $\overline{g}$.
32. p. 16/1, l. 4: $k \leq \ldots$ should read $k \leq q = 2m^*(t,q,n)$. Corrected version of error 30 is required to prove this.
33. p. 16/1, l. 6: $x_0^{2m+q}\overline{g}$ should read $x_0^{2m^*+q}\overline{g}$.
34. p. 16/1, l. 11: $x_0^{2m+q}\mathfrak{X}$ should read $x_0^{2m^*+q}\mathfrak{X}$.
35. p. 16/1, l. 15: $[\overline{f}_{\varrho i}] \leq \ldots = \ldots$ corrected as in error 29.
36. p. 16/1, l. 21: $x_1, \ldots, x_\varrho$ should read $x_0, x_1, \ldots, x_\varrho$.
37. p. 16/1, l. 25: $g_i \neq 0$ should read $\overline{g}_i \neq 0$.
38. p. 16/1, l. 30: $[f_{\varrho i}] \leq \ldots$ corrected as in error 29.
39. p. 16/1, l. 36: $[g_i] = \ldots$ should read $[g_i]_\varrho = [g]_\varrho - [f_{\varrho i}]_\varrho$.
40. p. 16/2, l. 31: $M(t,q,n) = \ldots$ should read $M(t,q,n) = M(qt^2+t, q, n-1)$.
41. p. 16/2, ll. 32-33: Omit "Therefore, $M(t,q,n) = \ldots$".
42. p. 16/2, ll. 22, 27, 34: $\mathfrak{G}_n$ is denoted by $\mathfrak{G}_{n-1}$ in [24] as well as in (5). The notation $\mathfrak{G}_r$ in [6, p. 17/1, l. 38] is also misleading.
43. p. 17/1, l. 21: $[a_i] \leq qt$ should read $[a_i]_1 \leq qt$.
44. p. 17/1, l. 32: $M(qt^2, q, r-1)$ should read $M(qt^2+t, q, r-1)$.
45. p. 17/1, l. 40: same as error 44.
46. p. 17/2, ll. 31-39: unfortunate notation: $u_{11}, \ldots, u_{1\varrho}, \ldots, u_{\varrho 1}, \ldots, u_{\varrho\varrho}$ would be better as $u'_{11}, \ldots, u'_{1\varrho}, \ldots$, $u'_{\varrho 1}, \ldots, u'_{\varrho\varrho}$. In ll. 39 and 44 (as well as p. 18/1, ll. 23, 26, 28), $\mathfrak{g}_\varrho$ is not the $\varrho$-th fundamental ideal.
47. p. 17/2, l. 47: $N(t,q,\varrho,e_{\varrho+1},\ldots,e_n) = \ldots = \ldots$ should read $N(t,q,\varrho,e_{\varrho+1},\ldots,e_n) = M(te_{\varrho+1},\ldots,e_n,q\varrho) = \ldots = \ldots$. Omit the explicit formula.
48. p. 18/2, l. 14: $[\phi_i] \leq \ldots$ should read $[\phi_i] \leq [g] + 2m^*(t,q,n)$.
49. p. 18/2, l. 17: $[z_\varrho] \leq \ldots$ should read $[z_\varrho] \leq [g] + q + 2m^*(t,q,n)$.
50. p. 18/2, l. 19: $[\xi_\varrho] \leq \ldots$ should read $[\xi_\varrho] \leq [g] + 2m^*(t,q,n)$.
51. p. 19/1, l. 20: $\kappa(t,q,n) = q + \ldots = q + v(t,q,n)$ should read

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

    where $l_n := M(t,q,n)$ and $l_\lambda := M(t\cdot l_{\lambda+1}\cdot\ldots\cdot l_n, q, \lambda)$.
52. p. 19/2, ll. 24-39: Omit this, since due to error 51, the explicit formula for $\kappa(t,q,n)$ will no longer be used. However, the desired relation $\kappa(t,q,n) \geq \kappa(t,q,n-1)$ can be obtained without computation from the monotonic growth of $M(t,q,n)$ relative to $t$ and $n$.
53. p. 20/1, l. 1: $l \geq$ should read $l \geq (l_1-1)\cdots(l_n-1)+1$.
54. p. 20/1, ll. 11-14: $l_n = \ldots$ and $l_\lambda = \ldots = \ldots$ should read $l_n = M(t,q,n)$ and $l_\lambda = N(t,q,\lambda,l_{\lambda+1},\ldots,l_n) = M(t\cdot l_{\lambda+1}\cdot\ldots\cdot l_n, q, \lambda)$, respectively.
55. p. 21/1, l. 23: $E_i(x_i)g_{r-1} \equiv 0\ (\mathfrak{m})$ should read $E_i(x_i)\mathfrak{g}_{r-1} \equiv 0\ (\mathfrak{m})$.
56. p. 21/1, l. 38: "By ..." should read "By Lemma 2 and its Corollary".
57. p. 21/2, l. 24: $g \equiv 0\ (\mathfrak{m}, \mathfrak{o}^\kappa)$ should read $g \equiv 0\ (\mathfrak{m}, \mathfrak{o}_i^\kappa)$.
58. p. 22/2, l. 19: $n_0 = 0$, $n_\varrho = \ldots$ should read

$$n_0 = 0, \qquad n_\varrho = n_{\varrho-1} + m(1, 2m^*(t,q,n)+q, n+1)\cdot\left[1 + \binom{n_{\varrho-1}+\varrho-1}{\varrho-1}\right].$$

59. p. 22/2, l. 29: $\overline{q} = \ldots$ should read $\overline{q} = m(1, 2m^*(t,q,n)+q, n+1)$.
60. p. 22/2, l. 37: $n_{\lambda-1} - [f]_{\lambda-1}$ should read $n_{\lambda-1} - [f_\kappa]_{\lambda-1}$.
61. p. 22/2, l. 39: $\overline{t} < t_{\lambda-1}\cdot s$ should read $\overline{t} \leq t_{\lambda-1}\cdot s$.
62. p. 23/2, l. 19: $i = 1, \ldots, p$ should read $i = p+1, \ldots, \overline{t}$.

63. p. 23/2, l. 23: $[a_i]_\lambda < \ldots$ should read $[a_i]_\lambda \leq \ldots$.
64. p. 24/2, l. 4: $\equiv$ should be $\equiv$.
65. p. 25/1, l. 19: $\mathfrak{G}^*_{\varrho-1}/\mathfrak{M}^*_{\varrho-1}$ should read $\mathfrak{G}^*_{\varrho-1}/\mathfrak{M}_{\varrho-1}$.
66. p. 25/1, l. 48: [no change in English translation].
67. p. 25/2, l. 28: $t$ should read $p$.
68. p. 25/2, l. 28: "$t$-row" should read "$p$-row".
69. p. 26/1, l. 2: $x_{\lambda-1}, \ldots, x_n$ should read $x_{\lambda+1}, \ldots, x_n$.
70. p. 26/1, l. 6: $[g] \leq n_{\lambda-1}$ should read $[g]_{\lambda-1} \leq n_{\lambda-1}$.
71. p. 26/1, l. 7: $[k_i] \leq n_{\lambda-1}$ should read $[k_i]_{\lambda-1} \leq n_{\lambda-1}$.
72. p. 26/1, l. 10: $|U|^\gamma \cdot k_i = U_p k_{i1} + \ldots + U_n k_{in}$ should read $|U|^\gamma \cdot k_i = U_{i1} k_{i1} + \ldots + U_{i,m_i} k_{i,m_i}$.
73. p. 26/1, l. 14: $[k_{ij}] \leq n_{\lambda-1}$ should read $[k_{ij}]_{\lambda-1} \leq n_{\lambda-1}$.
74. p. 26/1, l. 15: $(k_{11}, \ldots, k_{pn})$ should read $(k_{11}, \ldots, k_{p,n_p})$.
75. p. 26/1, l. 17: same as error 74.
76. p. 26/1, l. 19: same as error 74.
77. p. 26/1, l. 40: $E^{(\varrho)}_{\varrho-1} = e_{\varrho-1,p}$ should read $E^{(\varrho)}_{\varrho-1} = e_{\varrho-1,1}$. Noether omits lower indices for $E^{(\varrho)}_{\varrho-1}$, $R^{(\varrho)}_{\varrho-1}$ in [24].
78. p. 26/1, l. 42: $x_{\varrho-1}, \ldots, x_n$ should read $x_{\varrho+1}, \ldots, x_n$.
79. p. 27/1, l. 29: [no change in English translation].
80. p. 27/2, l. 9: It is further assumed that $n \geq 2$.
81. p. 28/2, ll. 55-58: $|U|^{\gamma_i} \cdot p_i(x_1, \ldots, x_r) = \ldots$, $|U|^\gamma \cdot P^{(r)}(x_r) = \ldots$ should read $|U|^{\gamma_i} \cdot p_i(x_1, \ldots, x_r) = U_{i1} p_{i1} + \ldots + U_{i\mu} p_{i\mu}$ $(i = 1, \ldots, \nu)$, $|U|^\gamma \cdot P^{(r)}(x_r) = U^*_1 P_1 + \ldots + U^*_\mu P_\mu$.
82. p. 29/1, l. 21: $\mathfrak{p} \neq 0$ should read $\mathfrak{p} \neq \mathfrak{o}$.
83. p. 29/1, l. 34: $F(x_r) \not\equiv 0$ $(\mathfrak{p}')$ should read $F^\kappa(x_r) \not\equiv 0$ $(\mathfrak{p}')$.
84. p. 29/1, l. 46: $\mathfrak{R}^{(i)}$ should read $R^{(i)}_{i-1}$ in two places (see error 77).
85. p. 29/2, ll. 12-16: This claim is correct, but not obvious (see §1.8).
86. p. 29/2, l. 26: $\kappa(2,2,2) = 256$ should be $\kappa(2,2,2) = 1503$ (see error 51). But even Hermann's formula yields a different number, namely 947.

# 2 Extensions of Hentzelt-Noether-Hermann Theory in Later Papers

## 2.1 Krull's Ideal Reports, Fundamental Ideal Quotients

Between 1935 and 1939, Krull produced summaries in [12, p. 52ff] and [13, p. 17ff] of the developments from [6] different than those described in §1, which contain some new ideas. In what follows, Theorem 4 (Krull's theorem, [12, p. 54] and [13, p. 17]), which was neither proved by Krull nor mentioned by Reufel [28] or Seidenberg [29], is especially important for our purposes:

**Theorem 4.** *If $\mathfrak{a} \subset K[x_0, x_1, \ldots, x_n]$ is an H-ideal with $\dim \mathfrak{a} = d = n-r$, then for $i = r, r+1, \ldots, n, n+1$, the ideal quotient $\mathfrak{g}_i(\mathfrak{a}) : \mathfrak{g}_{i-1}(\mathfrak{a})$ is unmixed $(n-i)$-dimensional, and produces all $(n-1)$-dimensional prime ideals belonging to $\mathfrak{a}$. Formally, if $\mathfrak{a}$ and $\mathfrak{g}_i(\mathfrak{a})$ are given by* (3) *and* (4)*, then for $i = r, r+1, \ldots, n, n+1$,*

$$\operatorname{Rad}(\mathfrak{g}_i(\mathfrak{a}) : \mathfrak{g}_{i-1}(\mathfrak{a})) = \mathfrak{p}_{i1} \cap \ldots \cap \mathfrak{p}_{is_i} \tag{16}$$

*and hence* $\operatorname{Ass}\{\mathfrak{a}\} = \bigcup_{i=r}^{n+1} \operatorname{Ass}\{\mathfrak{g}_i(\mathfrak{a}) : \mathfrak{g}_{i-1}(\mathfrak{a})\}$

The proof of (16), which Veltzke and the author gave in [31], originates from the well-known theorem on ideal quotients $\mathfrak{q} : \mathfrak{b}$ (see [26, §2.12, Theorem 20] for example), where it is shown that case (C) cannot occur. However, since case (B) is certainly possible, (16) cannot be improved to $\mathfrak{g}_i(\mathfrak{a}) : \mathfrak{g}_{i-1}(\mathfrak{a}) = \mathfrak{q}_{i1} \cap \ldots \cap \mathfrak{q}_{is_i}$. The computation of all prime ideals belonging to $\mathfrak{a}$ can be reduced to the unmixed case using (16), which represents a fundamental simplification, but fundamental ideals are required at this point (only for normal primary decomposition in [6]). On the other hand, Seidenberg proves in [29, Proposition 19] the constructibility of a decomposition of $\mathfrak{a}$ as the intersection of unmixed ideals and in this way obtains a similar reduction to the unmixed case.

### 2.2 Papers on Defining the Elementary Divisor Form by Krull and van der Waerden

Here we reach back to §1.2 (7) and §1.7. The importance of elementary divisor forms illustrated there leaves us with the desire to define the term in a simpler way. Krull [15] did this in 1949, where he also coined the term *fundamental polynomial* for the elementary divisor form. Following this up in 1958, van der Waerden proved in [34] the equivalence of this fundamental polynomial with the *associated form* that he had already defined in 1937. Finally in 1974, Seidenberg introduced the term *fundamental form* for this in [29, Propositions 30-32].

### 2.3 Papers on Polynomial Factorization by van der Waerden, Kneser and Krull

These papers are connected to [6, Theorem 1], where it is falsely claimed that it is always possible in finitely many steps to factor a polynomial over a finite extension of a prime field into its irreducible factors (see §1.2). As van der Waerden showed in [32], separability of the algebraic extension must also be assumed. Kneser showed in [11] that the theorem can be false in other cases as well. Continuing Kneser's work, Krull gave more precise statements for specific fields in [16, 17, 18].

### 2.4 Fundamental Papers by Fröhlich-Shepherdson and Reufel

The significance of the general question of polynomials being factorable "in finitely many steps" and the issue of strong algorithm-theoretic foundations of Hentzelt-Noether-Hermann theory emerge from the results sketched in the previous section. By the results cited in §2.3, it seems reasonable to move forward with the demand for some sort of axiom for polynomial factorization "in finitely many steps". Between 1935 and 1939, Krull had already spoken in this direction in his "ideal reports" ([12, p. 50] and [13, p. 17]). When Krull said [in translation] in 1948 about [6], "for us, all important ideal operations can be carried out in finitely many steps using certain canonical algorithms" [14, p. 56], this statement already anticipated the 1965 results of his student Reufel [28]. Reufel in turn could point to the 1956 paper of Fröhlich and Shepherdson [2], which refers to van der Waerden's paper [32] and his first edition of *Moderne Algebra* [33] from 1930. To characterize the goal, we quote from the beginning of [2]:

> Van der Waerden [33, pp. 128-131] has discussed the problem of carrying out certain field theoretic procedures effectively, i.e. in a finite number of steps. He defined an "explicitly given" field as one whose elements are uniquely represented by distinguishable symbols with which one can perform the operations of addition, multiplication, subtraction and division in a finite number of steps. He pointed out that if a field $K$ is explicitly given then any finite extension $K'$ of $K$ can be explicitly given, and if there is a splitting algorithm for $K$, i.e. an effective procedure for splitting polynomials with coefficients in $K$ into their irreducible factors in $K[x]$, then there is a splitting algorithm for $K'$ (provided that $K'$ is obtained from $K$ by transcendental or separable algebraic extensions only). He observed in [32], however, that there was no general splitting algorithm applicable to all explicitly given fields $K, \ldots$. In this paper, we review these results in the light of the precise definition of algorithm (finite procedure) $\ldots$ .

Completely independently of [2], Lazard [21] introduced the same concepts in 1976 in connection with [33] using the terms [in translation] *computable fields and rings* with practical algorithms in mind. The first comprehensive revision of Henzelt-Noether-Hermann theory appeared in Reufel's 1965 paper [28]. There, we read in the introduction [in translation]:

> ... Thus the most important problem of the present paper is the simplification of Hermann's comprehensive and difficult to read study and the corrections of some of the mistakes that appear there. This is possible using some ideas that can be extracted from [6] and a method for constructing certain polynomials (see §2) which do not appear in [6] and which the author has been unable to find in the literature. Unfortunately, the revision is also rather long since ... degree bounds were given. ... But if we disregard these degree bounds, then a rather short presentation for the solution of our problem is given (see §6). In §5, we describe a method for constructing the elementary divisor form and norm. ...

In the quote, "certain polynomials" refers to $X_j$-polynomials. For the definition, see [28] itself or the author's review [28R], in which the theory in Reufel's paper is clearly modernized.

Reufel takes the most space for his definition of fundamental ideals using (5) and (6), which he also reduces to constructing $b^{(i)}$ and $B^{(i)}$, denoted by H in [28, Theorem 2]. The proof of constructibility of $H$ in §4 encompasses six pages in its most concise form. But above all, Reufel makes it clear throughout his presentation that Hentzelt-Noether-Hermann theory deals with algorithms. Veltzke's corrected degree bounds and Fröhlich and Shepherdson's previously mentioned paper [2] are connected with this.

Thus Reufel arrived at a differentiation in the issue of demanding an axiomatization of polynomial factorization, which we hinted at in the beginning of this section using the words "some sort". Reufel recognized in 1965 (thus before Seidenberg's 1974 paper [29]), that these axioms need to be formulated differently, each according to whether the existence of algorithms could be proved for (A) determining the normal primary decomposition or (B) determining all associated prime ideals. From (14), it is clear that (B) implies (A), but the converse is not true at all, as Reufel shows in [28, p. 241] using an example by Fröhlich and Shepherdson [2, Theorem 7.27]. Reufel formulated these axioms as follows:

**Definition 3** ([28, p. 239])**.** A *weak factorization algorithm for $k$* is an algorithm having property (F′): If $X_1, \ldots, X_n$ are finitely many indeterminates and $f \in k[X_1, \ldots, X_n]$, then the algorithm admits the construction of a representation $f = f_1 \cdots f_k$ (in finitely many steps), where every $f_i$ is a power of an irreducible polynomial in $k[X_1, \ldots, X_n]$.

From Definition 3 follows

**Theorem 5** ([28, Theorem 1])**.** *If $k$ has a weak factorization algorithm, then there is an algorithm which, given a basis for any submodule $E$ of a finitely generated free $k[X_1, \ldots, X_n]$-module $M$, allows us to construct a normal primary decomposition (in $M$) in finitely many steps.*

From an example by Fröhlich and Shepherdson, Reufel [28, p. 241] can conclude that the existence of algorithms for computing all associated prime ideals cannot be proved from (F′). Consequently, we need to replace property (F′) with a stronger property (F):

**Definition 4** ([28, p. 240])**.** A *strong factorization algorithm for $k$* is an algorithm having property (F): There exists an algorithm that computes the prime factors of every $f \in k[X_1]$, $f \neq 0$.

By [33, p. 129], it follows from (F) that every $f \in k[X_1, \ldots, X_n]$ can be factored into its prime factors. Thus (F) is a stronger property than (F′), hence (F) $\implies$ (F′). Furthermore, Reufel [28, p. 240] shows that if the characteristic of $k$ is 0, then $k$ has a strong factorization algorithm if and only if $k$ has a weak factorization algorithm. But as Reufel remarked in [28, p. 240], properties (F) and (F′) themselves are not always satisfied for fields of characteristic 0, so by [2, §7], there exist fields of characteristic 0 without (F), and hence without (F′) also. To describe the consequences of (F), we need

**Definition 5** ([28, footnote 7])**.** A prime ideal $\mathfrak{p} \subset K[X_1, \ldots, X_n]$ is called *separable* if for every field extension $k'$ of $k$, the extended ideal of $\mathfrak{p}$ in $k'[X_1, \ldots, X_n]$ is the intersection of prime ideals.

From this Reufel formulates

**Theorem 6** ([28, Theorem 2])**.** *If $k$ has a strong factorization algorithm, then the separable prime ideals of $E$ can be computed in finitely many steps (by specifying a basis).*

Consequently, all associated prime ideals for fields of characteristic 0 can be computed. However, Theorem 6 cannot be generalized any further: from [2, Theorem 7.27], Reufel concludes

**Theorem 7** ([28, Theorem 5]). *There exists a field $F$ that has a strong factorization algorithm, but no algorithm that, given a basis of a submodule of a finitely generated free $F[X_1, \ldots, X_n]$-module ($n \geq 2$), allows us to construct a prime ideal in finitely many steps.*

Thus it is evident that for fields of characteristic $p > 0$, we need a further axiom in addition to (F), in order to guarantee the computability of all associated prime ideals. Seidenberg's 1974 paper [29] gave such an additional property (P), which we discuss in the next section.

### 2.5 Seidenberg's Revision of Hentzelt-Noether-Hermann Theory

In order not to interrupt the the previous section's l. of thought, we begin with the result of Seidenberg, who also recognized in [29] that property (F) is insufficient for computing all associated prime ideals. Thus, he formulated in [29, Proposition 39]:

**Property (P).** *For fields $K$ of characteristic $p > 0$, an algorithm exists, which decides the solvability of systems of linear equations with coefficients in $k$, and computes the solution in the subfield $k^p$, if it exists.*

In [29, Proposition 43], (P) is shown to be equivalent to the existence of an algorithm that allows us to verify the identity

$$[k^p(z_1, \ldots, z_s) : k^p] = p^s \tag{17}$$

for any $z_1, \ldots, z_s$ in $k$. In [29, p. 274], property (P) is characterized by (17). Then the main result is

**Theorem 8** ([29, Proposition 46]). *Constructing all associated prime ideals is possible if and only if $k$ has properties* (F) *and* (P).

This result sheds light on the structure of Seidenberg's paper [29], which is arranged by individual propositions, and which claims to nullify Hermann's work [6]:

| | | |
|---|---|---|
| Propositions | 1-29 | Constructions for any ground field (characteristic 0 is assumed for several) |
| Propositions | 30-32 | Properties of the fundamental form |
| Propositions | 33-38 | Constructions for ground fields with property (F) |
| Propositions | 39-46 | Constructions for ground fields with properties (F) and (P) |
| Propositions | 47-54 | Independence of properties (P) and (F) (examples given here, but not Reufel's) |
| Propositions | 55-66 | Computation of some bounds |

Propositions 67-96 go beyond Hermann's paper [6] with the goal in Propositions 73-96 of presenting a finite theory of polynomial ideals after laying the groundwork in Propositions 67-72. Since Seidenberg (as well as Reufel) works with transformed ideals using (2), practical algorithms cannot be immediately derived from his ideas.

Seidenberg raises the legitimate criticism in his introduction that not all ideal theoretic operations are invertible in [6], e.g. the computation of elimination ideals, which he treats in [29, Propositions 22-23]. He does not use these for computing dimensions, but manages this by computing inverse ideals. Furthermore, it is worth comparing [29, Proposition 19] on representing $\mathfrak{a}$ as the intersection of unmixed ideals with the remarks following (16) in Theorem 4.

As in [6], Seidenberg's paper is also missing the computation of zeros and the computation of prime ideals from given generic zeros. The computation of equivalent H-ideals is also not mentioned, but follows as a special case of [29, Proposition 20], from which follows the computation of the smallest exponent $\varrho$ such that $\mathfrak{a} : \mathfrak{b}^\varrho = \mathfrak{a} : \mathfrak{b}^{\varrho+1}$. What is new in [29, Propositions 42, 45] is the constructibility of the prime ideals $\mathfrak{p}$ belonging to a primary ideal $\mathfrak{q}$ using only (P). Unfortunately, Reufel's paper [28], discussed in §2.4 above, has not found its well-deserved recognition, in spite of the author's detailed review [28R], neither is it cited in [29] nor used by [2].

So [29] has some minor gaps and some overlap with [28]. Thus we find Theorem 5 [28, Theorem 1] in [29, Remark after Proposition 36], as well as Theorem 7 [28, Theorem 5] in [29, Proposition 51], and an example of $(F') \not\Rightarrow (F)$ in [29, pp. 295-296]. However, Definition 5 and Theorem 6 [28, Theorem 2], on which the results are based, are missing.

We note further that Seidenberg always speaks of constructions (like Reufel, based on Fröhlich and Shepherdson) without proving that these are accomplished with algorithms. Hence, Reufel's formulations for (F′) and (F) given in our Definitions 3 and 4, which Seidenberg preferred, reads in original text

(F′) [29, Remark after Proposition 36]: Let (F′) be the condition on $k$ that one can write any polynomial in $k[X_1, \ldots, X_n]$ effectively as the product of primary ideals.

(F) [29, Proposition 33]: Consider the following problem. Given an $f \in k[X]-0$, $X = X_1$, to construct the complete factorization of $f$ over $k$. If this problem has a positive solution for $k$, we say the property (F), or, also, the *factorization theorem*, holds for $k$. For example, any prime field of given characteristic satisfies (F).

As cited at the beginning of this paper, Seidenberg acted on the hope that Hermann's paper [6] had no errors except for the axiomatic problems. [29, footnote 2] leads one to conclude that there would be interest in correcting the errors, which motivated §1, and specifically the list of errors in §1.9 of this paper.

This (sadly deluded) hope also caused Seidenberg to carry over the incorrect degree bounds from [6] into Propositions 55-66: *Computation of Some Bounds*, as the author discovered simultaneously with Fröberg in Stockholm. Before that, it was noticed by Lazard in Poitiers. We will concern ourselves with the corrections of Veltzke and Lazard in the next section.

In summary, it can be estimated that with Seidenberg's paper and (necessarily) the papers by Reufel, Fröhlich-Shepherdson, Veltzke and Lazard, the theoretical foundations for constructibility have been completed to a certain degree. The question of generalizing to all fields with the above properties remains a difficult task (see [21, pp. 134-135]). For the case of polynomial rings over the ring of integers, Seidenberg's constructions were compiled in the sequel paper [30].

### 2.6 Degree Bounds of Veltzke and Lazard

As we already noted in §2.5, Seidenberg passed the wrong degree bounds from [6] to [29, Propositions 53-66], which therefore needs to be corrected using our list of errors §1.9. As was established in §1.3, this pertains to [29, Propositions 55-60, 62-63]. Veltzke had already implemented these corrections in 1958 [31], where, among other things, the wrong formula for $m(t, q, n)$ in [6] was replaced by (9). As indicated in §1.3, Lazard [20, Theorem 1] was able to improve this for the term $-1$. In [22, final theorem], Lazard also presented the wrong degree bounds of Hermann and Seidenberg. We refer to the corrected formula (10) in §1.4 and §1.5, as well as to the almost bizarre example $\kappa(2, 2, 2)$ following (11) in §1.5.

As already noted in §1.3, Reufel used Veltzke's corrected formulas in [27, 28] (see also the author's reviews [27R, 28R]). Seidenberg's missing citation of Reufel's work has proved to be especially unfortunate.

But perhaps this is precisely what inspired Lazard in [22] to obtain improved degree bounds using essentially new methods. This has been achieved in an amazing way, in that these bounds were actually adopted [22, Proposition 10] and on the other hand are attainable using computers (see [22, Propositions 5-9], and also §3.4 in this paper).

## 3 Connections to this Series of Papers

### 3.1 Practicality of Ideal Theoretic Operations in Papers by Gröbner, Lazard & Keller

With Lazard's degree bounds, the transition of these procedures from proof of theoretic feasibility to practical execution seems possible (see §3.3) if we can dispense with the assumption of being transformed using (2). Lazard is right when he alludes in his key paper [21, pp. 132-133] to a gap between 1925 and

1974 relative to this. But in contrast with Gröbner, Schmid, Keller, and the author, most mathematicians interested in this (for example, Krull and Grell) acted on the assumption "that we would be satisfied if Henzelt-Noether-Hermann theory were fixed" [Krull's statement in a 1958 discussion with the author]. In addition, explicitly computed examples may not have been needed until then.

Independent of Hentzelt-Noether-Hermann theory, Gröbner, in several places in his 1949 book [3], gave the first examples without assuming practical algorithms in general. Gröbner's 1950 paper [4] goes further, which Veltzke [31] also addressed in 1958. In [4], the zeros of a P-ideal are not computed by factoring the elementary divisor form (7) as in [6], but rather for the first time using *elimination ideals*. The author continued and expanded Gröbner's crucial idea in XII. Veltzke recognized that passage to residue class rings in [4] in order to exclude those zeros of the elimination ideal that do not lead to zeros of the output ideal is unnecessary. For simple zero dimensional ideals, the consequences drawn from [4] for establishing normal primary decomposition lead to success.

Keller's 1965 paper [10] studies questions about computing a prime ideal from its generic zeros, and then deciding the prime ideal property without transforming using (2), even though the quotient construction plays a crucial role. We will draw our final conclusions from this in §3.4.

## 3.2 On the Logical Sequence of Operations in this Series of Articles

Since this series of articles arose largely from current interests, a logical sequence of operations is not readily recognizable. Because computing ideal intersections, ideal quotients, and equivalent H-ideals requires the computation of the second syzygy module according to §1.3, the latter must be used at the beginning of such a sequence, which will be presented in what follows with the relevant portions of the series of articles or the book [26] and additional remarks [footnotes].

| | | |
|---|---|---|
| 1.1 | Given rational generic zero | |
| 1.2 | Given basis | |
| 2.1 | Computing the minimal basis of an H-ideal | XVIII |
| 2.2 | Deciding membership of a form in an H-ideal | XVIII |
| 2.3 | Deciding equality of H-ideals | XVIII |
| 3.1 | Method of indeterminate coefficients | VIII |
| 3.2 | $u^*$ approach | VIII, XV |
| 3.3 | Proof of basis completeness | VIII, XVII 3.4 |
| 3.4 | Proof of the prime ideal property | [1] |
| 4.1 | Basis representation of ideal sums | trivial |
| 4.2 | Basis representation of ideal products | trivial |
| 5.1 | Computing second syzygy modules using Gaussian elimination | II |
| 5.2 | Consideration of already computed syzygies | XV |
| 5.3 | Computing third and higher syzygy modules using generalized Gaussian elimination | XIX |
| 6. | Computing ideal intersections of H-ideals | [2] |
| 7.1 | Computing ideal quotients $\mathfrak{a} : (F)$ | [3] |
| 7.2 | Computing ideal quotients $\mathfrak{a} : \mathfrak{b}$ of any two H-ideals | [2] |
| 8.1 | Computing equivalent H-ideals from a generic zero of an inhomogeneous P-ideal | VIII |
| 8.2 | Computing equivalent H-ideals from a basis of an inhomogeneous P-ideal | IX, IV |
| 9.1 | Deciding membership of a polynomial in a P-ideal | XVIII |
| 9.2 | Deciding equality of P-ideals | IX, XVIII |
| 9.3 | Computing the minimal basis of P-ideals | IX |
| 9.4 | Minimal bases of arbitrary length for P-ideals | [4] |
| 9.5 | P-ideal bases of minimal length | XVIII |

[1] For rational prime ideals, a consequence of VIII, XV, otherwise still open.
[2] Consequence of II, see [26, §5.14, p. 234].
[3] Consequence of II, see [26, §5.13, p. 232].
[4] See [26, §4.27, p. 184] and [1].

| | | |
|---|---|---|
| 9.6 | Computing intersections of P-ideals | [2] |
| 9.7 | Computing quotients of P-ideals | [2] |
| 10.1 | Computing elimination ideals of prime ideals with given rational generic zeros | XII, XVI |
| 10.2 | Computing elimination ideals with given bases | XII, XV, XVI |
| 10.3 | Computing bases using Gröbner's method | XII, [26, §4.5] |
| 10.4 | Computing zeros of H-ideals | XII |
| 10.5 | Computing prime ideals belonging to isolated components of an H-ideal | [5] |
| 10.6 | Proof of the prime ideal property for an H-ideal | [6] |
| 10.7 | Computing the radical of an H-ideal | [7] |
| 10.8 | Decomposing an H-ideal into quasi-primary components | XVII 1.8 |
| 10.9 | Proof of the quasi-primary property of an H-ideal | [8] |
| 10.10 | Normal primary decomposition of quasi-primary H-ideals | still open |
| 10.11 | Proof of the primary property of an H-ideal | [9] |
| 10.12 | Proof of unmixedness of an H-ideal | [10] |
| 10.13 | Passing to P-ideals using 8.1 or 8.2 and subsequent dehomogenization | trivial |
| 11.1 | Computing volume and Hilbert functions from the syzygy chain | XIV |
| 11.2 | Computing characteristic polynomials as the number of leading monomials not present | XIV |
| 11.3 | Computing characteristic polynomials from a rational generic zero | XIV |
| 11.4 | Listing Hilbert equations with given rational generic zeros | I, VIII, X, XV |
| 11.5 | Listing Hilbert equations with given basis | XI |
| 12.1 | Deciding perfectness from the length of the syzygy chain | III, [26, §5.18] |
| 12.2 | Deciding perfectness by considering sections | VI, [26, §5.18] |
| 12.3 | Deciding imperfectness from the invalidity of Bezout's theorem | [26, §6.4] |

## 3.3 Open Questions, Computing Fundamental Ideals

The schedule given in §3.2 leaves open the practical construction of the normal primary decomposition, whereupon this gap is reduced to normal decomposition of quasi-primary ideals. But whether this structural reduction also facilitates practical computation is likewise still open.

If we follow Hentzelt-Noether-Hermann theory, then by (14), computing fundamental ideals is required again. In addition, computing forms $B^{(i)}(x_i, x_{i+1}, \ldots, x_n)$ using (6) is required for transformed H-ideals. In particular, the author was also able to formulate these definitions in [25] without assuming any transformations, but another practical approach is open. A completely different method would also be desirable here because, as Kummer showed in [19, Theorem 12] (see also [26, §2.22, p. 94]), the fundamental ideal method using (14) does not always produce the optimal normal primary decomposition for monomial ideals.

In many cases however, Theorem 3 with (15) does produce a normal primary decomposition, namely when the unmixedness for quasi-primary ideals can be proved. Many components conjectured to be trivial can also be confirmed by subsequent verification of the intersection construction.

## 3.4 Practical Degree Bounds

After the schedule from §3.2, we deal here with determining the degree bounds for the algorithms that compute the second syzygy module of an H-ideal $\mathfrak{a} \subset K[x_0, x_1, \ldots, x_n]$ (items 5.1 - 5.3 in the schedule) and that compute the basis of rational prime ideals (items 3.2 - 3.3). We shall see that an algorithmic bound for the second task follows from the bound for the first task. The latter bound is simultaneously a bound for the algorithm that computes elimination ideals for a given basis (item 10.2). In what follows, we wish

[5] Follows from 10.4 using 3.1, 3.2, 3.3 in the case of rational generic zeros.
[6] Follows from 10.6 if only one rational generic zero is available, and by 3.1 and 3.2, this yields the output ideal.
[7] Follows from normal primary decomposition of the radical as the intersection of prime ideals computed in 10.5 using 6.
[8] Follows from 10.6 when only one rational generic zero is available, but no prime ideal exists.
[9] Would follow from 10.10.
[10] Would follow from 10.10, unless it can be inferred from other theorems on unmixedness.

to specify bounds $S$ for the total degree in each of the above algorithms, up to which the modules $\mathfrak{M}(t;\mathfrak{a})$ for $t = m_0, m_0+1, \ldots, M, M+1, \ldots, S$ will be examined (with minimal degree $m_0$, maximal degree $M$ of basis forms in $\mathfrak{a}$). In contrast, bounds for the maximal degree of elements of the basis of the second syzygy module were determined in [6, 22], each of which is added to $M$ in order to arrive at our bounds. For $M \geq 2$ the following bounds follow from [22, Propositions 10, 6, 7]:

$$n = 2 : S(M,2) = 3M - 2 \tag{18}$$
$$n = 3 : S(M,3) = 3\binom{M+1}{2} + M - 3 \tag{19}$$
$$n = 4 : S(M,4) = 3M^3 - 2M^2 + 4M - 4. \tag{20}$$

It follows from (19) that we must compute up to degree 18 for $M = 3$ (such as for the Macaulay ideal $\mathfrak{o}_{14}^{(12)}$) and up to degree 31 for $M = 4$, which can be done by computer. Bounds of 71 and 172 for $M = 3$ or $M = 4$, respectively, follow from (20), whose computability by computer needs to be checked.

In general, Lazard claims [22, 9.1(a)]

$$S(M,n) = (n+1)M - n, \tag{21}$$

from which $S(M,n) < (n+1)M$ would follow. This corrects the degree bounds of 2M that the author claimed in [XII, p. 127], [XV, p. 180], and [26, p. 145, l. 19 & p. 205, ll. 22-23] accordingly. In particular, the ideas of Lazard [22, p. 183] lead to a simple counterexample in $K[x_0,x_1,x_2,x_3]$ with $\mathfrak{a} = (F_1,F_2,F_3,F_4)$, where $F_1 = x_0^2$, $F_2 = x_0x_3 - x_1^2$, $F_3 = x_1x_3 - x_2^2$, $F_4 = x_2x_3$ and the second syzygy module is

$$\begin{pmatrix} F_2 & F_3 & F_4 & 0 & 0 & 0 & x_3^3 \\ -F_1 & 0 & 0 & F_3 & F_4 & 0 & -x_0x_3^2 \\ 0 & -F_1 & 0 & -F_2 & 0 & F_4 & -x_0x_1x_3 \\ 0 & 0 & -F_1 & 0 & -F_2 & -F_3 & -x_0x_1x_2 \end{pmatrix}.$$

Here, $M = 2$, $2M = 4$, but $S = 2 + 3 = 5$. I thank R. Fröberg of Stockholm for the appropriate reference.

For computing rational prime ideals $\mathfrak{p}$ with generic zeros $y_i = y_i(t_0,\ldots,t_d)$, where each $y_i$ is a form of degree $m$ in $t_0,\ldots,t_d$, the author claimed $m$ to be the bound for the combinatorial algorithm ($u^*$ approach, syzygy computation) in [26, p. 295, ll. 27-28]. This bound cannot be improved to $m-1$ (see [26, Ex. 8.6.2]).

Since the coordinate functions of generic zeros of rational prime ideals $\mathfrak{p}$ have degree $m$, they satisfy equations of degree at most $m$. To compute $\mathfrak{p}$, we must compute at least up to $t = m$. If $\mathfrak{a} \subseteq \mathfrak{p}$ is the H-ideal whose basis forms are those in $\mathfrak{p}$ of degree at most $m$, then $\mathfrak{M}(t;\mathfrak{a}) = \mathfrak{M}(t;\mathfrak{p})$ for $t = 1,\ldots,m$. Thus in particular, $\mathfrak{a}$ contains all elimination forms that depend only on $x_{i_0},\ldots,x_{i_d}$. By [10, p. 161], additional basis forms can be obtained by repeated division by coefficient polynomials $a$ of elimination forms $F$. Thus if $\mathfrak{a} = (F_1,\ldots,F_s)$ with maximal degree $M \geq m$, thus if $\deg(F_s) = M$, then $\mathfrak{a} : (A)$ is the set of all $C$ such that $CA = G_1F_1 + \ldots + G_sF_s$. Therefore, since $\deg(A) \leq M-1$, the additional forms have degree at most $S_1 := S(M,n)$.

But we also obtain these forms using our algorithm if the substitutions are continued up to degree $S_1$. If no new basis forms appear, we can stop. On the other hand, if $M_2$ is the new maximal degree ($M < M_2 \leq S_1$), then we continue up to $S_2 := S(M_2,n)$, etc. In this way, we obtain an algorithmic degree bound, as claimed. Unfortunately, the author has been unable to prove $m$ as a degree bound. In any case, for Lazard's degree bounds, which first of all are attainable for $n = 3$ using computers, the critical step of going from theoretical proof of algorithms to practical and complete procedures was successful.

## References

[1] H. Bresinsky, M. Fuller. Minimal Bases of Polynomial Ideals. *Houston Journal of Mathematics* **3** (1977): 453-457.

[2] A. Fröhlich, J. Shepherdson. Effective Procedures in Field Theory. *Philos. Trans. Royal Society A* **248** (1956): 407-432.

[3] W. Gröbner. *Moderne algebraische Geometrie* [*Modern Algebraic Geometry*]. Springer, 1949.

[4] W. Gröbner. Über die Eliminationstheorie [On Elimination Theory]. *Monatshefte für Mathematik* **54** (1950): 71-78. [English translation by M. Abramson in *ACM SIGSAM Bulletin* **32**/2 (1998): 40-46].

[5] K. Hentzelt (edited by Emmy Noether). Zur Theorie der Polynomideale und Resultanten [On the Theory of Polynomial Ideals and Resultants]. *Mathematische Annalen* **88** (1923): 53-79.

[6] G. Hermann. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale [The Question of Finitely Many Steps in Polynomial Ideal Theory]. Ph.D. dissertation, University of Göttingen, 1926. In *Mathematische Annalen* **95** (1926): 736-788. [English translation by M. Abramson in *ACM SIGSAM Bulletin* **32**/3 (1998): 8-31.

[7] D. Hilbert. Über die Theorie der algebraischen Formen [On the Theory of Algebraic Forms]. *Mathematische Annalen* **36** (1890): 473-534. [English translation by M. Ackerman in *Hilbert's Invariant Theory Papers* (R. Hermann, ed). Lie Groups: History, Frontiers and Applications **8**, Math Sci Press, 1978, 143–224.]

[8] O. Keller. Eine Bemerkung zur Ausführung der Körpertheoretischen Operationen in erträglich vielen Schritten [A Remark on Carrying Out Field Theoretic Operations in Tolerably Many Steps]. *Mathematische Zeitschrift* **63** (1955): 277-285.

[9] O. Keller. Zur Berechnung des Galoisschen Körpers und der Galoisschen Gruppe einer Gleichung in erträglich vielen Schritte [On the Computation of Galois Fields and the Galois Group of an Equation in Tolerably Many Steps]. *Berichte über die Verhandlung Sächsischen Akademie der Wissenschaften zu Leipzig* **104**/5 (1961): 1-23.

[10] O. Keller. Berechnung eines Primideals aus seiner allgemeinen Nullstelle [Computation of a Prime Ideal from its Generic Zeros]. *Mathematische Zeitschrift* **87** (1965): 160-162.

[11] M. Kneser. Bemerkung über die Primpolynomzerlegung in endlich vielen Schritte [Remark on the Prime Factorization of Polynomials in Finitely Many Steps]. *Mathematische Zeitschrift* **57** (1953): 238-240.

[12] W. Krull. *Idealtheorie* [*Ideal Theory*]. Ergebnisse der Mathematik, Volume **4**, Issue 3. Springer, 1935.

[13] W. Krull. Theorie der Polynomideale und Eliminationtheorie [Polynomial Ideal Theory and Elimination Theory]. *Enzyklopedia der Mathematische Wissenschaft* I, second edition, Volume 5, Article 12. Teubner, 1939, 1-53.

[14] W. Krull. Parameterspezialisierung in Polynomringen [Parameter Specialization in Polynomial Rings] I. *Archiv der Mathematik* **1** (1948-49): 56-64.

[15] W. Krull. Parameterspezialisierung in Polynomringen [Parameter Specialization in Polynomial Rings] II. *Archiv der Mathematik* **1** (1948-49): 129-137.

[16] W. Krull. Über Polynomzerlegung mit endlich vielen Schritte [On Polynomial Factorization in Finitely Many Steps] I. *Mathematische Zeitschrift* **59** (1953): 57-60.

[17] W. Krull. Über Polynomzerlegung mit endlich vielen Schritte [On Polynomial Factorization in Finitely Many Steps] II. *Mathematische Zeitschrift* **59** (1954): 296-298.

[18] W. Krull. Über Polynomzerlegung mit endlich vielen Schritte [On Polynomial Factorization in Finitely Many Steps] III. *Mathematische Zeitschrift* **60** (1954): 109-111.

[19] R. Kummer, B. Renschuch. Potenzproduktideale [Monomial Ideals] I. *Publ. Math. Debrecen* **17** (1970): 81-98.

[20] D. Lazard. Algèbre linéaire sur les anneaux de polynomes [Linear Algebra over Polynomial Rings]. *Comptes Rendus des Journées Mathématiques de SMF* (Montpellier, 1974), 365-368. Montpellier University of Science and Technology in Languedoc, Cahiers Mathématique **3** (1974).

[21] D. Lazard. Algorithmes fondementaux en algèbre commutative [Fundamental Algorithms in Commutative Algebra]. *Astérisque* **38-39** (1976): 131-138.

[22] D. Lazard. Algébre linéaire sur $K[X_1, \ldots, X_n]$ et élimination [Linear Algebra over $K[X_1, \ldots, X_n]$ and Elimination]. *Bulletin de la Société Mathematique de France* **105** (1977): 165-190.

[23] P. McCarthy. Note on Primary Ideal Decomposition. *Canadian Journal of Mathematics* **18** (1966): 950-952.

[24] E. Noether. Eliminationstheorie und allgemeine Idealtheorie [Elimination Theory and General Ideal Theory]. *Mathematische Annalen* **90** (1923): 229-261.

[25] B. Renschuch. Zur Definition der Grundideal [On the Definition of the Fundamental Ideal]. *Mathematische Nachrichten* **55** (1973): 63-71.

[26] B. Renschuch. *Elementare und praktische Idealtheorie* [*Elementary and Practical Ideal Theory*]. Mathematik für Lehrer, Volume **16**. Berlin: VEB Deutsche Verlag der Wissenschaft, 1976.

[27] M. Reufel. Spezialisierung in Polynomringen [Specialization in Polynomial Rings]. Ph.D. dissertation, University of Bonn. *Bonner Mathematische Schriften* **19** (1963).

[27R] Review by B. Renschuch in *Zentralblatt für Mathematik* **118** (1965/66): 273-274.

[28] M. Reufel. Konstruktionsverfahren bei Moduln über Polynomringen [Constructive Methods in Modules over Polynomial Rings]. *Mathematische Zeitschrift* **90** (1965): 231 -250.

[28R] Review by B. Renschuch in *Zentralblatt für Mathematik* **161** (1969): 40-42.

[29] A. Seidenberg. Constructions in Algebra. *Transactions of the American Mathematical Society* **197** (1974): 273-313

[29R] Review by P. Samuel in *Mathematical Reviews* **50** (1975): #2141.

[30] A. Seidenberg. Constructions in a Polynomial Ring Over the Ring of Integers. *American J. Math.* **100** (1978): 685-703.

[31] C. Veltzke (married name Krause). *Berechnugsprobleme bei Polynomideale* [*Computational Problems in Polynomial Ideals*]. Diploma thesis, Humboldt University, Berlin, 1958.

[32] B. van der Waerden. Eine Bemerkung über die Unzerlegbarkeit von Polynomen [A Remark on the Indecomposability of Polynomials]. *Mathematische Annalen* **102** (1930): 738-739.

[33] B. van der Waerden. *Moderne Algebra* [*Modern Algebra*] 1, first edition. Springer GMW **33**, 1930.

[34] B. van der Waerden. Zur algebraischen Geometrie 19: Grundpolynom und zugeordnete Form [On Algebraic Geometry 19: The Fundamental Polynomial and Associated Form]. *Mathematische Annalen* **136** (1958): 139-155.

[35] H. Wussing. *Emmy Noether*. In H. Wussing, W. Arnold, eds. *Biographien bedeutender Mathematiker* [*Biographies of Important Mathematicians*]. Verlag Volk und Wissen, 1975, 504-513.

## Papers Cited from this Series of Articles [added in translation]

The original German paper did not include bibliographic data for Renschuch's papers in this series (only Roman numerals). We include full bibliographic data here. All titles listed here begin with "Beiträge zur konstruktiven Theorie der Polynomideale ["Contributions to Constructive Polynomial Ideal Theory" ]..." and all were published in *Wissentschaftliche Zeitschrift der Pädagogische Hochschule "Karl Liebknecht" Potsdam* [*Scientific Journal of the "Karl Liebknecht" Teachers College in Potsdam*]. Thus this listing includes only the Roman numeral, subtitle, any coauthors, volume, year, and page numbers. See also the translator's *Historical Background for B. Renschuch's Papers* in **37**/2 (2003): 33-34 of this publication.

I *Zur Bestimmung der Basis eines H-Ideals bei vorgegebener allgemeiner Nullstelle* [*On Determining the Basis of an H-Ideal for Given Generic Zeros*]. **17** (1973): 141-146.

II *Zur Bestimmung des zweiter Syzygienmoduls mit Hilfe des Gausschen Eliminierungsverfahren* [*On Determining the Second Syzygy Module using Gaussian Elimination*]. **17** (1973): 147-151.

III *Über eine Klasse imperfekter Primideale* [*On a Class of Imperfect Prime Ideals*]. **17** (1973): 151-153.

IV *Zur Berechnung von äquivalenten H-Idealen und Minimalbasen für inhomogene P-Ideale* [*On Computing Equivalent H-Ideals and Minimal Basis for Inhomogeneous P-ideals*] (with E. Matuatat). **18** (1974): 95-98.

V *Syzygienkette von* $(\mathfrak{a}, F)$ [*Syzygy Chains for* $(\mathfrak{a}, F)$ ]. **18** (1974): 98-100.

VI *Veronesche Projektionskurven in* $S_3$ [*Projective Veronese Curves in* $S_3$]. **18** (1974): 100-106.

VIII *Basisbestimmung von primen H-Idealen mit vorgegeben rationalen allgemeinen Nullstellen aus der Hilbertschen Gleichungen* [*Determining Bases for Prime H-Ideals with given rational generic zeros from the Hilbert Equations*]. **19** (1975): 106-113.

IX *Basisdarstellungen inhomogener Polynomideale* [*Bases of Inhomogeneous Polynomial Ideals*]. **19** (1975): 113-121.

X *Basisdarstellungen Vahlenscher Kurven und allgemeiner rationaler Raumkurven* [*Basis Representations of Vahlen Curves and General Rational Space Curves*]. **20** (1976): 109-122.

XI *Aufstellung der Hilbertschen Gleichungen für H-Ideale bei vorgegebener Basis* [*Displaying Hilbert Equations for H-Ideals for a Given Basis*]. **20** (1976): 123-125.

XII *Zur Berechnung von Eliminationsideale* [*On Computing the Elimination Ideal*]. **20** (1976): 126-130.

XIV *Zur Berechnung der Hilbertfunktion* [*On Computing Hilbert Functions*]. **21** (1977): 163-173.

XV *Algorithmen zur Berechnung von Idealen, Syszygienmoduln und Eliminationsideale* [*Algorithms for Computing Ideals, Syzygy Modules and Elimination Ideals*]. **21** (1977): 173-181.

XVI *Klassifikation eindimensionaler Abhyankarsche Ideale aus* $K[x_0, x_1, x_2, x_3]$ *mit* $m = 4$ *und* $m = 5$ [*Classification of one dimensional Abhyankar Ideals in* $K[x_0, x_1, x_2, x_3]$ *with* $m = 4$ *and* $m = 5$]. **23** (1979): 13-28.

XVII *Zur Hentzelt/Noether/Hermannschen Theorie der endlich viele Schritte* [*On Hentzelt/Noether/Hermann Theory of Finitely Many Steps*]. **24** (1980): 87-99, **25** (1981): 125-136. [the present paper]

XVIII *Zum Nachweis von Gleichheit, Elementrelation und Basen minimale Länge durch Gjuntersche Basen* [*On Proving Equality, Element Relations and Bases of Minimal Length Via Gjunter Bases*]. **27** (1983): 17-23.

XIX *Zur Berechnung 3-ter und höherer Syzygienmoduln* [*On Computing 3rd and Higher Syzygy Modules*]. **28** (1984): 143-148.