A CONCISE PROOF OF THE KRONECKER POLYNOMIAL SYSTEM SOLVER FROM SCRATCH

CLÉMENCE DURVYE AND GRÉGOIRE LECERF

Abstract. Nowadays polynomial system solvers are involved in sophisticated computations in algebraic geometry as well as in practical engineering. The most popular algorithms are based on Gröbner bases, resultants, Macaulay matrices, or triangular decompositions. In all these algorithms, multivariate polynomials are expanded in a monomial basis, and the computations mainly reduce to linear algebra. The major drawback of these techniques is the exponential explosion of the size of the polynomials needed to represent highly positive dimensional solution sets. Alternatively, the "Kronecker solver" uses data structures to represent the input polynomials as the functions that compute their values at any given point. In this paper we present the first self-contained and student friendly version of the Kronecker solver, with a substantially simplified proof of correctness. In addition, we enhance the solver in order to compute the multiplicities of the zeros without any extra cost.

Introduction

Polynomial system solving has been a central topic in computer algebra from the middle of the sixties. This topic may be seen from various points of view, which explains that many kinds of solvers have been designed so far. The most popular solvers are certainly the ones derived from the Buchberger algorithm to compute Gröbner bases. Other popular solvers are based on triangular decompositions, resultants, or Macaulay matrices. Nowadays polynomial system solvers are implemented in all the computer algebra systems, and lie at the heart of sophisticated tools to handle computations in algebraic geometry, but also to solve practical problems arising from engineering. Non-specialist readers may consult the following related books: [5, 18, 32, 20, 56, 66, 15, 16].

In all the aforementioned families of algorithms, the multivariate polynomials are represented by the vectors of their coefficients in the canonical monomial basis. Usually we say that the polynomials are *expanded*. With such a representation, each elementary operation can often be interpreted in terms of Gaussian elimination. Thus linear algebra subroutines often play a central role in all these methods. Because of the analogy between the Buchberger algorithm and the Knuth-Bendix algorithm in the language theory, we often refer to these methods as *rewriting techniques* [17].

Instead of expanding a polynomial in the monomial basis, alternative suitable data structures can be used in order to represent it as the function that computes its values at any given points. Several solvers have been designed for more than one decade in order to take advantage of such representations. We often refer to these algorithms as *evaluation techniques*. The *Kronecker solver*, that is the subject of this paper, belongs to this family of solvers.

Date: Preliminary version of June 16, 2006.

2000 *Mathematics Subject Classification.* Primary 14Q15; Secondary 68W30.

Key words and phrases. Polynomial system solving, elimination theory, algorithm, complexity.

This work was supported in part by the French Research Agency (ANR Gecko).

From the complexity point of view, expanding multivariate polynomials coming from elimination is often a bad idea because of the exponential explosion of the number of their monomials. On the contrary, eliminant polynomials behave very well from the evaluation point of view. Let us illustrate these facts with three families of examples. The first family of examples is the determinant of a $n \times n$ matrix. This determinant is an eliminant polynomial of degree n in the n^2 entries of the matrix. It is well known that its number of monomials is $n!$, whereas it can be evaluated at any point with $\mathcal{O}(n^3)$ arithmetic operations. The second family is the resultant of two univariate polynomials of degrees n with unknown coefficients. This resultant is an eliminant polynomial in the $2(n+1)$ unknowns. Its number of monomials increases exponentially in n, whereas it is well known that it can be evaluated in time almost linear in n [20, Chapter 11]. Finally, the third family concerns a system of n dense polynomials of degree d in $2n$ variables. Informally speaking, if these polynomials are sufficiently generic then their set of common solutions has dimension n and degree d^n. In this situation, eliminant polynomials in n variables have degree d^n, hence a number of monomials that grows with d^{n^2} when n tends to infinity, and when d is fixed. On the other hand, the algorithms presented in [50] can evaluate such eliminant polynomials with a number of arithmetic operations that only grows with d^n.

The next paragraphs contain a short survey on evaluation techniques. Then, we give an overview of the Kronecker solver, and we summarize the main contributions of this paper. The two first sections of this paper contain all the mathematical results needed to prove the correctness of the Kronecker solver, that is presented in the last section. The third section is devoted to the representation of radical unmixed ideals.

A Short Survey on Evaluation Techniques. The nice evaluation properties of eliminant polynomials were first explored in a series of works initiated by Giusti, Heintz, Morais and Pardo at the beginning of the nineties. The first algorithm, proposed in [24], was computing the dimension of the solution set of a system of homogeneous polynomials. The multivariate polynomials occurring during the computations were represented by *straight-line programs* (see definition in [8, Chapter 4]). In [29, 19, 43] it was then shown that the polynomials involved in the Nullstellensätz also had nice evaluation properties, and could be thus computed efficiently. The first step towards the design of a fast polynomial solver taking advantage of the straight-line program representation was first done in [27, 58]. Therein the goal was the development of a solver with a polynomial cost in geometric and Diophantine invariants of the solution sets, instead of other extrinsic quantities such as the Hilbert regularity deeply involved in the rewriting techniques. In the solver proposed in [27], the input system was represented by a straight-line program and the algorithm was incremental in the number of equations to be solved. The Noether position (see definition in Section 1.2) appeared as a central ingredient. However this first solver was using an evaluation data structure that was permitting loops of finite depth. The eliminant polynomials were represented by short programs, but their evaluation costs were still high.

As announced at the end of [27], this bad behavior could be suppressed thanks to the use of the Newton operator. This idea was first developed in [26] in order to "compress" the straight-line programs built in the intermediate steps of the solver. A refined version of [27] together with new lower bounds in Diophantine approximation were then published in [22]: the lifting fibers (namely, the ideals written $\mathcal{J}_i$ in the sequel) appeared as an efficient representation of the positive dimensional varieties. These works yielded a major theoretical complexity breakthrough in the elimination theory. The different versions of the solver were sharing the following

features: the input polynomials were encoded by a straight-line program; the resolution was computed equation by equation; it was assumed that the system had only a finite number of solutions; the algorithm was computing a *univariate representation* (see definition in Section 3) of the set of the solutions; the running time was linear in the size of the input straight-line program, and was polynomial in the largest geometric degree of the intermediate systems; straight-line programs were used all along the computations in order to represent all the multivariate polynomials. Later on an other refinement was proposed in [28] so that the cost remains polynomial in the latter quantities and in the height of the solution set for the classical Turing machine model.

The algorithms described in [22, 28] were simplified and their proofs detailed in Morais' Ph.D. Thesis [57]. The space complexity analysis and algorithmic improvements were then proposed in [55]. The bit-complexity analysis and important applications for the arithmetic Nullstellensätz problem were further developed in [33, 34].

In order to implement these solvers, it was necessary to begin with programming efficient evaluation data structures. With this goal in mind, the first steps were presented at the TERA'1996 conference held in Santander (Spain) by Aldaz, and by Castaño, Llovet, and Martìnez [9]. Later on a `C++` implementation of straight-line programs was done by Hägele. Then another library was written in the `Haskell` language [7]. Independently, other experiments were conducted to implement the algorithm of [24] in the `Maple` computer algebra system, that was readily offering an evaluation data structure [23]. All these trials led to the conclusion that huge evaluation data structures were involving so much memory management that the expected theoretical costs could not be observed in practice.

The solution to this problem came from a program transformation technique called *deforestation* [23], that was used in theoretical computer science to eliminate the building of intermediate data introduced by composition of functions. In some cases this transformation can be performed automatically, but it required some effort to use it in the context of [24]. Informally speaking, the deforestation led in [23] to a paradigm telling us that the computation and the storage of the intermediate evaluation data structures are useless if one rewrites the algorithms in a suitable manner. Finally, this paradigm led to a successful implementation of the ideas contained in [24].

The deforestation paradigm was then applied to the solver given in [57]. Presented in [30], this work led to a complete rewriting of the solver, to several algorithmic simplifications, and to sharp complexity bounds. Therein, the new central ingredients were the Kronecker representation of the varieties (originally due to Kronecker in [44], see definition in Section 3) and the idea of the lifted curves (namely, the ideals written $\mathcal{K}_i$ in the sequel). The new algorithm was programed in the `Magma` computer algebra system, and was called `Kronecker` [46] in homage to Leopold Kronecker for his seminal work about the elimination theory. The complete removal of the intermediate straight-line programs led to the following features: only the input system needs to be represented by a straight-line program, and the algorithm handles polynomials in at most two variables over the ground field. Similar complexity analyzes and the idea of the lifted curve were independently presented in [37].

Later, evaluation techniques led to algorithms that compute the equidimensional decomposition of any polynomial system. These algorithms either perform a pretreatment on the input system in order to avoid multiple components in the intermediate steps of the solving, or they use a generalization of the Newton operator to directly deal with multiple components. The former approach was developed in [47, 41, 40, 42, 39], while the latter approach was achieved in [49, 50]. Of course,

the rational and absolute irreducible decompositions can be easily deduced from the equidimensional decomposition by factoring the univariate representations of the equidimensional components. For instance, one can use the recent fast algorithms proposed in [6, 52, 51, 14].

Evaluation techniques have been applied with success to solve overdetermined systems [31] and parametric systems [35, 63, 59]. They are also well suited to computations in real algebraic geometry [2, 3, 4, 62, 61]. The `Kronecker` software has been used in order to solve problems arising from cryptography [21], to construct the "foveal spaces" that model the visual reception on the retina [54], and to design new multichannel wavelets [53]. Furthermore, the equation by equation incremental approach has recently been adapted to the context of numerical solving by homotopy continuation [65]. In this vein, theoretical comparisons between the numerical and symbolic frameworks have been established in [12, 11, 13].

Finally, concerning lower bounds on the complexity of polynomial system solving, the interested reader may consult [19, 58, 36, 25, 10]. In a nutshell, and under some technical assumptions, the main result of [10] tells us that the Kronecker solver belongs to some "optimal complexity class."

Overview of the Kronecker Solver. Throughout this paper, $\mathbb{K}$ denotes a commutative field of characteristic 0. The input polynomial system is given by a sequence of equations $f_1 = \cdots = f_n = 0$ and an inequation $g \neq 0$, where $f_1, \ldots, f_n$ and g belong to $\mathbb{K}[x_1, \ldots, x_n]$. In practice these polynomials are expected to be represented by an evaluation data structure (a straight-line program, for instance).

We write $\mathcal{I} : g^\infty = \{f \mid \exists n \geq 0,\ g^n f \in \mathcal{I}\}$ for the *saturation* of the ideal $\mathcal{I} \subseteq \mathbb{K}[x_1, \ldots, x_n]$ with respect to g, and we introduce the intermediate ideals

$$\mathcal{I}_i = (f_1, \ldots, f_i) : g^\infty, \text{ for } i \in \{1, \ldots, n\}.$$

By convention we let $\mathcal{I}_0 = (0)$. The version of the Kronecker solver considered in this paper requires the following hypotheses: f_{i+1} is a nonzerodivisor modulo $\mathcal{I}_i$, and $\mathcal{I}_i$ is radical, for all $i \in \{0, \ldots, n-1\}$. In particular we will see that these requirements imply the finiteness of the solution set of the system. In Section 4.1 we will show that, after performing a random affine change of the variables in the input system, the algorithm can safely compute the finite sets of zeros of the ideals

$$\mathcal{J}_i = \sqrt{\mathcal{I}_i + (x_1, \ldots, x_{n-i})},$$

in sequence for i from 1 to n, with a high probability of success. The set of zeros of $\mathcal{J}_i$ is represented by i univariate polynomials $q, w_{n-i+2}, \ldots, w_n$ in $\mathbb{K}[x_{n-i+1}]$ such that

$$\mathcal{J}_i = (q, q' x_{n-i+2} - w_{n-i+2}, \ldots, q' x_n - w_n) + (x_1, \ldots, x_{n-i}).$$

Such a representation is called a *Kronecker representation* of $\mathcal{J}_i$, but it also bears the name of *rational univariate representation* [1, 60].

The computation of a Kronecker representation of $\mathcal{J}_{i+1}$ from a representation of $\mathcal{J}_i$ divides into the following three steps:

(1) *Lifting step.* Compute a Kronecker representation of
$$\mathcal{K}_i = \sqrt{\mathcal{I}_i + (x_1, \ldots, x_{n-i-1})}.$$
(2) *Intersection step.* Compute a representation of $\sqrt{\mathcal{K}_i + (f_{i+1})}$.
(3) *Cleaning step.* Compute a representation of $\sqrt{\mathcal{K}_i + (f_{i+1})} : g^\infty$.

Of course the algorithm stops as soon as it encounters an empty set of solutions, that is as soon as $\mathcal{I}_i = (1)$. Geometrically speaking, $\mathcal{K}_i$ is a one dimensional ideal whose set of zeros is a solution curve of the ith first equations. This ideal is computed from $\mathcal{J}_i$ by means of an effective version of the implicit function theorem. Then,

during the intersection step, we compute the intersection of the latter curve with the hypersurface defined by $f_{i+1} = 0$. This intersection is made of a finite set of points, from which we remove the ones contained in the hypersurface defined by $g = 0$ during the cleaning step.

Our Contributions. For the first time, this paper presents a concise version of the Kronecker solver together with a self-contained proof of the correctness. The only prerequisites concern elementary facts about the Zariski topology, the primary decomposition of ideals (for instances, see [45, Chapter X, Section 3] or [32, Chapter 4]), and the theory of modules over principal rings (for instance, see [45, Chapter III, Section 7]). In the first section, we start with a constructive treatment of the dimension via the Noether normalization. In the second section, we prove all the mathematical results involved in our incremental approach to solving, including the principal ideal theorem, the definition of the degree of an ideal, and the Bézout theorem. Of course, all these results are very classical in the literature but our presentation is rather compact and does not make use of the Hilbert series. Our proofs follow geometrical ideas that are directly connected to our algorithms.

Beyond the pedagogical interests, we made substantial simplifications in the proof of the correctness of the solver, which made us possible to drop some radicality hypotheses in several places. For instance our Theorem 1.27 generalizes [30, Corollary 2] to unmixed ideals.

Our simplifications also concern the presentation of the algorithm. In particular, the intersection step detailed in 4.3 corresponds to the algorithm sketched in [48, Chapter V, Section 4], and implemented in the `Kronecker` package [46]; this algorithm is simpler than the one described in [30, Section 6.2].

Finally these simplifications and improvements have allowed us to enhance the Kronecker solver in order to compute the multiplicities of the zeros without any extra cost (see Section 4.3). We are now working on the propagation of this enhancement to the aforementioned equidimensional decomposition algorithms in order to compute the local algebras at the generic points of the irreducible components. That will be a first step toward the computation of the primary decomposition by means of evaluation techniques.

1. Dimension and Multiplication Endomorphisms

We start this section with some classical definitions: algebraic and integral dependencies, and the dimension of an ideal $\mathcal{I}$ in a polynomial ring via the transcendence degree. We present the Noether normalization as a practical ingredient to compute the dimension. Then, we relate the unmixedness of $\mathcal{I}$ to some torsion-freeness of a suitable module. At the end of this section we give some important properties of the multiplication by a polynomial f in the quotient by $\mathcal{I}$.

Throughout this paper, $\mathcal{I}$ denotes an ideal of $\mathbb{K}[x_1, \ldots, x_n]$. The *total degree* of a polynomial q is written $\deg(q)$, and its *partial degree* in the variable x_j is written $\deg_{x_j}(q)$.

1.1. Algebraic and Integral Dependencies.

Let $\mathbb{A}$ be a subring of $\mathbb{K}[x_1, \ldots, x_n]$ with unity.

Definition 1.1. Some polynomials $e_1, \ldots, e_s$ in $\mathbb{K}[x_1, \ldots, x_n]$ are *algebraically dependent* modulo $\mathcal{I}$ when there exists a nonzero polynomial E with s variables over $\mathbb{K}$ such that $E(e_1, \ldots, e_s) \in \mathcal{I}$. Otherwise they are *algebraically independent* modulo $\mathcal{I}$. A polynomial $e \in \mathbb{K}[x_1, \ldots, x_n]$ is *algebraic* over $\mathbb{A}$ modulo $\mathcal{I}$ if there exists a nonzero polynomial $q \in \mathbb{A}[T]$ such that $q(e) \in \mathcal{I}$. Such a polynomial e is *integral* over $\mathbb{A}$ modulo $\mathcal{I}$ if there exists a nonzero *monic* (*i.e.* with leading coefficient 1) polynomial $q \in \mathbb{A}[T]$ such that $q(e) \in \mathcal{I}$.

Algebraic and integral dependencies are preserved when passing to the radical of $\mathcal{I}$, as detailed in the following lemma:

Proposition 1.2. *Some polynomials $e_1, \ldots, e_s$ in $\mathbb{K}[x_1, \ldots, x_n]$ are algebraically independent modulo $\mathcal{I}$ if, and only if, they are algebraically independent modulo $\sqrt{\mathcal{I}}$. A polynomial $e \in \mathbb{K}[x_1, \ldots, x_n]$ is algebraic (respectively, integral) over $\mathbb{A}$ modulo $\mathcal{I}$ if, and only if, it is algebraic (respectively, integral) over $\mathbb{A}$ modulo $\sqrt{\mathcal{I}}$.*

Proof. The proof is straightforward from the definitions. □

We will use the following classical properties several times:

Proposition 1.3. *Let e_1, e_2 be in $\mathbb{K}[x_1, \ldots, x_n]$.*

(a) *If e_1 and e_2 are integral over $\mathbb{A}$ modulo $\mathcal{I}$ then so are $e_1 + e_2$ and $e_1 e_2$.*
(b) *If e_1 is integral over $\mathbb{A}$ modulo $\mathcal{I}$, and if e_2 is integral over $\mathbb{A}[e_1]$ modulo $\mathcal{I}$, then e_2 is integral over $\mathbb{A}$ modulo $\mathcal{I}$.*

Proof. See for instance [45, Chapter VII, Section 1, Propositions 1.3 and 1.4]). □

For any $e \in \mathbb{K}[x_1, \ldots, x_n]$, we denote by $e^\sharp \in \mathbb{K}[x_0, x_1, \ldots, x_n]$ the *homogenization* of e with respect to the new variable x_0, and by $\mathcal{I}^\sharp \subseteq \mathbb{K}[x_0, x_1, \ldots, x_n]$ the ideal generated by the homogenized polynomials of $\mathcal{I}$. For any $e \in \mathbb{K}[x_0, x_1, \ldots, x_n]$ we write $e^\flat$ for $e(1, x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n]$.

Lemma 1.4. *Some polynomials $e_1, \ldots, e_s$ in $\mathbb{K}[x_1, \ldots, x_n]$ are algebraically dependent modulo $\mathcal{I}$ if, and only if, $x_0, e_1^\sharp, \ldots, e_s^\sharp$ are algebraically dependent modulo $\mathcal{I}^\sharp$.*

Proof. If $e_1, \ldots, e_s$ are algebraically dependent modulo $\mathcal{I}$ then, by homogenizing, we directly obtain that $x_0, e_1^\sharp, \ldots, e_s^\sharp$ are algebraically dependent modulo $\mathcal{I}^\sharp$. Conversely, let E be a nonzero polynomial over $\mathbb{K}$ such that $E(x_0, e_1^\sharp, \ldots, e_s^\sharp) \in \mathcal{I}^\sharp$. Since $\mathcal{I}^\sharp$ is homogeneous, we can assume that E is homogeneous for the weighted degree $(1, \deg(e_1), \ldots, \deg(e_s))$. The conclusion thus follows by substituting 1 for x_0 in $E(x_0, e_1^\sharp, \ldots, e_s^\sharp) \in \mathcal{I}^\sharp$. □

Definition 1.5. A polynomial $e \in \mathbb{K}[x_1, \ldots, x_n]$ is *generally integral* over $\mathbb{A}$ modulo $\mathcal{I}$ if there exists a nonzero monic polynomial $q \in \mathbb{A}[T]$ such that $q(e) \in \mathcal{I}$, and such that

$$\deg(q(x_1, \ldots, x_n, T^{\deg(e)})) = \deg_T(q(x_1, \ldots, x_n, T^{\deg(e)})), \tag{1.1}$$

where q is seen in $\mathbb{K}[x_1, \ldots, x_n, T]$.

For any subring $\mathbb{A}$ of $\mathbb{K}[x_1, \ldots, x_n]$, we write $\mathbb{A}^\sharp$ for the subring of $\mathbb{K}[x_0, x_1, \ldots, x_n]$ generated by x_0 and by the homogenized polynomials of $\mathbb{A}$. For example, if $\mathbb{A} = \mathbb{K}[x_1, \ldots, x_r]$ then $\mathbb{A}^\sharp$ is $\mathbb{K}[x_0, x_1, \ldots, x_r]$. The following properties are direct consequences of the definition:

$$\forall e \in \mathbb{A}^\sharp,\ e^\flat \in \mathbb{A}, \tag{1.2}$$

$$\forall e \in \mathbb{A}^\sharp,\ \text{any homogeneous component of } e \text{ belongs to } \mathbb{A}^\sharp. \tag{1.3}$$

Assertion (1.3) is equivalent to saying that $\mathbb{A}^\sharp$ inherits the usual graduation of $\mathbb{K}[x_0, x_1, \ldots, x_n]$.

Lemma 1.6. *Let $e \in \mathbb{K}[x_1, \ldots, x_n]$. The following assertions are equivalent:*

(a) *e is generally integral over $\mathbb{A}$ modulo $\mathcal{I}$.*
(b) *$e^\sharp$ is generally integral over $\mathbb{A}^\sharp$ modulo $\mathcal{I}^\sharp$.*
(c) *$e^\sharp$ is integral over $\mathbb{A}^\sharp$ modulo $\mathcal{I}^\sharp$.*

Proof. If (a) holds then there exists a polynomial $q = T^\alpha + a_1 T^{\alpha-1} + \cdots + a_\alpha \in \mathbb{A}[T]$ such that $q(e) \in \mathcal{I}$, and such that equality (1.1) holds. It thus follows that

$$(e^\sharp)^\alpha + x_0^{\deg(e)-\deg(a_1)} a_1^\sharp (e^\sharp)^{\alpha-1} + \cdots + x_0^{\alpha\deg(e)-\deg(a_\alpha)} a_\alpha^\sharp \in \mathcal{I}^\sharp,$$

which leads to (b). Of course (b) implies (c). If (c) holds then there exists a polynomial $q = T^\alpha + a_1 T^{\alpha-1} + \cdots + a_\alpha \in \mathbb{A}^\sharp[T]$ such that $q(e^\sharp) \in \mathcal{I}^\sharp$. By property (1.3), we can take all the a_i homogeneous of degree $i\deg(e)$, so that we obtain (a) from property (1.2). □

Proposition 1.3 does not extend nicely to generally integral dependencies. Nevertheless, we have the following weaker properties:

Proposition 1.7. *Let e_1, e_2 be in $\mathbb{K}[x_1, \ldots, x_n]$.*

(a) *If e_1 and e_2 are generally integral over $\mathbb{A}$ modulo $\mathcal{I}$, then so is always $e_1 e_2$, and so is $e_1 + e_2$ whenever $\deg(e_1 + e_2) = \max(\deg(e_1), \deg(e_2))$.*

(b) *If $\mathbb{A}$ inherits the usual graduation of $\mathbb{K}[x_1, \ldots, x_n]$, if e_1 is homogeneous and generally integral over $\mathbb{A}$ modulo $\mathcal{I}$, and if e_2 is generally integral over $\mathbb{A}[e_1]$ modulo $\mathcal{I}$, then e_2 is generally integral over $\mathbb{A}$ modulo $\mathcal{I}$.*

Proof. We start with part (a). Without loss of generality we can assume that $\deg(e_1) \geq \deg(e_2)$. We know from Lemma 1.6 that $e_1^\sharp$ and $e_2^\sharp$ are integral over $\mathbb{A}^\sharp$ modulo $\mathcal{I}^\sharp$, so are $(e_1 + e_2)^\sharp = e_1^\sharp + x_0^{\deg(e_1)-\deg(e_2)} e_2^\sharp$ and $(e_1 e_2)^\sharp = e_1^\sharp e_2^\sharp$ by Proposition 1.3(a). Part (a) thus follows from Lemma 1.6.

As for part (b), we proceed in a similar manner: $e_1^\sharp$ is integral over $\mathbb{A}^\sharp$ modulo $\mathcal{I}^\sharp$, and $e_2^\sharp$ is integral over $(\mathbb{A}[e_1])^\sharp$ modulo $\mathcal{I}^\sharp$. Thanks to the hypotheses on $\mathbb{A}$ and e_1, we obtain that $(\mathbb{A}[e_1])^\sharp = \mathbb{A}^\sharp[e_1^\sharp]$, so that Proposition 1.3(b) implies that $e_2^\sharp$ is integral over $\mathbb{A}^\sharp$ modulo $\mathcal{I}^\sharp$. Part (b) thus follows from Lemma 1.6 again. □

Example 1.8. Let $\mathbb{K} = \mathbb{Q}[\imath]$, with $\imath = \sqrt{-1}$, let $\mathcal{I} = (x_2 - x_1^2)$, $e_1 = x_2 + \imath x_1^2$, and $e_2 = -\imath x_1^2$. Of course e_2 is generally integral over $\mathbb{K}[x_1]$ modulo $\mathcal{I}$, and since $e_1^2 - 2x_1^2 e_1 + 2x_1^4 \in \mathcal{I}$ so is e_1. Because $e_1 + e_2 = x_2$ is not generally integral over $\mathbb{K}[x_1]$ modulo $\mathcal{I}$, the hypothesis $\deg(e_1 + e_2) = \max(\deg(e_1), \deg(e_2))$ is necessary in Proposition 1.7(a). In addition, since $x_2 - e_1/(1+\imath) \in \mathcal{I}$, we have that x_2 is generally integral over $\mathbb{K}[x_1, e_1]$ modulo $\mathcal{I}$, which shows that the homogeneity of e_1 is necessary in Proposition 1.7(b). Finally, from $x_1^2 - e_1/(1+\imath) \in \mathcal{I}$ we obtain that x_1 is homogeneous and generally integral over $\mathbb{K}[e_1]$ modulo $\mathcal{I}$. Since we have already seen that x_2 is generally integral over $\mathbb{K}[x_1, e_1]$ modulo $\mathcal{I}$, this shows that the graduation hypothesis on $\mathbb{A}$ is necessary in Proposition 1.7(b).

1.2. **Dimension and Noether Position.** The *transcendence degree* of a field extension $\mathbb{F}$ of $\mathbb{K}$ is classically defined as the maximal number of elements in $\mathbb{F}$ which are algebraically independent. If the transcendence degree r is finite then any maximal (with respect to the inclusion ordering) subset of elements of $\mathbb{F}$ that are algebraically independent is finite and has cardinality r (for instance, see [45, Chapter VIII, Section 1]).

Definition 1.9. If $\mathcal{I}$ is a prime ideal then the *dimension* $\dim(\mathcal{I})$ of $\mathcal{I}$ is the transcendence degree of the quotient field of $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$ over $\mathbb{K}$. In general, the dimension of $\mathcal{I} \neq (1)$ is the maximum of the dimensions of its associated primes, and, by convention, the ideal (1) has dimension -1. The ideal $\mathcal{I}$ is *unmixed* if the dimensions of its associated primes are all equal.

Remark that the dimension of $\mathcal{I}$ is preserved when performing linear changes of the coordinates. The following less classical definition will be useful for our computational purposes:

Definition 1.10. The ideal $\mathcal{I}$ is in *Noether position* if there exists $r \in \{0, \ldots, n\}$ such that the variables $x_1, \ldots, x_r$ are algebraically independent modulo $\mathcal{I}$, and such that $x_{r+1}, \ldots, x_n$ are integral over $\mathbb{K}[x_1, \ldots, x_r]$ modulo $\mathcal{I}$.

Example 1.11. The ideal $\mathcal{I} = (x_2 - x_1^2)$ is in Noether position with $r = 1$.

By Proposition 1.3, if $\mathcal{I}$ is in Noether position then any $e \in \mathbb{K}[x_1, \ldots, x_n]$ is integral over $\mathbb{K}[x_1, \ldots, x_r]$ modulo $\mathcal{I}$, so that another way to say that $\mathcal{I}$ is in Noether position is to say that $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$ is an *integral ring extension* of $\mathbb{K}[x_1, \ldots, x_r]$. When $\mathcal{I} \neq (1)$, we are to show that the integer r in Definition 1.10 coincides with the dimension of $\mathcal{I}$, hence is unique. Of course, when $\mathcal{I} = (1)$, $\mathcal{I}$ is in Noether position with $r = 0$ while $\dim(\mathcal{I}) = -1$.

Theorem 1.12. *Assume that $\mathcal{I} \neq (1)$.*

(a) *Assume that $x_{r+1}, \ldots, x_n$ are integral over $\mathbb{K}[x_1, \ldots, x_r]$ modulo $\mathcal{I}$. Then we have $\dim(\mathcal{I}) \leq r$. The latter inequality is an equality if, and only if, $x_1, \ldots, x_r$ are algebraically independent modulo $\mathcal{I}$.*

(b) *Assume that $x_1, \ldots, x_r$ are algebraically independent modulo $\mathcal{I}$. Then we have $\dim(\mathcal{I}) \geq r$. If the latter inequality is an equality then $x_{r+1}, \ldots, x_n$ are algebraic over $\mathbb{K}[x_1, \ldots, x_r]$ modulo $\mathcal{I}$. The converse holds if $\mathcal{I}$ is unmixed.*

Proof. In order to prove part (a), let us first assume that $\mathcal{I}$ is prime. Since any maximal subset of algebraically independent elements of $\{x_1, \ldots, x_r\}$ modulo $\mathcal{I}$ is also maximal in $\{x_1, \ldots, x_n\}$, part (a) follows from [45, Chapter VIII, Section 1, Theorem 1.1]. If $\mathcal{I}$ is not prime, then we can assume that $\mathcal{I}$ is radical with prime decomposition $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m$, by Proposition 1.2. Since $x_{r+1}, \ldots, x_n$ remain integral over $\mathbb{K}[x_1, \ldots, x_r]$ modulo each $\mathfrak{p}_l$, we deduce that $\dim(\mathfrak{p}_l) \leq r$ for all $l \in \{1, \ldots, m\}$, whence $\dim(\mathcal{I}) \leq r$. If $x_1, \ldots, x_r$ are algebraically dependent modulo $\mathcal{I}$ then they are also algebraically dependent modulo each $\mathfrak{p}_l$, for all $l \in \{1, \ldots, m\}$, whence $\dim(\mathcal{I}) < r$. Conversely, if $\dim(\mathcal{I}) < r$, then there exists $E_l \in \mathfrak{p}_l \cap \mathbb{K}[x_1, \ldots, x_r] \setminus \{0\}$ for all l. Therefore $E_1 \cdots E_m$ belongs to $\mathcal{I} \cap \mathbb{K}[x_1, \ldots, x_r] \setminus \{0\}$, whence the algebraically dependence of $x_1, \ldots, x_r$ over $\mathbb{K}$ modulo $\mathcal{I}$, which ends part (a).

Let us now deal with part (b). If $\mathcal{I}$ is prime then part (b) straightforwardly follows from [45, Chapter VIII, Section 1, Theorem 1.1]. If $\mathcal{I}$ is not prime then we can assume again that $\mathcal{I}$ is radical. If $x_1, \ldots, x_r$ are algebraically independent modulo $\mathcal{I}$, then there necessarily exists $l \in \{1, \ldots, m\}$ such that $x_1, \ldots, x_r$ are algebraically independent modulo $\mathfrak{p}_l$, whence $\dim(\mathcal{I}) \geq r$. If $x_{r+1}, \ldots, x_n$ are algebraic over $\mathbb{K}[x_1, \ldots, x_r]$ modulo $\mathcal{I}$, then they are also algebraic modulo $\mathfrak{p}_l$, whence $\dim(\mathcal{I}) = \dim(\mathfrak{p}_l) = r$ whenever $\mathcal{I}$ is unmixed. Conversely, assume that $\dim(\mathcal{I}) = r$ holds, and let $i \in \{r+1, \ldots, n\}$. For each $l \in \{1, \ldots, m\}$, if $x_1, \ldots, x_r$ are algebraically dependent modulo $\mathfrak{p}_l$ then we take $E_l \in \mathfrak{p}_l \cap \mathbb{K}[x_1, \ldots, x_r] \setminus \{0\}$; otherwise we take $E_l \in \mathfrak{p}_l \cap \mathbb{K}[x_1, \ldots, x_r, x_i] \setminus \{0\}$. Since $E_1 \cdots E_m \in \mathcal{I}$, it follows that x_i is algebraic over $\mathbb{K}[x_1, \ldots, x_r]$ modulo $\mathcal{I}$, which ends part (b). □

Example 1.13. If $n = 3$ and $\mathcal{I} = (x_1 x_2 - 1, x_3) \cap (x_1)$ then x_1 is algebraically independent modulo $\mathcal{I}$, and x_2, x_3 are algebraic over $\mathbb{K}[x_1]$ modulo $\mathcal{I}$. Since $\dim(\mathcal{I}) = 2$, this shows that we can not discard the unmixedness hypothesis in Theorem 1.12(b). This example also shows that Theorem 1.12(a) does not hold if $x_{r+1}, \ldots, x_n$ are only supposed to be algebraic over $\mathbb{K}[x_1, \ldots, x_r]$ modulo $\mathcal{I}$.

Example 1.14. If $n = 2$ and $\mathcal{I} = (x_1 x_2 - 1) \cap (x_1, x_2)$ then x_1 is algebraically independent modulo $\mathcal{I}$, and x_2 is algebraic over $\mathbb{K}[x_1]$ modulo $\mathcal{I}$, and $\dim(\mathcal{I}) = 1$. This shows that the unmixedness hypothesis in Theorem 1.12(b) is too strong.

It can be observed that the Noether position is preserved when extending the ground field. Therefore if $\mathcal{I}$ is in Noether position then Theorem 1.12 implies that $\dim(\mathcal{I})$ does not depend on the ground field $\mathbb{K}$.

In general the Noether position of $\mathcal{I}$ does not imply the Noether position of $\mathcal{I}^\sharp$ (consider Example 1.11). In order for $\mathcal{I}^\sharp$ to be in Noether position, we need to strengthen the preceding definition.

Definition 1.15. An ideal $\mathcal{I}$ of dimension r is in *general Noether position* if $\mathcal{I}$ is in Noether position, and if, the variables $x_{r+1}, \ldots, x_n$ are generally integral over $\mathbb{K}[x_1, \ldots, x_r]$ modulo $\mathcal{I}$.

Since $\mathbb{K}[x_1, \ldots, x_r]$ inherits the usual graduation of $\mathbb{K}[x_1, \ldots, x_n]$, Lemma 1.6 implies that the Noether and the general Noether positions coincide whenever $\mathcal{I}$ is homogeneous.

Example 1.16. The ideal $\mathcal{I} = (x_2^2 - x_1)$ is in general Noether position.

Proposition 1.17. *If $\mathcal{I}$ has dimension r and is in general Noether position then any $e \in \mathbb{K}[x_1, \ldots, x_n]$ is generally integral over $\mathbb{K}[x_1, \ldots, x_r]$ modulo $\mathcal{I}$.*

Proof. This property is a direct consequence of Proposition 1.7(a). □

Given an ideal $\mathcal{I}$ of $\mathbb{K}[x_1, \ldots, x_n]$, there is *a priori* no reason that it is in Noether position even after a permutation of the variables. For example, $\mathcal{I} = (x_1 x_2)$ is not in Noether position when seen in $\mathbb{K}[x_1, x_2]$ nor in $\mathbb{K}[x_2, x_1]$. In fact, it is well known that almost all linear changes of the variables in $\mathcal{I}$ produces a new ideal in Noether position (see for instance [45, Chapter VIII, Section 2], or [32, Chapter 3]). For example, by substituting $x_1 + x_2$ for x_1 in $\mathcal{I} = (x_1 x_2)$, we obtain the new ideal $(x_2^2 + x_1 x_2)$ which is Noether position.

For any $n \times n$ matrix M over $\mathbb{K}$, we write $\mathcal{I} \circ M$ for the ideal $\{f \circ M(x_1, \ldots, x_n)^t \mid f \in \mathcal{I}\}$. The existence of a general Noether position will follow from a repeated use of the following lemma:

Lemma 1.18. *Let $i \in \{1, \ldots, n\}$ and assume that $x_{i+1}, \ldots, x_n$ are integral (respectively, generally integral) over $\mathbb{K}[x_1, \ldots, x_i]$ modulo $\mathcal{I}$, and that $x_1, \ldots, x_i$ are algebraically dependent modulo $\mathcal{I}$. Then, for any nonzero polynomial $a \in \mathcal{I} \cap \mathbb{K}[x_1, \ldots, x_i]$, and for any point $(\alpha_1, \ldots, \alpha_{i-1}, 1) \in \mathbb{K}^i$ that does not annihilate the homogeneous component h of highest degree of a, the variables $x_i, \ldots, x_n$ are integral (respectively, generally integral) over $\mathbb{K}[x_1, \ldots, x_{i-1}]$ modulo $\mathcal{I} \circ M$, where M is defined by*

$$M(x_1, \ldots, x_n)^t = (x_1 + \alpha_1 x_i, \ldots, x_{i-1} + \alpha_{i-1} x_i, x_i, \ldots, x_n)^t.$$

In addition, we have that $\deg_{x_i}(a \circ M) = \deg(a \circ M)$.

Proof. A straightforward calculation shows that the coefficient of $x_i^{\deg(a)}$ in $a(x_1 + \alpha_1 x_i, \ldots, x_{i-1} + \alpha_{i-1} x_{i-1}, x_i)$ is $h(\alpha_1, \ldots, \alpha_{i-1}, 1)$. Therefore, if the latter quantity is nonzero then x_i is generally integral over $\mathbb{K}[x_1, \ldots, x_{i-1}]$ modulo $\mathcal{I} \circ M$. Since $x_{i+1}, \ldots, x_n$ remain integral (respectively, generally integral) over $\mathbb{K}[x_1, \ldots, x_i]$, the conclusion follows from Proposition 1.3(b) (respectively, Proposition 1.7(b)). □

Theorem 1.19. *There exists a Zariski dense subset of upper triangular $n \times n$ matrices M with 1 on their diagonal such that $\mathcal{I} \circ M$ is general Noether position.*

Proof. Let M be an upper triangular matrix with 1 on its diagonal, written in the following form:

$$M = \begin{pmatrix} 1 & \alpha_{1,2} & \ldots & \alpha_{1,n} \\ 0 & 1 & \ldots & \alpha_{2,n} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & 1 \end{pmatrix}.$$

For all $i \in \{1, \ldots, n\}$ we define the $n \times n$ matrix M_i by:

$$M_i(x_1, \ldots, x_n)^t = (x_1 + \alpha_{1,i}x_i, \ldots, x_{i-1} + \alpha_{i-1,i}x_i, x_i, \ldots, x_n)^t.$$

A straightforward calculation shows that $M = M_n \cdots M_1$. Let $r = \dim(\mathcal{I})$. Since $M_r \cdots M_1$ only affects the variables $x_1, \ldots, x_r$, we see that $\mathcal{I} \circ M$ is in general Noether position if, and only if, $\mathcal{I} \circ M_n \cdots M_{r+1}$ is in general Noether position. Therefore the theorem follows from the following stronger claim: for any $i \in \{r, \ldots, n\}$, there exists a Zariski dense subset of values for $(\alpha_{k,l} | i+1 \leq l \leq n, 1 \leq k \leq l-1)$ such that $x_{i+1}, \ldots, x_n$ are generally integral over $\mathbb{K}[x_1, \ldots, x_i]$ modulo $\mathcal{I} \circ M_n \cdots M_{i+1}$.

The proof of the claim is done by descending induction on i. If $i = n$ then the claim holds trivially. Assume that the claim is true for some $i \in \{r+1, \ldots, n\}$. Since $i \geq r+1$, Theorem 1.12(a) implies that $x_1, \ldots, x_i$ can not be algebraically independent modulo $\mathcal{I} \circ M_n \cdots M_{i+1}$. Then Lemma 1.18 asserts that there exists a Zariski dense subset of values for $(\alpha_{k,i} | 1 \leq k \leq i-1)$ for which $x_i, \ldots, x_n$ are generally integral over $\mathbb{K}[x_1, \ldots, x_{i-1}]$ modulo $\mathcal{I} \circ M_n \cdots M_i$, which completes the proof of the claim. □

Corollary 1.20. *Theorem 1.19 holds if we replace the space of the upper triangular matrices with* 1 *on their diagonal by the whole space of the invertible matrices.*

Proof. The set of matrices M such that all their principal minors are nonzero is dense. It is classical that such a matrix M can be uniquely written as the product of a lower triangular matrix L by an upper triangular matrix U with 1 on its diagonal [38, Section 3.5]. Since $\mathcal{I} \circ L$ is in general Noether position if, and only if, $\mathcal{I}$ is itself in general Noether position, the conclusion follows from Theorem 1.19. □

From the existence of general Noether positions, we can now deduce:

Corollary 1.21. *If* $\mathcal{I} \neq (1)$ *then* $\dim(\mathcal{I}^\sharp) = \dim(\mathcal{I}) + 1$.

Proof. Thanks to Theorem 1.19, we can assume that $\mathcal{I}$ is in general Noether position. Therefore the conclusion follows from Lemmas 1.4 and 1.6, and Theorem 1.12(a). □

1.3. **Unmixedness and Torsion.** From now on, we assume that $\mathcal{I} \neq (1)$, and we write $r \geq 0$ for the dimension of $\mathcal{I}$. In addition we will use the following notation:

$$\mathbb{A} = \mathbb{K}[x_1, \ldots, x_r], \quad \mathbb{B} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I},$$
$$\mathbb{A}' = \mathbb{K}(x_1, \ldots, x_r), \quad \mathbb{B}' = \mathbb{A}'[x_{r+1}, \ldots, x_n]/\mathcal{I}',$$

where $\mathcal{I}'$ denotes the extension of $\mathcal{I}$ to $\mathbb{A}'[x_{r+1}, \ldots, x_n]$. The ring $\mathbb{B}$ can naturally be seen as an $\mathbb{A}$-module. The following proposition gives us a useful criterion for testing the unmixedness of $\mathcal{I}$:

Proposition 1.22. *Assume that* $\mathcal{I}$ *is in Noether position. Then* $\mathbb{B}$ *is a torsion-free* $\mathbb{A}$*-module if, and only if,* $\mathcal{I}$ *is unmixed.*

Proof. Let $\mathcal{Q}_1 \cap \cdots \cap \mathcal{Q}_s$ represent a reduced primary decomposition of $\mathcal{I}$. Here we follow the terminology of [45, Chapter X]: "reduced" means that the associated primes $\mathcal{P}_1, \ldots, \mathcal{P}_s$ belonging to $\mathcal{Q}_1, \ldots, \mathcal{Q}_s$ respectively are distinct, and that $\mathcal{I}$ can not be expressed as an intersection of a proper subset of $\{\mathcal{Q}_1, \ldots, \mathcal{Q}_s\}$. By Theorem 1.12(a), the ideal $\mathcal{I}$ is unmixed if, and only if, $\mathbb{A} \cap \mathcal{P}_l = (0)$, for all $l \in \{1, \ldots, s\}$. On the other hand, the fact that $\mathbb{B}$ has torsion reformulates into the following property: there exist $a \in \mathbb{A} \setminus \{0\}$ and $b \notin \mathcal{I}$ such that $ab \in \mathcal{I}$. If $\mathbb{B}$ has torsion then there exist $a \in \mathbb{A} \setminus \{0\}$, $l \in \{1, \ldots, s\}$, and b such that $ab \in \mathcal{Q}_l$ and $b \notin \mathcal{Q}_l$. Therefore we must have $a \in \mathcal{P}_l$, hence $\mathcal{I}$ is not unmixed. Conversely, if $\mathcal{I}$ is not unmixed then there exists $a \in (\mathbb{A} \cap \mathcal{P}_l) \setminus \{0\}$ for some l, hence some power of a is a torsion element for $\mathbb{B}$. □

Example 1.23. If $\mathcal{I} = (x_1x_2) \subseteq \mathbb{K}[x_1, x_2]$ then $\mathcal{I}$ is unmixed of dimension 1 but $\mathbb{B}$ has torsion. This example shows that the Noether position is necessary in Proposition 1.22.

Corollary 1.24. *If $\mathcal{I}$ is radical, then $\mathcal{I}'$ is radical. The converse holds if $\mathcal{I}$ is unmixed.*

Proof. The proof is straightforward from Proposition 1.22. □

Example 1.25. If $\mathcal{I} = (x_2) \cap (x_1, x_2)^2$, then $\mathcal{I}' = (x_2)$ but $\mathcal{I}$ is not radical. This example shows that the unmixedness of $\mathcal{I}$ is in general necessary in Corollary 1.24.

Corollary 1.26. *Assume that $\mathcal{I}$ is unmixed, and let g in $\mathbb{K}[x_1, \ldots, x_n]$ be such that $\mathcal{I} : g^\infty \neq (1)$. Then $\mathcal{I} : g^\infty$ is unmixed of dimension r. If $\mathcal{I}$ is in Noether position or in general Noether position then so is $\mathcal{I} : g^\infty$.*

Proof. Without loss of generality we can assume that $\mathcal{I}$ is in Noether position (respectively, general Noether position), by Theorem 1.19. From Proposition 1.22 we know that $\mathbb{B}$ is a torsion-free $\mathbb{A}$-module. Therefore the assumption $\mathcal{I} : g^\infty \neq (1)$ implies that $x_1, \ldots, x_r$ are algebraically independent modulo $\mathcal{I} : g^\infty$. On the other hand, the inclusion $\mathcal{I} \subseteq \mathcal{I} : g^\infty$ gives us that $x_{r+1}, \ldots, x_n$ are integral (respectively, generally integral) over $\mathbb{A}$ modulo $\mathcal{I} : g^\infty$. It follows that $\mathcal{I} : g^\infty$ inherits the Noether position of $\mathcal{I}$ (respectively, general Noether position), whence $\dim(\mathcal{I} : g^\infty) = r$ by Theorem 1.12(a). Finally, the torsion-freeness of $\mathbb{B}$ implies the one of $\mathbb{K}[x_1, \ldots, x_n]/(\mathcal{I} : g^\infty)$, and Proposition 1.22 completes the proof. □

If $\mathcal{I}$ is generated by a regular sequence, then it is known (see [18, Corollary 18.17] for example) that $\mathbb{B}$ is a locally free $\mathbb{A}$-module of finite rank and hence free by the Quillen-Suslin theorem [45, Chapter XXI, Theorem 3.5]. In this situation, one can naturally speak about the characteristic and minimal polynomials of the endomorphism of multiplication by any f in $\mathbb{B}$. In the following subsection we study polynomials with similar properties under the only hypothesis that $\mathbb{B}$ is torsion-free.

1.4. **Characteristic and Minimal Polynomials.** If $\mathcal{I}$ is in Noether position then $\mathbb{B}'$ is a $\mathbb{A}'$-vector space of finite dimension, so that, for any f in $\mathbb{K}[x_1, \ldots, x_n]$, we can define $\chi \in \mathbb{A}'[T]$ (respectively, μ) as the characteristic (respectively, minimal) polynomial of the endomorphism of multiplication by f in $\mathbb{B}'$. In short, we will respectively call them the *characteristic* and the *minimal* polynomials of f modulo $\mathcal{I}$.

Theorem 1.27. *Assume that $\mathcal{I}$ is in Noether position, and let $d = \deg(f)$.*

(a) *χ and μ belong to $\mathbb{A}[T]$. In addition, if $\mathcal{I}$ and f are homogeneous, then $\chi(T^d)$ and $\mu(T^d)$ are homogeneous when seen in $\mathbb{K}[x_1, \ldots, x_r, T]$.*
(b) *If the Noether position is general then the total degrees of $\chi(T^d)$ and $\mu(T^d)$ seen in $\mathbb{K}[x_1, \ldots, x_r, T]$ equal their respective partial degree in T.*
(c) *If $\mathcal{I}$ is unmixed then $\chi(f)$ and $\mu(f)$ belong to $\mathcal{I}$.*

Proof. Since f is integral over $\mathbb{A}$ modulo $\mathcal{I}$, there exists a polynomial $q \in \mathbb{A}[T]$ such that $q(f) \in \mathcal{I}$. Since $q(f) = 0$ holds in $\mathbb{B}'$, the minimal polynomial μ divides q in $\mathbb{A}'[T]$. In particular, all the irreducible factors of μ divide q. Since q and these factors are monic in T, the classical Gauss lemma [45, Chapter IV, Theorem 2.1] implies that all these factors actually belong to $\mathbb{A}[T]$, so do μ and χ. If $\mathcal{I}$ and f are homogeneous then q can be chosen so that $q(T^d)$ is homogeneous. Therefore all the irreducible factors of $\mu(T^d)$ are homogeneous, which concludes part (a).

If the Noether position is general then Proposition 1.17 implies that f is generally integral over $\mathbb{A}$ modulo $\mathcal{I}$. We can thus take q such that equality (1.1) holds. This

equality between the degrees hold for any irreducible factor of q, hence for μ and χ, which concludes part (b).

Since $\mu(f) \in \mathcal{I}'$, there exist $a \in \mathbb{A} \setminus \{0\}$ and $b \in \mathcal{I}$ such that $\mu(f) = b/a$. Thus we have $a\mu(f) = 0$ in $\mathbb{B}$. By Proposition 1.22, $\mathbb{B}$ is torsion-free, whence $\mu(f) \in \mathcal{I}$. The same proof holds for χ, which concludes part (c). □

Example 1.28. With $\mathcal{I} = (x_2^2, x_1x_2)$ and $f = x_2 + 1$, we have $\mathcal{I}' = (x_2)$ and $\mu = T - 1$ but $\mu(f) = x_2 \notin \mathcal{I}$. Therefore it is necessary to assume that $\mathcal{I}$ is unmixed in Theorem 1.27(c).

Example 1.29. Theorem 1.27(b) does not hold if the Noether position is not general as exemplified by taking $\mathcal{I} = (x_2 - x_1^2)$ and $f = x_2$ so that $\mu = T - x_1^2$.

2. Incremental Approach to Solving

In this section we carry on with the notation introduced at the beginning of Section 1.3. We describe the devices to compute a Noether position when adding a new polynomial f to the ideal $\mathcal{I} \neq (1)$, and we give a proof of the well known principal ideal theorem. Then, we present a formula to compute a characteristic polynomial modulo $\mathcal{I} + (f)$, that is the cornerstone of the Kronecker solver, but that is also a main ingredient in the definition of the degree of an ideal, and in the proof of a Bézout theorem.

2.1. Incremental Noether Position.

If $\mathcal{I}$ is in Noether position then, for a given $f \in \mathbb{K}[x_1, \ldots, x_n]$, we are going to show how to change the variables so that $\mathcal{I}$ and $\mathcal{I} + (f)$ become in Noether position. We start with a lemma that relates the first properties of $\mathcal{I} + (f)$ to the constant coefficients χ_0 and μ_0 of χ and μ respectively.

Lemma 2.1. *Assume that $\mathcal{I}$ is unmixed and in Noether position.*

(a) *μ_0 and χ_0 belong to $\mathcal{I} + (f)$, and $(\mathcal{I} + (f)) \cap \mathbb{A} \subseteq \sqrt{(\mu_0)} = \sqrt{(\chi_0)}$.*
(b) *f is a zerodivisor in $\mathbb{B}$ if, and only if, $\chi_0 = 0$ (or equivalently, $\mu_0 = 0$), if, and only if, $x_1, \ldots, x_r$ are algebraically independent modulo $\mathcal{I} + (f)$.*
(c) *$\mathcal{I} + (f) = (1)$ if, and only if, $\chi_0 \in \mathbb{K} \setminus \{0\}$ (or equivalently, $\mu_0 \in \mathbb{K} \setminus \{0\}$).*

Proof. From Theorem 1.27(c), we have that $\mu(f) \in \mathcal{I}$ and $\chi(f) \in \mathcal{I}$, whence $\mu_0 \in \mathcal{I} + (f)$ and $\chi_0 \in \mathcal{I} + (f)$. Let a be a polynomial in $(\mathcal{I} + (f)) \cap \mathbb{A}$, and let $g \in \mathbb{K}[x_1, \ldots, x_n]$ be such that $a - gf \in \mathcal{I}$. Since g in integral over $\mathbb{A}$ modulo $\mathcal{I}$, there exist $\nu_0, \ldots, \nu_{\alpha-1}$ in $\mathbb{A}$ such that $g^\alpha + \nu_{\alpha-1}g^{\alpha-1} + \cdots + \nu_0 \in \mathcal{I}$. By multiplying the latter expression by f^α, we obtain that $a^\alpha + \nu_{\alpha-1}a^{\alpha-1}f + \cdots + \nu_0 f^\alpha \in \mathcal{I}$. We deduce that μ divides $\rho = a^\alpha + \nu_{\alpha-1}a^{\alpha-1}T + \cdots + \nu_0 T^\alpha$ in $\mathbb{A}'[T]$. Since μ is monic, this division holds in $\mathbb{A}[T]$, and therefore a^α is a multiple of μ_0, which concludes part (a).

If $\mu_0 = 0$ then we have $\nu(f)f = 0$ in $\mathbb{B}$, with $\nu(T) = \mu(T)/T$. Since $\deg(\nu) < \deg(\mu)$ we obtain that $\nu(f) \notin \mathcal{I}$, whence f is a zerodivisor. Conversely, if f is a zerodivisor then there exists $g \notin \mathcal{I}$ such that $fg \in \mathcal{I}$. Therefore there exists a primary component $\mathcal{Q}$ of $\mathcal{I}$ such that $g \notin \mathcal{Q}$ and $fg \in \mathcal{Q}$. It follows that f belongs to $\sqrt{\mathcal{Q}}$, and that $\mu_0 \in \mathcal{I} + (f) \subseteq \sqrt{\mathcal{Q}}$. Since $\mathcal{I}$ is unmixed, $\sqrt{\mathcal{Q}}$ has dimension r, which implies that $\mu_0 = 0$ thanks to Theorem 1.12(a). By part (a), $\mu_0 = 0$ if, and only if, $x_1, \ldots, x_r$ are algebraically independent modulo $\mathcal{I} + (f)$, which concludes part (b). Finally part (c) straightforwardly follows from part (a). □

This lemma already gives us the following property: if f is a zerodivisor in $\mathbb{B}$, then $x_1, \ldots, x_r$ are algebraically independent modulo $\mathcal{I} + (f)$, and thus $\mathcal{I} + (f)$ is in Noether position (the general position is also preserved). If f is a nonzerodivisor in $\mathbb{B}$, then we can compute a Noether position for $\mathcal{I} + (f)$ as follows:

Proposition 2.2. *Assume that $\mathcal{I}$ is unmixed.*

(a) *If f is a zerodivisor in $\mathbb{B}$ then* $\dim(\mathcal{I}+(f)) = r$. *In addition, if $\mathcal{I}$ is in Noether position or in general Noether position then so is $\mathcal{I}+(f)$.*

(b) *If f is a nonzerodivisor in $\mathbb{B}$ then* $\dim(\mathcal{I}+(f))$ *equals* -1 *or* $r-1$. *In addition, if $\mathcal{I}$ is in Noether position (respectively, general Noether position), then for any $(\alpha_1,\ldots,\alpha_{r-1},1) \in \mathbb{K}^r$ that does not annihilate the homogeneous component h of highest degree of μ_0, the ideals $\mathcal{I}\circ M$ and $(\mathcal{I}+(f))\circ M$ are in Noether position (respectively, general Noether position), and $deg_{x_r}(\mu_0 \circ M) = \deg(\mu_0 \circ M)$, where M is the matrix defined by*

$$M(x_1,\ldots,x_n)^t = (x_1+\alpha_1 x_r,\ldots,x_{r-1}+\alpha_{r-1}x_r, x_r,\ldots,x_n)^t.$$

Proof. As previously discussed, part (a) is a consequence of Lemma 2.1(b) and Theorem 1.12(a).

If $\mu_0 \in \mathbb{K}\setminus\{0\}$ then part (b) trivially holds by Lemma 2.1(c). Otherwise, if $\mu_0 \notin \mathbb{K}$ then we use Lemma 1.18 with $\mathcal{I}+(f)$, $i=r$ and μ_0: we obtain that $x_r,\ldots,x_n$ are generally integral over $\mathbb{K}[x_1,\ldots,x_{r-1}]$ modulo $(\mathcal{I}+(f))\circ M$. In order to complete the proof it remains to prove that $x_1,\ldots,x_{r-1}$ are algebraically independent modulo $(\mathcal{I}+(f))\circ M$. To this aim, let $a \in \mathbb{K}[x_1,\ldots,x_{r-1}]\cap(\mathcal{I}+(f))\circ M$. By Lemma 2.1(a), $\mu_0\circ M$ divides a power of a. But since Lemma 1.18 tells us that $\deg_{x_r}(\mu_0\circ M) = \deg(\mu_0\circ M) > 0$, we deduce that $a=0$, which finishes the proof of part (b). □

2.2. **Incremental Unmixedness of the Radical.** The proof of the following version of the classical principal ideal theorem is adapted from [64, Chapter I, Section 6.2]. Recall that we assume that $\mathcal{I} \neq (1)$ from Section 1.3.

Theorem 2.3. *Assume that $\mathcal{I}$ is unmixed, and let $f \in \mathbb{K}[x_1,\ldots,x_n]$ be a nonzerodivisor in $\mathbb{B}$. If $\mathcal{I}+(f) \neq (1)$ then $\sqrt{\mathcal{I}+(f)}$ is unmixed of dimension $r-1$.*

Proof. Thanks to Theorem 1.19, Proposition 2.2(b), and Lemma 2.1(c), we can assume that $r \geq 1$, $\dim(\mathcal{I}+(f)) = r-1$, $\mathcal{I}$ and $\mathcal{I}+(f)$ are in general Noether position, and that $\deg_{x_r}(\mu_0) = \deg(\mu_0) \geq 1$. Let us first prove the theorem when $\mathcal{I}$ and f are homogeneous.

Let $E \in \mathbb{K}[x_1,\ldots,x_{r-1},T]$ be such that $E(x_1,\ldots,x_{r-1},f) \in \mathcal{I}$. Since $\mu(T)$ divides $E(x_1,\ldots,x_{r-1},T)$, it follows that μ_0 divides $E(x_1,\ldots,x_{r-1},0)$. Therefore the inequality $\deg_{x_r}(\mu_0) > 0$ implies that $E(x_1,\ldots,x_{r-1},0) = 0$. Since f is a nonzerodivisor in $\mathbb{B}$, we deduce that $E=0$. In other words $x_1,\ldots,x_{r-1},f$ are algebraically independent modulo $\mathcal{I}$. Since $\deg_{x_r}(\mu_0) = \deg(\mu_0)$, Theorem 1.27(a) implies that x_r is integral over $\mathbb{K}[x_1,\ldots,x_{r-1},f]$ modulo $\mathcal{I}$. Thanks to Proposition 1.3(b) we obtain that $x_{r+1},\ldots,x_n$ are integral over $\mathbb{K}[x_1,\ldots,x_{r-1},f]$ modulo $\mathcal{I}$. This way we have shown that $\mathbb{B}$ is an integral ring extension of $\mathbb{K}[x_1,\ldots,x_{r-1},f]$.

Thanks to Proposition 1.22, in order to prove that $\sqrt{\mathcal{I}+(f)}$ is unmixed, it is sufficient to prove that $\mathbb{K}[x_1,\ldots,x_n]/\sqrt{\mathcal{I}+(f)}$ is torsion-free when seen as a $\mathbb{K}[x_1,\ldots,x_{r-1}]$-module. With this aim in view, let $b \in \mathbb{K}[x_1,\ldots,x_n]$ and $a \in \mathbb{K}[x_1,\ldots,x_{r-1}]\setminus\{0\}$ be such that $ab \in \sqrt{\mathcal{I}+(f)}$. We claim that a power of b belongs to $\mathcal{I}+(f)$.

Let $m \in \mathbb{N}$ and $g \in \mathbb{K}[x_1,\ldots,x_n]$ be such that $a^m b^m - fg \in \mathcal{I}$. In order to prove the latter claim, we consider $\mathbb{B}$ as a $\mathbb{K}[x_1,\ldots,x_{r-1},f]$-module $\mathbb{B}_f$, and we denote by $\mathbb{B}'_f$ the corresponding finitely dimensional $\mathbb{K}(x_1,\ldots,x_{r-1},f)$-vector space. By the classical Gauss lemma [45, Chapter IV, Theorem 2.1], the minimal polynomials of g and b^m in $\mathbb{B}'_f$ belong to $\mathbb{K}[x_1,\ldots,x_{r-1},f][T]$. Let $\rho(T) = T^\alpha + \rho_{\alpha-1}T^{\alpha-1}+\cdots+\rho_0$ denote the minimal polynomial of g in $\mathbb{B}'_f$. Then the minimal polynomial of b^m in

$\mathbb{B}'_f$ is

$$f^\alpha \rho(a^m T/f)/a^{m\alpha} = T^\alpha + \rho_{\alpha-1}\left(\frac{f}{a^m}\right) T^{\alpha-1} + \cdots + \left(\frac{f}{a^m}\right)^\alpha \rho_0.$$

We deduce that $(a^m)^j$ divides $f^j \rho_{\alpha-j}$ in $\mathbb{K}[x_1, \ldots, x_{r-1}, f]$, for all $j \in \{0, \ldots, \alpha-1\}$. Since $x_1, \ldots, x_{r-1}, f$ are algebraically independent, and since $a \in \mathbb{K}[x_1, \ldots, x_{r-1}]$, we obtain that $(a^m)^j$ divides $\rho_{\alpha-j}$, whence $(b^m)^\alpha \in \mathcal{I} + (f)$, which concludes the proof in the homogeneous situation.

In the general situation, for any isolated prime $\mathfrak{p}$ of $\mathcal{I} + (f)$, it can be verified that $\mathfrak{p}^\sharp$ is an isolated prime of $\mathcal{I}^\sharp + (f^\sharp)$. It follows that $\dim(\mathfrak{p}^\sharp) = r$, hence that $\dim(\mathfrak{p}) = r - 1$, by Corollary 1.21. □

Example 2.4. Let $\mathcal{I} = (x_1, x_2) \cap (x_3, x_4)$. The ideal $\mathcal{I}$ is unmixed. If we take the nonzerodivisor $f = x_2 - x_3$, then $\sqrt{\mathcal{I} + (f)} = (x_1, x_2, x_3) \cap (x_2, x_3, x_4)$ is unmixed while $\mathcal{I} + (f) = (x_1, x_2, x_3) \cap (x_2, x_3, x_4) \cap (x_1, x_2 - x_3, x_3^2, x_4)$ is not.

Corollary 2.5. *Assume that $\mathcal{I}$ is unmixed and in Noether position (respectively, general Noether position), let $s \in \{0, \ldots, r\}$. Then $\sqrt{\mathcal{I} + (x_{s+1}, \ldots, x_r)}$ is in Noether position (respectively, general Noether position) and unmixed of dimension s.*

Proof. Since the minimal polynomial of $f = x_r$ modulo $\mathcal{I}$ is $\mu = T - x_r$, Lemma 2.1 implies that x_r is a nonzerodivisor in $\mathbb{B}$, and that $\mathcal{I} + (x_r) \neq (1)$. Theorem 2.3 thus ensures that $\sqrt{\mathcal{I} + (x_r)}$ is unmixed of dimension $r - 1$. Then we obtain that $\sqrt{\mathcal{I} + (x_r)}$ in Noether position (respectively, general Noether position) from Theorem 1.12(a). Finally, since

$$\sqrt{\sqrt{\mathcal{I} + (x_{s+1}, \ldots, x_r)} + (x_s)} = \sqrt{\mathcal{I} + (x_s, \ldots, x_r)}, \tag{2.1}$$

a straightforward induction completes the proof. □

Corollary 2.6. *Assume that $\mathcal{I}$ is unmixed and in Noether position (respectively, general Noether position), and let $f \in \mathbb{K}[x_1, \ldots, x_n]$.*

(a) *If χ_0 does not vanish at $x_1 = \cdots = x_r = 0$, then f is a nonzerodivisor in $\mathbb{K}[x_1, \ldots, x_n]/(\mathcal{I} + (x_1, \ldots, x_r))$.*
(b) *If f is a nonzerodivisor in $\mathbb{B}$ then the set of points $(\beta_1, \ldots, \beta_r) \in \mathbb{K}^r$ such that f is a nonzerodivisor in $\mathbb{K}[x_1, \ldots, x_n]/(\mathcal{I} + (x_1 - \beta_1, \ldots, x_r - \beta_r))$ is Zariski dense.*

Proof. Let ψ denote the specialization of χ at $x_1 = \cdots = x_r = 0$, and let $\mathcal{J} = \mathcal{I} + (x_1, \ldots, x_r)$. By Corollary 2.5, $\mathcal{J}$ has dimension 0, and thus is unmixed. From Theorem 1.27 we have that $\chi(f) \in \mathcal{I}$, whence $\psi(f) \in \mathcal{J}$. Therefore the constant coefficient of the minimal polynomial of f in $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{J}$ can not be zero, and thus Lemma 2.1(b) implies that f is a nonzerodivisor in $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{J}$. This concludes the proof of part (a). If f is a nonzerodivisor in $\mathbb{B}$ then Lemma 2.1(b) implies that $\chi_0 \neq 0$, which immediately yields part (b). □

2.3. **Incremental Computation of the Characteristic Polynomial.** We next present the key formula to compute the characteristic polynomial of x_r modulo $\mathcal{I} + (f)$.

Proposition 2.7. *Assume that $\mathcal{I}$ has dimension $r \geq 1$, is unmixed, and is in Noether position. Let f be a nonzerodivisor in $\mathbb{B}$. Then $\chi_0(x_1, \ldots, x_{r-1}, T)$ is proportional over $\mathbb{K}(x_1, \ldots, x_{r-1})$ to the characteristic polynomial of x_r modulo the extension $\mathcal{J}'$ of $\mathcal{J} = \mathcal{I} + (f)$ to $\mathbb{K}(x_1, \ldots, x_{r-1})[x_r, \ldots, x_n]$. The proportionality over $\mathbb{K}$ holds if, and only if, $\mathcal{J}$ is in Noether position.*

Proof. Let $\tilde{\mathcal{I}}$ denote the extension of $\mathcal{I}$ to $\mathbb{K}(x_1,\ldots,x_{r-1})[x_r,x_{r+1},\ldots,x_n]$, and let $\tilde{\mathbb{B}} = \mathbb{K}(x_1,\ldots,x_{r-1})[x_r,x_{r+1},\ldots,x_n]/\tilde{\mathcal{I}}$. By Proposition 1.22, $\mathbb{B}$ is a torsion-free $\mathbb{A}$-module, so is $\tilde{\mathbb{B}}$ seen as a $\mathbb{K}(x_1,\ldots,x_{r-1})[x_r]$-module. From [45, Chapter III, Theorem 7.3], it follows that $\tilde{\mathbb{B}}$ is free, and, thanks to the Noether position of $\mathcal{I}$, that $\tilde{\mathbb{B}}$ has finite rank. Therefore, by [45, Chapter III, Theorem 7.9], there exist two bases $e_1,\ldots,e_\delta$ and $e'_1,\ldots,e'_\delta$ of $\tilde{\mathbb{B}}$, and some monic polynomials $h_1,\ldots,h_\delta \in \mathbb{K}(x_1,\ldots,x_{r-1})[x_r]$ such that h_l divides h_{l+1} for all $l \in \{1,\ldots,\delta-1\}$, and such that $fe_l = h_l e'_l$ in $\tilde{\mathbb{B}}$ for all $l \in \{1,\ldots,\delta\}$.

On the one hand, since a basis of $\tilde{\mathbb{B}}$ induces a basis of $\mathbb{B}'$, we obtain that $\chi_0 = ah_1\cdots h_\delta$, for some $a \in \mathbb{K}(x_1,\ldots,x_{r-1})$. On the other hand, we claim that the set $\mathcal{B} = \{x_r^{\alpha_l} e'_l \mid 1 \le l \le \delta,\ 0 \le \alpha_l \le \deg(h_l)-1\}$ is a basis of $\tilde{\mathbb{B}}/(f)$ seen as a $\mathbb{K}(x_1,\ldots,x_{r-1})$-algebra. Let us first verify that $\mathcal{B}$ actually generates $\tilde{\mathbb{B}}/(f)$. Let $g \in \tilde{\mathbb{B}}/(f)$. Any antecedant $\tilde{g}$ of g in $\tilde{\mathbb{B}}$ can be written $g = \sum_{l=1}^{\delta} g_l e'_l$, with $g_1,\ldots,g_\delta \in \mathbb{K}(x_1,\ldots,x_{r-1})[x_r]$. Since, by construction, the ideal generated by f in $\tilde{\mathbb{B}}$ equals $(h_1e'_1,\ldots,h_\delta e'_\delta)$, we can write $g = \sum_{l=1}^{\delta} r_l e'_l$ in $\tilde{\mathbb{B}}/(f)$, where each r_l denotes the remainder in the division of g_l by h_l. Secondly, let us verify that $\mathcal{B}$ is free. Let $r_1,\ldots,r_\delta \in \mathbb{K}(x_1,\ldots,x_{r-1})[x_r]$ be such that $\deg(r_l) < \deg(h_l)$ and $\sum_{l=1}^{\delta} r_l e'_l = 0$ in $\tilde{\mathbb{B}}/(f)$. Then there exist some polynomials $q_1,\ldots,q_\delta \in \mathbb{K}(x_1,\ldots,x_{r-1})[x_r]$ such that $\sum_{l=1}^{\delta} r_l e'_l + \sum_{l=1}^{\delta} q_l h_l e'_l = 0$ in $\tilde{\mathbb{B}}$. Therefore, for all l we obtain $r_l + q_l h_l = 0$, whence $q_l = r_l = 0$ since $\deg(h_l) > \deg(r_l)$.

In the basis $\mathcal{B}$, the matrix of multiplication by x_r in $\tilde{\mathbb{B}}/(f)$ is a diagonal block matrix, whose blocks are the companion matrices of the h_l. Therefore the characteristic polynomial q of x_r in $\tilde{\mathbb{B}}/(f)$ equals $h_1\cdots h_\delta$. We thus obtain that χ_0 is proportional to q over $\mathbb{K}(x_1,\ldots,x_{r-1})$.

Let us now deal with the last assertion of the proposition. If $\mathcal{J} = (1)$ then it trivially holds thanks to Lemma 2.1(c). Let us now assume that $\mathcal{J} \neq (1)$. Theorem 2.3 gives us that $\dim(\mathcal{J}) = r-1$. Therefore if $\mathcal{J}$ is in Noether position then there exists a monic polynomial $p \in \mathbb{K}[x_1,\ldots,x_{r-1}][T]$ such that $p(x_r) \in \mathcal{J}$. Since Lemma 2.1(a) implies that χ_0 divides a power of $p(x_r)$, we deduce that the leading coefficients of χ_0 seen in $\mathbb{K}[x_1,\ldots,x_{r-1}][x_r]$ belongs to $\mathbb{K}$, and thus that χ_0 is proportional over $\mathbb{K}$ to $q(x_r)$. Conversely, if χ_0 is proportional over $\mathbb{K}$ to $q(x_r)$, then x_r is integral over $\mathbb{K}[x_1,\ldots,x_{r-1}]$ modulo $\mathcal{J}$ by Lemma 2.1(a). We thus obtain that $\mathcal{J}$ is in Noether position by Proposition 1.3(b) and Theorem 1.12(a). □

Example 2.8. The basis $\mathcal{B}$ in the proof of Proposition 2.7 is built from the isomorphism between the $\mathbb{K}(x_1,\ldots,x_{r-1})[x_r]$-modules $\tilde{\mathbb{B}}/(f)$ and

$$\bigoplus_{l=1}^{\delta} \mathbb{K}(x_1,\ldots,x_{r-1})[x_r]/(h_l).$$

In general this direct sum can not be read as a decomposition of $\tilde{\mathbb{B}}/(f)$ into stable $\mathbb{K}(x_1,\ldots,x_{r-1})$-algebras. This can be seen by taking $n=2$, $\mathcal{I} = (x_2^2 + x_1x_2)$, $r=1$, and $f = x_1^2$. Then $\{1,x_2\}$ forms a basis of the $\mathbb{K}[x_1]$-module $\tilde{\mathbb{B}} = \mathbb{K}[x_1,x_2]/\tilde{\mathcal{I}}$, in which the matrix of multiplication by f is the diagonal matrix with $h_1 = x_1^2$ and $h_2 = x_1^2$ on its diagonal. As $\mathbb{K}[x_1]$-modules we thus have $\tilde{\mathbb{B}}/(f) = \mathbb{K}[x_1]/(h_1) \bigoplus \mathbb{K}[x_1]/(h_2)x_2$. These two submodules are stable by multiplication by x_1 but $\mathbb{K}[x_1]/(h_1)$ is not stable by multiplication by x_2.

2.4. **Degree and Bézout's Theorem.** In this last subsection we prove the necessary results in the degree theory that are needed in the cost analysis of the Kronecker solver. We will not reproduce this analysis in this paper, and refer the reader to [30]. The materials presented in this subsection are not used in the proof

of the correctness of the solver; we shall only use them in Section 4 when discussing about complexity.

Let M denote an invertible $n \times n$ matrix over $\mathbb{K}$. In short, we write $\mathcal{I}_M = \mathcal{I} \circ M$, $\mathbb{B}_M = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}_M$, $\mathbb{B}'_M = \mathbb{A}'[x_{r+1}, \ldots, x_n]/\mathcal{I}'_M$, where $\mathcal{I}'_M$ denotes the extension of $\mathcal{I}_M$ to $\mathbb{A}'[x_{r+1}, \ldots, x_n]$. We write δ (respectively, δ_M) for the dimension of $\mathbb{B}'$ (respectively, $\mathbb{B}'_M$) seen as a $\mathbb{A}'$-vector space. Proposition 2.7 is a central ingredient to prove the next theorem that asserts that if $\mathcal{I}$ and $\mathcal{I}_M$ are both in general Noether position then $\delta = \delta_M$.

Theorem 2.9. *Assume that $\mathcal{I}$ is unmixed and in general Noether position.*

(a) $\delta_M \leq \delta$.
(b) $\delta_M = \delta$ *if, and only if, $\mathcal{I}_M$ is in general Noether position.*

Proof. The proof is postponed in Appendix A. □

Theorem 2.9 ensures that the following definition of the degree of $\mathcal{I}$ actually makes sense.

Definition 2.10. The *degree* of an unmixed ideal $\mathcal{I}$, written $\deg(\mathcal{I})$, is the dimension of $\mathbb{B}'_M$ seen as an $\mathbb{A}'$-vector space, for any matrix M such that $\mathcal{I} \circ M$ is in general Noether position.

Remark that $\deg((0)) = 1$, and that $\deg(\mathcal{I}) = 0$ if, and only if, $\mathcal{I} = (1)$.

Proposition 2.11. *Assume that $\mathcal{I}$ is unmixed.*

(a) $\deg(\sqrt{\mathcal{I}}) \leq \deg(\mathcal{I})$*; the inequality is an equality if, and only if, $\mathcal{I}$ is radical.*
(b) $\deg(\mathcal{I} : g^\infty) \leq \deg(\mathcal{I})$*, for any polynomial g; the inequality is an equality if, and only if, g is a nonzerodivisor in $\mathbb{B}$.*

Proof. By Theorem 1.19, we can assume that $\mathcal{I}$ is in general Noether position. The inequality of part (a) trivially follows from the inclusion of $\mathcal{I}'$ in the extension of $\sqrt{\mathcal{I}}$ to $\mathbb{A}'[x_{r+1}, \ldots, x_n]$. If the equality holds in part (a) then this extension of $\sqrt{\mathcal{I}}$ coincides with $\mathcal{I}'$. Therefore $\mathcal{I}'$ is radical, and so is $\mathcal{I}$ by Corollary 1.24. We are done with part (a).

If $\mathcal{I} : g^\infty = (1)$ then part (b) trivially holds. Otherwise Corollary 1.26 tells us that $\mathcal{I} : g^\infty$ is unmixed of dimension r and in general Noether position. On the other hand the extension of $\mathcal{I} : g^\infty$ to $\mathbb{A}'[x_{r+1}, \ldots, x_n]$ coincides with $\mathcal{I}' : g^\infty$. Therefore we obtain that $\deg(\mathcal{I} : g^\infty) \leq \deg(\mathcal{I})$. If g is a nonzerodivisor in $\mathbb{B}$, then $\mathcal{I} = \mathcal{I} : g^\infty$, whence $\deg(\mathcal{I} : g^\infty) = \deg(\mathcal{I})$. Conversely, if the latter equality holds then $\mathcal{I}' : g^\infty = \mathcal{I}'$, whence $\mathcal{I} : g^\infty = \mathcal{I}$ by Proposition 1.22. □

Proposition 2.7 is also the core of the following version of the Bézout theorem:

Theorem 2.12. *Assume that $\mathcal{I}$ is unmixed. Let f be a nonzerodivisor in $\mathbb{B}$, and let $\tilde{\mathcal{J}}$ denote the intersection of the primary components $\mathcal{Q}$ of $\mathcal{J} = \mathcal{I} + (f)$ belonging to an isolated associated prime $\mathfrak{p}$. Then we have that $\deg(\tilde{\mathcal{J}}) \leq \deg(\mathcal{I}) \deg(f)$. In addition, if $\mathcal{I}$ and f are homogeneous, then the latter inequality is an equality.*

Proof. By Theorem 1.19, we can assume that $\mathcal{I}$ and $\mathcal{J}$ are in general Noether position. From Theorem 2.3 we know that $\tilde{\mathcal{J}}$ is unmixed of dimension -1 or $r-1$. By means of Theorem 1.12(a) we observe that the extensions of $\tilde{\mathcal{J}}$ and $\mathcal{J}$ coincide in $\mathbb{K}(x_1, \ldots, x_{r-1})[x_r, \ldots, x_n]$. Then Proposition 2.7 tells us that $\deg(\tilde{\mathcal{J}})$ equals the total degree of the constant coefficient χ_0 of the characteristic polynomial of f in $\mathbb{B}'$. Thanks to Theorem 1.27(b), we deduce that $\deg(\tilde{\mathcal{J}}) \leq \deg(\mathcal{I}) \deg(f)$. Finally, Theorem 1.27(a) implies that the latter inequality is an equality in the homogeneous case. □

3. Univariate Representations

Before the presentation of the Kronecker solver in the next section, it remains to explain how radical unmixed ideals are represented during the computations. In this section we carry on using the notation introduced in Section 1.3. We always write r for the dimension of $\mathcal{I}$, and δ for the dimension of $\mathbb{B}'$ seen as a $\mathbb{A}'$-vector space; we also assume that $\mathcal{I} \neq (1)$.

3.1. Existence and First Properties.

We start with a classical proposition that leads to the definition of a univariate representation of a radical unmixed ideal:

Proposition 3.1. *Assume that $\mathcal{I}$ is radical, unmixed, and in Noether position. Let $u = \lambda_{r+1}x_{r+1} + \cdots + \lambda_n x_n$ be a $\mathbb{K}$-linear form. Then, $\mathcal{I}'$ is radical, and the following assertions are equivalent:*

(a) *The powers of u generate $\mathbb{B}'$.*
(b) *The degree of the minimal polynomial of u in $\mathbb{B}'$ equals δ.*
(c) *There exist unique polynomials $q, v_{r+1}, \ldots, v_n$ in $\mathbb{A}'[T]$ such that $\mathcal{I}' = (q(u), x_{r+1} - v_{r+1}(u), \ldots, x_n - v_n(u))$, q is monic, and $\deg(v_j) \leq \deg(q) - 1$ for all $j \in \{r+1, \ldots, n\}$.*
(d) *There exist unique polynomials $q, w_{r+1}, \ldots, w_n$ in $\mathbb{A}'[T]$ such that $\mathcal{I}' = (q(u), q'(u)x_{r+1} - w_{r+1}(u), \ldots, q'(u)x_n - w_n(u))$, q is monic, and $\deg(w_j) \leq \deg(q) - 1$ for all $j \in \{r+1, \ldots, n\}$.*

Proof. We consider the morphism ψ from $\mathbb{A}'[T]$ to $\mathbb{B}'$ that sends T to u. Since its kernel is generated by the minimal polynomial of u in $\mathbb{B}'$, each of the four assertions are equivalent to saying that $\mathbb{B}'$ is isomorphic to $\mathbb{A}'[T]/\ker(\psi)$. □

Definition 3.2. A linear form u satisfying assertions (a)–(d) of Proposition 3.1 is a *primitive element* for $\mathcal{I}$. The polynomials $q, v_{r+1}, \ldots, v_n$ in assertion (c) form a *univariate representation* of $\mathcal{I}$. The polynomials $q, w_{r+1}, \ldots, w_n$ in assertion (d) form a *Kronecker representation* of $\mathcal{I}$.

Let $\Lambda_{r+1}, \ldots, \Lambda_n$ be new auxiliary variables, we introduce the following objects:

$$\mathbb{K}_\Lambda = \mathbb{K}(\Lambda_{r+1}, \ldots, \Lambda_n), \ \mathbb{A}_\Lambda = \mathbb{K}[\Lambda_{r+1}, \ldots, \Lambda_n, x_1, \ldots, x_r],$$

$$\mathbb{A}'_\Lambda = \mathbb{K}(\Lambda_{r+1}, \ldots, \Lambda_n, x_1, \ldots, x_r), \text{ and } \mathbb{B}'_\Lambda = \mathbb{A}'_\Lambda[x_{r+1}, \ldots, x_n]/\mathcal{I}'_\Lambda,$$

where $\mathcal{I}'_\Lambda$ denotes the extension of $\mathcal{I}$ to $\mathbb{A}'_\Lambda[x_{r+1}, \ldots, x_n]$. We write $\mathcal{I}_\Lambda$ for the extension of $\mathcal{I}$ to $\mathbb{K}[\Lambda_{r+1}, \ldots, \Lambda_n, x_1, \ldots, x_n]$ and we let

$$\mathbb{B}_\Lambda = \mathbb{K}[\Lambda_{r+1}, \ldots, \Lambda_n, x_1, \ldots, x_n]/\mathcal{I}_\Lambda.$$

We introduce the $\mathbb{K}_\Lambda$-linear form $u_\Lambda = \Lambda_{r+1}x_{r+1} + \cdots + \Lambda_n x_n$. The minimal polynomial of u_Λ in $\mathbb{B}'_\Lambda$ is written q_Λ, and we let

$$w_{\Lambda,j} = -\frac{\partial q_\Lambda}{\partial \Lambda_j}, \text{ for all } j \in \{r+1, \ldots, n\}.$$

Proposition 3.3. *Assume that $\mathcal{I}$ is unmixed and in Noether position.*

(a) *$\mathcal{I}$ is radical if, and only if, q_Λ is squarefree.*
(b) *If $\mathcal{I}$ is radical then u_Λ is primitive for $\mathcal{I}_\Lambda$, q_Λ belongs to $\mathbb{A}_\Lambda[T]$, $q_\Lambda(u_\Lambda)$ belongs to $\mathcal{I}_\Lambda$, and q_Λ is homogeneous of degree δ when seen as a polynomial in $\mathbb{A}'[\Lambda_{r+1}, \ldots, \Lambda_n, T]$. In addition, if the Noether position is general, then the total degree of q_Λ is δ when seen in $\mathbb{K}_\Lambda[x_1, \ldots, x_r, T]$.*

Proof. It is easy to check that $\mathcal{I}_\Lambda$ is in Noether position and unmixed of dimension n. From Theorem 1.27, we know that $q_\Lambda \in \mathbb{A}_\Lambda[T]$ and that

$$q_\Lambda(u_\Lambda) \in \mathcal{I}_\Lambda. \tag{3.1}$$

By differentiating $q_\Lambda(u_\Lambda)$ with respect to Λ_j, we obtain that

$$q'_\Lambda(u_\Lambda)x_j - w_{\Lambda,j}(u_\Lambda) \in \mathcal{I}_\Lambda. \tag{3.2}$$

If $\mathcal{I}$ is radical then $\mathcal{I}_\Lambda$ is radical, hence q_Λ is squarefree. Conversely, if q_Λ is squarefree then $q'_\Lambda(u_\Lambda)$ is invertible in $\mathbb{B}'_\Lambda$. It thus follows from (3.2) that the monomorphism $\mathbb{A}'_\Lambda[T]/(q_\Lambda(T)) \hookrightarrow \mathbb{B}'_\Lambda$ that sends T to u_Λ is surjective, and then that:

$$\mathcal{I}'_\Lambda = (q_\Lambda(u_\Lambda), q'_\Lambda(u_\Lambda)x_{r+1} - w_{\Lambda,r+1}(u_\Lambda), \dots, q'_\Lambda(u_\Lambda)x_n - w_{\Lambda,n}(u_\Lambda)).$$

Thanks to Corollary 1.24, the radicality of $\mathcal{I}'_\Lambda$ implies the one of $\mathcal{I}_\Lambda$, and thus the one of $\mathcal{I}$, which ends the proof of part (a). Since a basis of $\mathbb{B}'$ induces a basis of $\mathbb{B}'_\Lambda$, q_Λ is the characteristic polynomial of a matrix whose entries are homogeneous of degree one in $\Lambda_{r+1}, \dots, \Lambda_n$, and thus q_Λ is homogeneous of degree δ when seen in $\mathbb{A}'[\Lambda_{r+1}, \dots, \Lambda_n, T]$. The last assertion directly comes from Theorem 1.27(b). □

We are now ready to characterize the univariate representations of $\mathcal{I}$. For any linear form $u = \lambda_{r+1}x_{r+1} + \cdots + \lambda_n x_n$, we write $q_\lambda, w_{\lambda,r+1}, \dots, w_{\lambda,n}$ for the respective specializations of $q_\Lambda, w_{\Lambda,r+1}, \dots, w_{\Lambda,n}$ at $\Lambda_{r+1} = \lambda_{r+1}, \dots, \Lambda_n = \lambda_n$.

Corollary 3.4. *Assume that $\mathcal{I}$ is radical, unmixed, and in Noether position.*

(a) *u is primitive for $\mathcal{I}$ if, and only if, q_λ is squarefree.*

(b) *If u is primitive for $\mathcal{I}$, then $q_\lambda, w_{\lambda,r+1}, \dots, w_{\lambda,n}$ is the Kronecker representation of $\mathcal{I}$ associated to u. In particular, $q_\lambda, w_{\lambda,r+1}, \dots, w_{\lambda,n}$ all belong to $\mathbb{A}[T]$, and $q_\lambda(u), q'_\lambda(u)x_{r+1} - w_{\lambda,r+1}(u), \dots, q'_\lambda(u)x_n - w_{\lambda,n}(u)$ all belong to $\mathcal{I}$. In addition, if the Noether position is general, then the total degree of q_λ is δ, and the total degrees of $w_{\lambda,r+1}, \dots, w_{\lambda,n}$ are at most δ, when seen in $\mathbb{K}[x_1, \dots, x_r, T]$.*

Proof. By substituting $\lambda_{r+1}, \dots, \lambda_n$ for $\Lambda_{r+1}, \dots, \Lambda_n$ in (3.1) and (3.2), we obtain that $\deg(q_\lambda) = \delta$ and that

$$(q_\lambda(u), q'_\lambda(u)x_{r+1} - w_{\lambda,r+1}(u), \dots, q'_\lambda(u)x_n - w_{\lambda,n}(u)) \subseteq \mathcal{I}.$$

If $q_\lambda(u)$ is squarefree then $q'_\lambda(u)$ is invertible in $\mathbb{B}'$, and therefore the map from $\mathbb{A}'[T]/(q_\lambda(T))$ to $\mathbb{B}'$ that sends T to u is surjective. It follows from Proposition 3.1(a) that u is a primitive element. Conversely, if u is a primitive element, then the degree of the minimal polynomial q of u equals δ, by Proposition 3.1(b), and we thus obtain that q and q_λ have the same degrees, hence are equal. In particular, q_λ is squarefree, which concludes part (a). The rest of the proof comes directly from Proposition 3.3(b). □

Corollary 3.5. *Assume that $\mathcal{I}$ is radical, unmixed, and in Noether position. Then the set of points $(\lambda_{r+2}, \dots, \lambda_n) \in \mathbb{K}^{n-r-1}$ such that $u = x_{r+1} + \lambda_{r+2}x_{r+2} + \cdots + \lambda_n x_n$ is a primitive element for $\mathcal{I}$ is Zariski dense.*

Proof. By Proposition 3.3, the discriminant of q_Λ is nonzero and homogeneous in the variables $\Lambda_{r+1}, \dots, \Lambda_n$. Therefore if the specialization of this discriminant at $\Lambda_{r+1} = 1, \Lambda_{r+2} = \lambda_{r+2}, \dots, \Lambda_n = \lambda_n$ is nonzero then u is a primitive element for $\mathcal{I}$ by Corollary 3.4(a). □

3.2. **Specialization of the Independent Variables.** In this subsection, s denotes an integer in $\{0, \dots, r\}$, and we let $\mathcal{J} = \mathcal{I} + (x_{s+1}, \dots, x_r)$. We show how to compute a Kronecker representation of $\sqrt{\mathcal{J}}$ from one of $\mathcal{I}$, with the same primitive element. For this purpose, we introduce $\mathcal{J}_\Lambda = \mathcal{I}_\Lambda + (x_{s+1}, \dots, x_r)$ for the extension of $\mathcal{J}$ to $\mathbb{K}[\Lambda_{r+1}, \dots, \Lambda_n, x_1, \dots, x_n]$. Let $\mathbb{C}_\Lambda = \mathbb{K}[\Lambda_{r+1}, \dots, \Lambda_n, x_1, \dots, x_n]/\mathcal{J}_\Lambda$, and let Q_Λ represent the specialization of q_Λ at $x_{s+1} = \cdots = x_r = 0$. We write $\mathcal{J}'_\Lambda$ for the extension of $\mathcal{J}_\Lambda$ to $\mathbb{K}_\Lambda(x_1, \dots, x_s)[x_{s+1}, \dots, x_n]$, and we let $\mathbb{C}'_\Lambda = \mathbb{K}_\Lambda(x_1, \dots, x_s)[x_{s+1}, \dots, x_n]/\mathcal{J}'_\Lambda$.

Proposition 3.6. *Assume that $\mathcal{I}$ is radical, unmixed, and in Noether position (respectively, general Noether position). Then $\mathcal{J}$ is in Noether position (respectively, general Noether position), $\sqrt{\mathcal{J}}$ is unmixed of dimension s, and we have that:*

(a) *The squarefree part of Q_Λ is the minimal polynomial of u_Λ modulo the extension of $\sqrt{\mathcal{J}}$ to $\mathbb{K}_\Lambda(x_1,\ldots,x_s)[x_{s+1},\ldots,x_n]$.*
(b) *$\mathcal{J}$ is radical if, and only if, Q_Λ is squarefree.*

Proof. The Noether position (respectively, general Noether position) of $\mathcal{J}$, the unmixedness of $\sqrt{\mathcal{J}}$, and its dimension come from Corollary 2.5 directly. Let us now focus on the case when $s = r-1$. We introduce $\tilde{\mathcal{I}}_\Lambda$ for the extension of $\mathcal{I}_\Lambda$ to $\mathbb{K}_\Lambda(x_1,\ldots,x_{r-1})[x_r,x_{r+1},\ldots,x_n]$, and we let

$$\tilde{\mathbb{B}}_\Lambda = \mathbb{K}_\Lambda(x_1,\ldots,x_{r-1})[x_r,x_{r+1},\ldots,x_n]/\tilde{\mathcal{I}}_\Lambda.$$

By Proposition 1.22, $\mathbb{B}_\Lambda$ is a torsion-free $\mathbb{A}_\Lambda$-module, hence $\tilde{\mathbb{B}}_\Lambda$ is a torsion-free $\mathbb{K}_\Lambda(x_1,\ldots,x_{r-1})[x_r]$-module. By [45, Theorem 7.3], and since $\tilde{\mathcal{I}}_\Lambda$ is in Noether position, we deduce that $\tilde{\mathbb{B}}_\Lambda$ is a free $\mathbb{K}_\Lambda(x_1,\ldots,x_{r-1})[x_r]$-module of finite rank.

Since q_Λ is the characteristic polynomial of u_Λ in $\mathbb{B}'_\Lambda$, and since a basis of $\tilde{\mathbb{B}}_\Lambda$ induces a basis of $\mathbb{B}'_\Lambda$, we deduce that q_Λ is also the characteristic polynomial of u_Λ in $\tilde{\mathbb{B}}_\Lambda$. Since a basis of $\tilde{\mathbb{B}}_\Lambda$ induces a basis of $\mathbb{C}'_\Lambda$, we deduce that Q_Λ is the characteristic polynomial of u_Λ in $\mathbb{C}'_\Lambda$. It follows that the squarefree part of Q_Λ is the minimal polynomial of u_Λ in $\mathbb{K}_\Lambda(x_1,\ldots,x_{r-1})[x_r,\ldots,x_n]/\sqrt{\mathcal{J}'_\Lambda}$. Since the extension of $\sqrt{\mathcal{J}}$ to $\mathbb{K}_\Lambda(x_1,\ldots,x_{r-1})[x_r,\ldots,x_n]$ is $\sqrt{\mathcal{J}'_\Lambda}$, we are done with part (a) when $s = r-1$. For the other values of s, we can straightforwardly proceed by induction thanks to equality (2.1) (used in the proof of Corollary 2.5).

Let us now deal with part (b). If $\mathcal{J}$ is radical then $\mathcal{J}'_\Lambda$ is radical, and thus the characteristic polynomial Q_Λ of u_Λ in $\mathbb{C}'_\Lambda$ coincides with its minimal polynomial. We thus obtain that Q_Λ is squarefree. Conversely, if Q_Λ is squarefree then the minimal polynomial of u_Λ modulo $\mathcal{J}'_\Lambda$ is squarefree. Therefore $\mathcal{J}$ is radical by Proposition 3.3(a). □

Example 3.7. Let $\mathcal{I} = (x_1-x_4, x_2-x_3)\cap(x_3,x_4) = (x_1x_3-x_3x_4, x_2x_3-x_3^2, x_1x_4-x_4^2, x_2x_4-x_3x_4) \subseteq \mathbb{K}[x_1,\ldots,x_4]$. This ideal satisfies the hypotheses of Proposition 3.6 with $r=2$. We have $q_\Lambda(T) = T^2-(\Lambda_1x_2+\Lambda_2x_1)T$, $\deg(\mathcal{I})=2$, and $\mathcal{J} = \mathcal{I}+(x_1+x_2) = (x_1,x_2,x_3^2,x_3x_4,x_4^2)$ (with $s=r=2$). Therefore we get $\deg(\mathcal{J}) = 3 > \deg(\mathcal{I})$, which shows that one can not expect to obtain information on $\deg(\mathcal{J})$ from Q_Λ in general.

We are now ready to give formulas to compute a univariate representation of $\sqrt{\mathcal{J}}$, when u is a primitive element for $\sqrt{\mathcal{J}}$. Let $\tilde{Q}_\Lambda$ represent the squarefree part of Q_Λ, and let

$$\tilde{W}_{\Lambda,j} = -\frac{\partial \tilde{Q}_\Lambda}{\partial \Lambda_j}.$$

Let $\tilde{Q}_\lambda, \tilde{W}_{\lambda,r+1},\ldots,\tilde{W}_{\lambda,n}$ represent the specializations of $\tilde{Q}_\Lambda, \tilde{W}_{\Lambda,r+1},\ldots,\tilde{W}_{\Lambda,n}$ at $\Lambda_{r+1}=\lambda_{r+1},\ldots,\Lambda_n=\lambda_n$. By Proposition 3.6(a), $\tilde{Q}_\Lambda$ is the minimal polynomial of u_Λ modulo the extension of $\sqrt{\mathcal{J}}$ to $\mathbb{K}_\Lambda(x_1,\ldots,x_{s-1})[x_s,\ldots,x_n]$, so that by Corollary 3.4(b), $\tilde{Q}_\lambda, \tilde{W}_{\lambda,r+1},\ldots,\tilde{W}_{\lambda,n}$ is the Kronecker representation of $\sqrt{\mathcal{J}}$ with primitive element u.

Let us now assume that we only know the representation $q_\lambda, w_{\lambda,r+1},\ldots,w_{\lambda,n}$ of $\mathcal{I}$. From the only specializations $Q_\lambda, W_{\lambda,r+1},\ldots,W_{\lambda,n}$ of the latter representation at $x_{s+1}=\cdots=x_r=0$, one can easily compute the Kronecker representation of $\sqrt{\mathcal{J}}$ as follows:

Corollary 3.8. *Assume that $\mathcal{I}$ is radical, unmixed and in Noether position, and that u is primitive for $\mathcal{I}$ and for $\sqrt{\mathcal{J}}$.*

Let M_λ denote the greatest common divisor of Q_λ and Q'_λ, let $\tilde{q} = Q_\lambda/M_\lambda$ denote the squarefree part of Q_λ, let $P_\lambda = Q'_\lambda/M_\lambda$, and let P_λ^{-1} denote the inverse of P_λ in $\mathbb{K}[T]/(\tilde{q}(T))$. Then M_λ divides all the $W_{\lambda,j}$, so that can set $V_{\lambda,j} = W_{\lambda,j}/M_\lambda$, for each $j \in \{r+1,\dots,n\}$.

We define $\tilde{w}_j$ as the remainder of $\tilde{q}' V_{\lambda,j} P_\lambda^{-1}$ divided by $\tilde{q}(T)$, for all $j \in \{r+1,\dots,n\}$, and we let $\tilde{w}_j = 0$, for $j \in \{s+1,\dots,r\}$. Then $\tilde{q}, \tilde{w}_{s+1}, \dots, \tilde{w}_n$ is the Kronecker representation of $\sqrt{\mathcal{J}}$ with primitive element u.

Proof. We have to prove that $\tilde{q} = \tilde{Q}_\lambda, \tilde{w}_{r+1} = \tilde{W}_{\lambda,r+1}, \dots, \tilde{w}_n = \tilde{W}_{\lambda,n}$. Since u is a primitive element for $\sqrt{\mathcal{J}}$, Corollary 3.4(a) implies that $\tilde{Q}_\lambda$ is squarefree, whence $\tilde{q} = \tilde{Q}_\lambda$. It follows that M_λ is the specialization of the greatest common divisor M_Λ of Q_Λ and Q'_Λ at $\Lambda_{r+1} = \lambda_{r+1}, \dots, \Lambda_n = \lambda_n$.

Let $Q_\Lambda = Q_{\Lambda,1}^{\alpha_1} \cdots Q_{\Lambda,l}^{\alpha_l}$ represent the irreducible factorization of Q_Λ. Of course, we have $\tilde{Q}_\Lambda = Q_{\Lambda,1} \cdots Q_{\Lambda,l}$. We introduce $\hat{Q}_{\Lambda,j} = \tilde{Q}_\Lambda / Q_{\Lambda,j}$ and

$$\tilde{W}_{\Lambda,j,k} = -\frac{\partial Q_{\Lambda,k}}{\partial \Lambda_j}, \text{ for all } j \in \{r+1,\dots,n\}, \text{and all } k \in \{1,\dots,l\}.$$

We write $Q_{\lambda,j}$, $\hat{Q}_{\lambda,j}$ and $\tilde{W}_{\lambda,j,k}$ for the respective specializations of $Q_{\Lambda,j}$, $\hat{Q}_{\Lambda,j}$ and $\tilde{W}_{\Lambda,j,k}$ at $\Lambda_{r+1} = \lambda_{r+1}, \dots, \Lambda_n = \lambda_n$. From

$$\frac{W_{\Lambda,j}}{M_\Lambda} = \sum_{k=1}^{l} \alpha_k \tilde{W}_{\Lambda,j,k} \hat{Q}_{\Lambda,k}, \text{ where } W_{\Lambda,j} = -\frac{\partial Q_\Lambda}{\partial \Lambda_j},$$

we deduce that

$$V_{\lambda,j} = \sum_{k=1}^{l} \alpha_k \tilde{W}_{\lambda,j,k} \hat{Q}_{\lambda,k}.$$

Independently, a straightforward computation gives us the following identities:

$$\tilde{W}_{\lambda,j} = \sum_{k=1}^{l} \tilde{W}_{\lambda,j,k} \hat{Q}_{\lambda,k}, \text{ and } P_\lambda = \sum_{k=1}^{l} \alpha_k Q'_{\lambda,k} \hat{Q}_{\lambda,k}.$$

Finally the fact that $P_\lambda \tilde{W}_{\lambda,j}$ equals $\tilde{Q}'_\lambda V_{\lambda,j}$ in $\mathbb{K}[T]/(\tilde{Q}_\lambda(T))$ is equivalent to the following identity in $\mathbb{K}[T]/(\tilde{Q}_\lambda(T))$:

$$\left(\sum_{k=1}^{l} \alpha_k Q'_{\lambda,k} \hat{Q}_{\lambda,k}\right)\left(\sum_{k=1}^{l} \tilde{W}_{\lambda,j,k} \hat{Q}_{\lambda,k}\right) = \left(\sum_{k=1}^{l} Q'_{\lambda,k} \hat{Q}_{\lambda,k}\right)\left(\sum_{k=1}^{l} \alpha_k \tilde{W}_{\lambda,j,k} \hat{Q}_{\lambda,k}\right),$$

which is clearly satisfied modulo each $Q_{\lambda,k}$ for all $k \in \{1,\dots,l\}$. □

Corollary 3.9. *Assume that $\mathcal{I}$ is radical, unmixed, and in Noether position (respectively, general Noether position), and that $\mathcal{I} + (x_1,\dots,x_r)$ is radical.*

(a) *$\mathcal{J}$ is radical, unmixed of dimension s, and in Noether position (respectively, general Noether position).*
(b) *If $u = \lambda_{r+1}x_{r+1} + \cdots + \lambda_n x_n$ is a primitive element for $\mathcal{I} + (x_1,\dots,x_r)$ then it is a primitive element for $\mathcal{J}$.*

Proof. In order to prove part (a), it remains to prove that $\mathcal{J}$ is radical. Since $\mathcal{I} + (x_1,\dots,x_r)$ is radical, Proposition 3.6(b) (applied with $s = 0$) implies that the specialization of q_Λ at $x_1 = \cdots = x_r = 0$ is squarefree. We deduce that Q_Λ is squarefree, and Proposition 3.6(b) thus gives us the radicality of $\mathcal{J}$.

By combining Proposition 3.6 applied with $s = 0$ and Corollary 3.4(a) we obtain that the specialization of q_Λ at $x_1 = \cdots = x_r = 0$ and $\Lambda_{r+1} = \lambda, \dots, \Lambda_n = \lambda_n$ is squarefree, so is the specialization of Q_Λ at $\Lambda_{r+1} = \lambda, \dots, \Lambda_n = \lambda_n$. Therefore part (b) follows from Corollary 3.4(a). □

Corollary 3.10. *Assume that $\mathcal{I}$ is radical, unmixed, and in Noether position. Then the set of points $(\beta_1, \ldots, \beta_r) \in \mathbb{K}^r$ such that $\mathcal{I} + (x_1 - \beta_1, \ldots, x_r - \beta_r)$ is radical is Zariski dense.*

Proof. Proposition 3.3(a) tells us that q_Λ is squarefree, and thus that its discriminant is nonzero. If the specialization of this discriminant at $x_1 = \beta_1, \ldots, x_r = \beta_r$ is nonzero, then Proposition 3.6(b) implies that $\mathcal{I}+(x_1-\beta_1, \ldots, x_r-\beta_r)$ is radical. □

The following corollary gathers our previous genericity results in a form that will be useful in Section 4.1. We let ϕ denote an affine change of the variables of the following form:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} 1 & \alpha_{1,2} & \ldots & \alpha_{1,n} \\ 0 & 1 & \ldots & \alpha_{2,n} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}, \tag{3.3}$$

where all the $\alpha_{k,l}$ and β_k are taken in $\mathbb{K}$.

Corollary 3.11. *Assume that $\mathcal{I}$ is radical and unmixed of dimension $r \geq 1$. Let f and g be in $\mathbb{K}[x_1, \ldots, x_n]$ such that f is a nonzerodivisor in $\mathbb{B}$, and such that $(\mathcal{I}+(f)) : g^\infty \neq (1)$. Then $\sqrt{\mathcal{I} + (f)}$ and $\sqrt{\mathcal{I} + (f)} : g^\infty$ are unmixed of dimension $r - 1$, and there exists a Zariski dense subset of maps ϕ such that:*

(a) *$\mathcal{I} \circ \phi$, $\sqrt{\mathcal{I} + (f)} \circ \phi$ and $(\sqrt{\mathcal{I} + (f)} : g^\infty) \circ \phi$ are in general Noether position;*
(b) *$\mathcal{I} \circ \phi + (x_1, \ldots, x_r)$ is radical;*
(c) *$(\sqrt{\mathcal{I} + (f)} : g^\infty) \circ \phi + (x_1, \ldots, x_{r-1}) = (\sqrt{\mathcal{I} + (f)} \circ \phi + (x_1, \ldots, x_{r-1})) : (g \circ \phi)^\infty$;*
(d) *x_r is a primitive element for $\sqrt{(\mathcal{I} + (f)) \circ \phi + (x_1, \ldots, x_{r-1})}$;*
(e) *x_{r+1} is a primitive element for $\sqrt{\mathcal{I} \circ \phi + (x_1, \ldots, x_{r-1}, x_r - a)}$, for each root $a \in \bar{\mathbb{K}}$ (the algebraic closure of $\mathbb{K}$) of the minimal polynomial of x_r modulo $\sqrt{(\mathcal{I} + (f)) \circ \phi + (x_1, \ldots, x_{r-1})}$.*

Proof. Remark that $(\mathcal{I} + (f)) : g^\infty \neq (1)$ implies that $(\mathcal{I} + (f)) \neq (1)$, so that Theorem 2.3 implies that $\sqrt{\mathcal{I} + (f)}$ is unmixed of dimension $r - 1$, and so is $\sqrt{\mathcal{I} + (f)} : g^\infty$ by Corollary 1.26. By combining Theorem 1.19, Corollary 1.26 and Proposition 2.2 we obtain that there exists a Zariski dense subset of maps ϕ such that property (a) holds. Property (b) comes from Corollary 3.10. Since g is a nonzerodivisor modulo $\sqrt{\mathcal{I} + (f)} : g^\infty$, property (c) follows from Corollary 2.6.

Now we suppose that properties (a)–(c) hold. From Corollary 2.5, we know that $\sqrt{(\mathcal{I} + (f)) \circ \phi + (x_1, \ldots, x_{r-1})}$ has dimension 0. We introduce the linear forms $l_1, \ldots, l_n$ defined by

$$(l_1, \ldots, l_n) = \phi^{-1}(x_1, \ldots, x_n).$$

By construction, $l_1, \ldots, l_{r-1}$ are algebraically independent modulo $\mathcal{I} + (f)$ and $l_r, \ldots, l_n$ are generally integral over $\mathbb{K}[l_1, \ldots, l_{r-1}]$ modulo $\mathcal{I}+(f)$. Since the linear part of ϕ is upper triangular, we deduce from Proposition 1.17 that $x_r, \ldots, x_n$ are also generally integral over $\mathbb{K}[l_1, \ldots, l_{r-1}]$ modulo $\mathcal{I} + (f)$. Therefore we can naturally see $\sqrt{\mathcal{I} + (f) + (l_1, \ldots, l_{r-1})}$ as an ideal of $\mathbb{K}[x_r, \ldots, x_n]$, so that Corollary 3.5 gives us that the set of points $(\lambda_{r+1}, \ldots, \lambda_n)$ such that $l_r = x_r + \lambda_{r+1}x_{r+1} + \cdots + \lambda_n x_n$ is a primitive element for $\sqrt{\mathcal{I} + (f) + (l_1, \ldots, l_{r-1})}$ is Zariski dense, which yields property (d).

Let $a \in \bar{\mathbb{K}}$ be as defined in part (e). By Corollary 2.5, $\sqrt{\mathcal{I} + (l_1, \ldots, l_{r-1}, l_r - a)}$ has dimension 0. We can use Corollary 3.5 again in order to obtain that the set of points $(\lambda_{r+2}, \ldots, \lambda_n)$ such that $l_{r+1} = x_{r+1} + \lambda_{r+2}x_{r+2} + \cdots + \lambda_n x_n$ is

a primitive element for $\sqrt{\mathcal{I} + (l_1, \ldots, l_{r-1}, l_r - a)}$ is Zariski dense, which yields property (e). □

4. The Kronecker Solver

This section contains a complete presentation of the Kronecker solver together with its proof of correctness. The top level function is given in the first subsection, the subroutines are detailed after. We recall from the introduction that the input system is written $f_1 = \cdots = f_n = 0$, $g \neq 0$, and is assumed to verify that, for all $i \in \{0, \ldots, n-1\}$, f_{i+1} is a nonzerodivisor modulo $\mathcal{I}_i$, and $\mathcal{I}_i$ is radical. The algorithm computes some representations of $\mathcal{I}_i = (f_1, \ldots, f_i) : g^\infty$ in sequence for i from 0 to n. Since it is easy to make the algorithm stop as soon as it reaches $\mathcal{I}_i = (1)$, in order to simplify the presentation, we will assume in the rest of the paper that $\mathcal{I}_i \neq (1)$ for all $i \in \{0, \ldots, n\}$.

Example 4.1. Throughout this section, we illustrate the algorithm by means of the following example with $n = 3$ variables over the rational number field:

$$\begin{aligned} f_1 &= x_1^2 + x_2^2 + x_3^2 - 2, \\ f_2 &= x_1^2 + x_2^2 - 1, \\ f_3 &= x_1 - x_2 + 3x_3, \\ g &= x_3 - 1. \end{aligned}$$

4.1. The Top Level Algorithm.

Under our hypotheses we have the following central properties:

Proposition 4.2. *For all $i \in \{0, \ldots, n-1\}$, the ideals $\sqrt{\mathcal{I}_i + (f_{i+1})}$ and $\mathcal{I}_{i+1}$ are unmixed of dimension $n - i - 1$.*

Proof. By definition, $\mathcal{I}_0$ equals (0), hence is unmixed of dimension n. By induction, assume that $\mathcal{I}_i$ is unmixed of dimension $n-i$ for some $i \in \{0, \ldots, n-1\}$. Since f_{i+1} is assumed to be a nonzerodivisor modulo $\mathcal{I}_i$, Theorem 2.3 implies that $\sqrt{\mathcal{I}_i + (f_{i+1})}$ is either (1) or unmixed of dimension $n - i - 1$. From

$$\sqrt{\mathcal{I}_{i+1}} = \sqrt{(\mathcal{I}_i + (f_{i+1})) : g^\infty} = \sqrt{\mathcal{I}_i + (f_{i+1})} : g^\infty,$$

we deduce that $\mathcal{I}_i + (f_{i+1})$ has dimension $n - i - 1$ since $\mathcal{I}_{i+1}$ is assumed to be proper. When $i \leq n-2$, $\mathcal{I}_{i+1}$ is assumed to be radical, so that its unmixedness and its dimension follow from Corollary 1.26. When $i = n-1$, $\mathcal{I}_i + (f_{i+1})$ is necessarily unmixed of dimension 0, so that Corollary 1.26 gives us that $\mathcal{I}_{i+1}$ is unmixed of dimension 0. □

We recall from the introduction that we have defined $\mathcal{J}_i = \sqrt{\mathcal{I}_i + (x_1, \ldots, x_{n-i})}$ and $\mathcal{K}_i = \sqrt{\mathcal{I}_i + (x_1, \ldots, x_{n-i-1})}$. Before entering the main computations, the solver performs a random affine change of the variables in the input polynomials $f_1, \ldots, f_n$ and g so that the following properties hold:

- (A_1) $\mathcal{I}_i$ is unmixed of dimension $n - i$ and in general Noether position, for all $i \in \{0, \ldots, n\}$.
- (A_2) $\sqrt{\mathcal{I}_i + (f_{i+1})}$ is unmixed of dimension $n - i - 1$ and in general Noether position, for all $i \in \{0, \ldots, n-1\}$.
- (A_3) $\sqrt{\mathcal{I}_i + (f_{i+1})} : g^\infty$ is unmixed of dimension $n-i-1$ and in general Noether position, for all $i \in \{0, \ldots, n-1\}$.
- (A_4) $\mathcal{I}_i + (x_1, \ldots, x_{n-i})$ is radical for all $i \in \{0, \ldots, n-1\}$.
- (A_5) $\mathcal{J}_{i+1} = \sqrt{\mathcal{K}_i + (f_{i+1})} : g^\infty$, for all $i \in \{0, \ldots, n-1\}$.

(A_6) x_{n-i} is a primitive element for $\sqrt{\mathcal{K}_i + (f_{i+1})}$, for all $i \in \{0, \ldots, n-1\}$.

(A_7) x_{n-i+1} is a primitive element for $\sqrt{\mathcal{K}_i + (x_{n-i} - a)}$ for each root $a \in \bar{\mathbb{K}}$ (the algebraic closure of $\mathbb{K}$) of the minimal polynomial of x_{n-i} modulo $\sqrt{\mathcal{K}_i + (f_{i+1})}$, for all $i \in \{1, \ldots, n-1\}$.

(A_8) $\mathcal{K}_i = \mathcal{I}_i + (x_1, \ldots, x_{n-i-1})$, is unmixed of dimension 1, and is in general Noether position when seen in $\mathbb{K}[x_{n-i}, \ldots, x_n]$, for all $i \in \{0, \ldots, n-1\}$.

(A_9) $\mathcal{J}_i$ is zero dimensional, for all $i \in \{0, \ldots, n\}$.

(A_{10}) x_{n-i+1} is a primitive element for $\mathcal{J}_i$, for all $i \in \{1, \ldots, n\}$.

(A_{11}) x_{n-i+1} as a primitive element for $\mathcal{K}_i$, for all $i \in \{1, \ldots, n-1\}$.

(A_{12}) x_{n-i+1} as a primitive element for $\mathcal{I}_i$, for all $i \in \{1, \ldots, n-1\}$.

We are to show that such a change of the variables can be found at random with a very high probability of success. More precisely, we are to prove that almost all affine changes of the variables ϕ defined in (3.3) ensures properties (A_1)–(A_{12}).

Proposition 4.3. *There exists a Zariski dense subset of maps ϕ for which properties (A_1)–(A_{12}) are satisfied if we replace the input system by $f_1 \circ \phi = \cdots = f_n \circ \phi = 0$, $g \circ \phi \neq 0$.*

Proof. For any $i \in \{0, \ldots, n-1\}$, Corollary 3.11 applied with $\mathcal{I}_i$, f_{i+1} and g gives us properties (A_1)–(A_7) directly. Assume now that (A_1)–(A_7) hold. Then (A_8) and (A_9) are necessarily satisfied, by Corollaries 2.5 and 3.9(a). Property (A_{10}) is obtained via Proposition 3.1(a) thanks to (A_6) and the inclusion $\sqrt{\mathcal{K}_i + (f_{i+1})} \subseteq \mathcal{J}_{i+1}$. Finally, properties ($A_{11}$) and ($A_{12}$) follow from Corollary 3.9(b) thanks to (A_4). □

Example 4.4. The input system of Example 4.1 does not satisfy (A_6). After the change of variables

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix},$$

we obtain the system

$$\begin{aligned} f_1 &= x_1^2 + x_2^2 + 5x_3^2 - 4x_2x_3 - 2, \\ f_2 &= x_1^2 + x_2^2 + 4x_3^2 - 4x_2x_3 - 1, \\ f_3 &= x_1 - x_2 + 3x_3, \\ g &= x_3 - 1, \end{aligned}$$

which satisfies all properties (A_1)–(A_{12}).

Here it is important to underline that such a change ϕ of the variables does not spoil the evaluation cost of the input system: using evaluation data structures for the input polynomials is a great advantage here. Once the change of the variables is performed in the input system, the solver is organized around one main loop. The ith iteration of this loop computes the univariate representation of $\mathcal{J}_{i+1}$ with primitive element x_{n-i} from the one of $\mathcal{J}_i$ with primitive element x_{n-i+1}. This iteration divides into the three following steps:

(1) *Lifting step.* Compute the Kronecker representation of $\mathcal{K}_i$ with primitive element x_{n-i+1}.
(2) *Intersection step.* Compute the univariate representation of $\sqrt{\mathcal{K}_i + (f_{i+1})}$ with primitive element x_{n-i}.

(3) *Cleaning step.* Compute the univariate representation of $\sqrt{\mathcal{K}_i + (f_{i+1})} : g^\infty = \mathcal{J}_{i+1}$ with primitive element x_{n-i}.

Example 4.5. Geometrically speaking, with Example 4.1, the first lifting step computes a Kronecker representation of a circle on the sphere defined by $f_1 = 0$. The first intersection step computes a univariate representation of four points on the two circles defined by $f_1 = f_2 = 0$. The second cleaning step takes one of the two circles aways by removing its two associated points in the latter representation.

Each of these steps is detailed in the next subsections. Let $\delta_i = \deg(\mathcal{I}_i)$ for each $i \in \{0, \ldots, n\}$, and let $\delta = \max(\delta_i \mid i \in \{0, \ldots, n\})$. The following corollary of Theorem 2.12 is the cornerstone of the cost analysis of the Kronecker solver, which is done in [30]:

Corollary 4.6. *For all $i \in \{0, \ldots, n-1\}$, let $\tilde{\mathcal{I}}_{i+1}$ denote the intersection of the primary components of $\mathcal{I}_i + (f_{i+1})$ belonging to an isolated associated prime. Then we have that $\delta_{i+1} \leq \deg(\tilde{\mathcal{I}}_{i+1}) \leq \deg(f_{i+1})\delta_i$. The latter inequalities are equalities whenever $g = 1$ and $f_1, \ldots, f_{i+1}$ are homogeneous.*

Proof. Theorem 2.12 implies that $\deg(\tilde{\mathcal{I}}_{i+1}) \leq \deg(f_{i+1})\delta_i$, with equality in the homogeneous case. If $i \leq n-2$ then $\mathcal{I}_{i+1}$ is assumed to be radical, whence $\mathcal{I}_{i+1} = \sqrt{\mathcal{I}_i + (f_{i+1})} : g^\infty = \sqrt{\tilde{\mathcal{I}}_{i+1}} : g^\infty$ by Theorem 2.3. If $i = n-1$, then we have that $\tilde{\mathcal{I}}_{i+1} = \mathcal{I}_i + (f_{i+1})$. In both cases Proposition 2.11 yields $\delta_{i+1} \leq \deg(\tilde{\mathcal{I}}_{i+1})$. Of course the latter inequality is an equality whenever $g = 1$. □

4.2. **Lifting Step.** We are now to detail the ith lifting step. For convenience we let $\mathcal{I} = \mathcal{I}_i$, $\mathcal{J} = \mathcal{J}_i$, $\mathcal{K} = \mathcal{K}_i$, and $r = n - i$, so that we can reuse the notation of the previous sections. The input of this lifting step is the univariate representation $Q, V_{r+1}, \ldots, V_n$ of $\mathcal{J}$ seen in $\mathbb{K}[x_{r+1}, \ldots, x_n]$ with primitive element x_{r+1}. We write $Q, W_{r+1}, \ldots, W_n$ for the associated Kronecker representation. The output is the Kronecker representation $\tilde{Q}, \tilde{W}_{r+1}, \ldots, \tilde{W}_n$ of $\mathcal{K}$ seen in $\mathbb{K}[x_r, \ldots, x_n]$ with the same primitive element x_{r+1}. We introduce $\hat{\mathbb{A}} = \mathbb{K}[[x_1, \ldots, x_r]]$, and $\hat{\mathbb{B}} = \hat{\mathbb{A}}[x_{r+1}, \ldots, x_n]/\hat{\mathcal{I}}$, where $\hat{\mathcal{I}}$ represents the extension of $\mathcal{I}$ to $\hat{\mathbb{A}}[x_{r+1}, \ldots, x_n]$.

Thanks to (A_{12}), we can consider the Kronecker (respectively, univariate) representation $q, w_{r+1}, \ldots, w_n$ (respectively, $q, v_{r+1}, \ldots, v_n$) of $\mathcal{I}$ with primitive element x_{r+1}.

From Corollary 3.8, we know that the specializations of $q, w_{r+1}, \ldots, w_n$ at $x_1 = \cdots = x_r = 0$ coincide with $Q, W_{r+1}, \ldots, W_n$ respectively, and that the specializations of $q, w_{r+1}, \ldots, w_n$ at $x_1 = \cdots = x_{r-1} = 0$ coincide with $\tilde{Q}, \tilde{W}_{r+1}, \ldots, \tilde{W}_n$ respectively. Furthermore, thanks to Corollary 3.4(b), it is sufficient to compute the approximation of $q, w_{r+1}, \ldots, w_n$ in $\hat{\mathbb{A}}[T]$ to precision $(x_1, \ldots, x_{r-1}, x_r^{\delta_i+1})$ in order to obtain $\tilde{Q}, \tilde{W}_{r+1}, \ldots, \tilde{W}_n$.

More generally we are going to present an algorithm that computes the approximation of $q, w_{r+1}, \ldots, w_n$ in $\hat{\mathbb{A}}[T]$ to any precision. This algorithm relies on a modified version of the classical Newton method. Let $\mathfrak{o}^{[0]}$ be any ideal of $\hat{\mathbb{A}}$ contained in $(x_1, \ldots, x_r)$. It is sufficient to describe how to go from the approximation $q^{[0]}, w_{r+1}^{[0]}, \ldots, w_n^{[0]}$ to precision $\mathfrak{o}^{[0]}$ to the approximation $q^{[1]}, w_{r+1}^{[1]}, \ldots, w_n^{[1]}$ to precision $\mathfrak{o}^{[1]}$, for any ideal $\mathfrak{o}^{[1]}$ containing $(\mathfrak{o}^{[0]})^2$. Inside the approximation algorithm we will need the following statement, in which part (b) is part of the classical Jacobian criterion:

Lemma 4.7. *The polynomials $v_{r+1} = w_{r+1}(q')^{-1}, \ldots, v_n = w_n(q')^{-1}$ are well defined in $\hat{\mathbb{A}}[T]$, and the following properties hold:*

(a) $\hat{\mathcal{I}} = (q(x_{r+1}), x_{r+1} - v_{r+1}(x_{r+1}), \ldots, x_n - v_n(x_{r+1}))$.

(b) *The Jacobian matrix J of $f_1, \ldots, f_i$ with respect to the variables $x_{r+1}, \ldots, x_n$ is invertible in $\hat{\mathbb{B}}$.*

Proof. We have already seen that q' is invertible modulo q in $\hat{\mathbb{A}}[T]$. Therefore $v_{r+1}, \ldots, v_n$ are well defined in $\hat{\mathbb{A}}[T]$, and we obtain the following inclusion from Corollary 3.4(b):

$$(q(x_{r+1}), x_{r+1} - v_{r+1}(x_{r+1}), \ldots, x_n - v_n(x_{r+1})) \subseteq \hat{\mathcal{I}}.$$

Conversely, for any $f \in \mathcal{I}$, we have that

$$f(x_1, \ldots, x_r, v_{r+1}(T), \ldots, v_n(T)) = 0 \text{ in } \mathbb{A}'[T]/(q(T)).$$

The fact that the latter equality also holds in $\hat{\mathbb{A}}[T]/(q(T))$ concludes part (a).

Let $u = \lambda_{r+1}x_{r+1} + \cdots + \lambda_n x_n$ be a $\mathbb{K}$-linear form, and let q_λ be its minimal polynomial in $\mathbb{B}'$. By Theorem 1.27(c), there exist some polynomials $h_1, \ldots, h_i$ in $\mathbb{K}[x_1, \ldots, x_n]$ and a nonnegative integer α such that $g^\alpha q_\lambda(u) = h_1 f_1 + \cdots + h_i f_i$. By differentiating with respect to $x_{r+1}, \ldots, x_n$, and by multiplying by g both sides of the latter equality, we deduce that all the entries of

$$g^{\alpha+1} q'_\lambda(u)(\lambda_{r+1}, \ldots, \lambda_n) - g(h_1, \ldots, h_i)J \tag{4.1}$$

belong to $(f_1, \ldots, f_i)$. Thanks to (A_5), g is a nonzerodivisor in $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{J}$, hence the constant coefficient of the minimal polynomial of g in $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{J}$ is in $\mathbb{K} \setminus \{0\}$ by Lemma 2.1. Therefore by Proposition 3.6(a), the constant coefficient of the minimal polynomial of g in $\mathbb{B}$ is invertible in $\hat{\mathbb{B}}$, and so is g. Since (4.1) also holds over $\hat{\mathbb{A}}$ and since $q'(u)$ is invertible in $\hat{\mathbb{B}}$, we deduce that J is invertible in $\hat{\mathbb{B}}$, which proves part (b). □

Since $q^{[1]}$ coincides with $q^{[0]}$ to precision $\mathfrak{o}^{[0]}$, there exists a unique polynomial $\Delta \in \mathfrak{o}^{[0]}[T]$ defined to precision $\mathfrak{o}^{[1]}$, with $\deg(\Delta) \leq \delta_i - 1$, and such that $q^{[0]}(T)$ divides $q^{[1]}(T + \Delta(T))$ to precision $\mathfrak{o}^{[1]}$, namely $\Delta(T)$ is the remainder of $-q^{[1]}(q^{[1]\prime})^{-1}$ divided by $q^{[0]}$ to the precision $\mathfrak{o}^{[1]}$. For each $j \in \{r+1, \ldots, n\}$, we introduce the polynomial $\tilde{v}_j^{[1]}(T)$ as the remainder of $v_j^{[1]}(T + \Delta(T))$ divided by $q^{[0]}(T)$ to precision $\mathfrak{o}^{[1]}$.

From Lemma 4.7(a), we know that:

$$f_j(x_1, \ldots, x_r, v_{r+1}^{[1]}(T), \ldots, v_n^{[1]}(T)) = 0 \text{ in } (\hat{\mathbb{A}}/\mathfrak{o}^{[1]})[T]/(q^{[1]}(T)),$$

for all $j \in \{1, \ldots, i\}$. By substituting $T + \Delta(T)$ for T in the latter equality we deduce that:

$$f_j(x_1, \ldots, x_r, \tilde{v}_{r+1}^{[1]}(T), \ldots, \tilde{v}_n^{[1]}(T)) = 0 \text{ in } (\hat{\mathbb{A}}/\mathfrak{o}^{[1]})[T]/(q^{[0]}(T)),$$

for all $j \in \{1, \ldots, i\}$. But thanks to Lemma 4.7(b), $\tilde{v}_{r+1}^{[1]}, \ldots, \tilde{v}_n^{[1]}$ can be obtained by means of the following Newton iteration computed in $(\hat{\mathbb{A}}/\mathfrak{o}^{[1]})[T]/(q^{[0]}(T))$ to precision $\mathfrak{o}^{[1]}$:

$$\begin{pmatrix} \tilde{v}_{r+1}^{[1]} \\ \vdots \\ \tilde{v}_n^{[1]} \end{pmatrix} = \begin{pmatrix} v_{r+1}^{[0]} \\ \vdots \\ v_n^{[0]} \end{pmatrix} - J^{-1} \begin{pmatrix} f_1 \\ \vdots \\ f_i \end{pmatrix} (x_1, \ldots, x_r, v_{r+1}^{[0]}, \ldots, v_n^{[0]}).$$

Now it remains to show how the $v_j^{[1]}$ can be recovered from the $\tilde{v}_j^{[1]}$. First of all, since $v_{r+1}^{[1]}(T) = T$, we easily recover $\Delta(T) = \tilde{v}_{r+1}^{[1]}(T) - T$. Then, for each $j \in \{r+1, \ldots, n\}$, by means of a second order Taylor expansion, we obtain that:

$$\tilde{v}_j^{[1]}(T) = v_j^{[1]}(T) + \Delta_j(T),$$

where $\Delta_j(T)$ represents the remainder of $\Delta(T){v_j^{[0]}}'(T)$ divided by $q^{[0]}(T)$ to precision $\mathfrak{o}^{[1]}$. This way we can deduce $v_j^{[1]}(T)$. In a similar manner we have that

$$q^{[1]}(T) = q^{[0]}(T) + \Delta_q(T),$$

where $\Delta_q(T)$ represents the remainder of $\Delta(T){q^{[0]}}'(T)$ divided by $q^{[0]}(T)$ to precision $\mathfrak{o}^{[1]}$.

Example 4.8. Let us illustrate the first lifting step of the resolution of the system of Example 4.1, that corresponds to the easiest case, when $i = 1$. At the first iteration of the lifting step we have: $q^{[0]} = Q = T^2 - 2/5$, $v_3^{[0]} = V_3 = T$, $\mathfrak{o}^{[0]} = (x_2)$, and $\mathfrak{o}^{[1]} = (x_2^2)$. The Newton iteration leads to $\tilde{v}_3^{[1]} = T + 2/5x_2$. We thus obtain $\Delta = 2/5x_2$, $\Delta_q = -4/5x_2T$, and then $q^{[1]}(T) = T^2 - 2/5 - 4/5x_2T$, which is of course the approximation of the monic part of $f_1(0, x_2, T)$ to precision $\mathfrak{o}^{[1]}$. As for the second and last iteration, we take $\mathfrak{o}^{[0]} = (x_2^2)$ and $\mathfrak{o}^{[1]} = (x_2^3)$, and obtain $q^{[1]}(T) = T^2 - 2/5 - 4/5x_2T + 1/5x_2^2$, that is the monic part of $f_1(0, x_2, T)$.

4.3. **Intersection Step.** We carry on with writing $\mathcal{I}$ for $\mathcal{I}_i$, $\mathcal{J}$ for $\mathcal{J}_i$, $\mathcal{K}$ for $\mathcal{K}_i$ and r for $n - i$. We further let $f = f_{i+1}(0, \dots, 0, x_r, \dots, x_n)$. The input of the ith intersection step is the Kronecker representation $\tilde{Q}, \tilde{W}_{r+1}, \dots, \tilde{W}_n$ of $\mathcal{K}$ seen in $\mathbb{K}[x_r, \dots, x_n]$ with primitive element x_{r+1}. We write $\tilde{Q}, \tilde{V}_{r+1}, \dots, \tilde{V}_n$ for the associated univariate representation. The output is the univariate representation $\hat{Q}, \hat{V}_r, \dots, \hat{V}_n$ of $\sqrt{\mathcal{K} + (f)}$ (seen in $\mathbb{K}[x_r, \dots, x_n]$) with primitive element x_r. We first give a formula for $\hat{Q}$.

Proposition 4.9. *The characteristic polynomial of x_r modulo $\mathcal{K} + (f)$ is equal to the following resultant in T:*

$$\chi_0 = \mathrm{Res}_T(f(x_r, \tilde{V}_{r+1}(T), \dots, \tilde{V}_n(T)), \tilde{Q}(T)). \tag{4.2}$$

In particular, $\hat{Q}(x_r)$ is the squarefree part of χ_0.

Proof. From (A_8) we know that $\mathcal{K}$ is unmixed of dimension 1 and is in general Noether position when seen in $\mathbb{K}[x_r, \dots, x_n]$. Thanks to ($A_2$), Corollary 2.5 implies that $f(x_r, \dots, x_n)$ is nonzerodivisor in $\mathbb{K}[x_r, \dots, x_n]/\mathcal{K}$. Therefore the conclusion follows directly from Proposition 2.7. □

By means of Corollary 3.8, and thanks to (A_7), for any root $a \in \bar{\mathbb{K}}$ of $\hat{Q}$, we can compute the univariate representation $\tilde{Q}_a, \tilde{V}_{a,r+1}, \dots, \tilde{V}_{a,n}$ of $\sqrt{\mathcal{K} + (x_r - a)}$ with primitive element x_{r+1}, so that we have:

$$\sqrt{\mathcal{K} + (x_r - a)} = (\tilde{Q}_a(x_{r+1}), x_r - a, x_{r+1} - \tilde{V}_{a,r+1}(x_{r+1}), \dots, x_n - \tilde{V}_{a,n}(x_{r+1})).$$

We deduce that:

$$\begin{aligned}\sqrt{\mathcal{K} + (x_r - a)} + (f) = (f(a, \tilde{V}_{a,r+1}(x_{r+1}), \dots, \tilde{V}_{a,n}(x_{r+1})), \tilde{Q}_a(x_{r+1})) \\ + (x_r - a, x_{r+1} - \tilde{V}_{a,r+1}(x_{r+1}), \dots, x_n - \tilde{V}_{a,n}(x_{r+1})).\end{aligned}$$

On the other hand, since x_r is primitive for $\sqrt{\mathcal{K} + (f)}$ by property (A_6), we have that

$$\sqrt{\mathcal{K} + (f)} + (x_r - a) = (x_r - \hat{V}_r(a), \dots, x_n - \hat{V}_n(a)).$$

Therefore we can compute $\hat{V}_{r+1}(a)$ by means of the following formula:

$$x_{r+1} - \hat{V}_{r+1}(a) = \gcd(f(a, \tilde{V}_{a,r+1}(x_{r+1}), \dots, \tilde{V}_{a,n}(x_{r+1})), \tilde{Q}_a(x_{r+1})),$$

where gcd means the greatest common divisor. By substituting $\hat{V}_{r+1}(a)$ for x_{r+1} in all the $\tilde{V}_{a,j}$, we obtain $\hat{V}_j(a) \in \bar{\mathbb{K}}$, for all $j \in \{r + 2, \dots, n\}$. Finally $\hat{V}_r, \dots, \hat{V}_n$ can be obtained by interpolation.

Example 4.10. Let us carry on with Example 4.1. We enter the first intersection step (that is $i = 1$) with $\tilde{Q} = T^2 - 2/5 - 4/5x_2 + 1/5x_1^2$ and $\tilde{V}_3 = T$. The resultant computation leads to $\chi_0 = 1/25x_2^4 - 2/5x_2^2 + 9/25$. Since χ_0 is squarefree, we have $\hat{Q}(T) = T^4 - 10T^2 + 9 = (T-1)(T+1)(T-3)(T+3)$. The gcd computations then give us: $\hat{V}_3(-1) = -1$, $\hat{V}_3(1) = 1$, $\hat{V}_3(-3) = -1$, and $\hat{V}_3(3) = 1$. By interpolating we finally obtain $\hat{V}_3(T) = -1/12T^3 + 13/12T$.

Of course in practice, computations are not really handled in $\bar{\mathbb{K}}$. Instead we appeal classical techniques of computer algebra: for each irreducible factor $\hat{Q}_l$ of $\hat{Q}$, we do the above computations with taking a as the residue class of z in $\mathbb{K}[z]/(\hat{Q}_l(z))$, and finally we recover the result by means of the Chinese remainder theorem.

4.4. **Cleaning Step.** The input of the ith cleaning step is the univariate representation $\hat{Q}, \hat{V}_r, \ldots, \hat{V}_n$ of $\sqrt{\mathcal{K}_i + (f_{i+1})}$ seen in $\mathbb{K}[x_r, \ldots, x_n]$ with primitive element x_r. The output is the univariate representation $\check{Q}, \check{V}_r, \ldots, \check{V}_n$ of $\sqrt{\mathcal{K}_i + (f_{i+1})} : g^\infty$ with the same primitive element x_r.

Proposition 4.11. *Let $e = \gcd(\hat{Q}, g(0, \ldots, 0, \hat{V}_r, \ldots, \hat{V}_n))$, then we have that $\check{Q} = \hat{Q}/e$, and that $\check{V}_j$ is the remainder of $\hat{V}_j$ divided by $\check{Q}$.*

Proof. The proof follows from the following straightforward calculations:

$$\begin{aligned}\sqrt{\mathcal{K}_i + (f_{i+1})} : g^\infty &= (\hat{Q}(x_r), x_{r+1} - \hat{V}_{r+1}(x_r), \ldots, x_n - \hat{V}_n(x_r)) : g^\infty \\ &= (\hat{Q}(x_r), x_{r+1} - \hat{V}_{r+1}(x_r), \ldots, x_n - \hat{V}_n(x_r)) : e(x_r)^\infty \\ &= (\check{Q}(x_r), x_{r+1} - \check{V}_{r+1}(x_r), \ldots, x_n - \check{V}_n(x_r)).\end{aligned}$$

□

Example 4.12. The first cleaning step in the resolution of Example 4.1 goes as follows: the gcd computation leads to $e = T^2 - 4T + 3$, and thus we get $\check{Q} = T^2 + 4T + 3$, $\check{V}_2 = T$, and $\check{V}_3 = -1$.

4.5. **Example 4.1 Continued.** Let us carry on with the resolution of Example 4.1. In Example 4.12, we have obtained that $\mathcal{J}_2 = (x_2^2 + 4x_2 + 3, x_3 + 1) + (x_1)$. The second lifting step gives us that $\mathcal{K}_2 = (x_2^2 + 4x_2 + 3 + x_1^2, x_3 + 1)$, and then the second intersection step yields $\sqrt{\mathcal{K}_2 + (f_3)} = (x_1^2 - x_1, x_2 + 3 - x_1, x_3 + 1)$. Finally after the second and last cleaning step, we obtain $\mathcal{J}_3 = (x_1^2 - x_1, x_2 + 3 - x_1, x_3 + 1)$. We get the solutions of the system of Example 4.1 by changing the variables back.

4.6. **Computation of the Multiplicities.** At the last intersection step, that is when $i = n - 1$, the multiplicity of a zero of $\mathcal{K}_{n-1} + (f_n)$ can be read off from the multiplicity of its coordinate x_1 as a zero of the polynomial χ_0 defined in (4.2) (see [16, Chapter 4, Proposition 2.7] for instance). Since the primary components of $\mathcal{I}_n = (\mathcal{K}_{n-1} + (f_n)) : g^\infty$ are a subset of the ones of $\mathcal{K}_{n-1} + (f_n)$, we thus obtain the multiplicities of the zeros of $\mathcal{I}_n$. As announced in the introduction, these multiplicities are actually computed by the Kronecker solver without any extra cost.

Example 4.13. Let $n = 3$, $f_1 = 2x_2^2 + x_3^2 + x_1x_2 + x_1x_3 + 3x_2x_3 + x_2 + x_3$, $f_2 = x_1^2 + 3x_2^2 + x_3^2 + 4x_1x_2 + 2x_1x_3 + 2x_2x_3$, $f_3 = x_1^2 + 4x_2^2 + 3x_3^2 + 4x_1x_2 + 2x_1x_3 + 6x_2x_3$, and $g = 1$. Properties (A_1)–(A_{12}) hold. We enter the last intersection step with

the following Kronecker representation of $\mathcal{K}_2$:

$$\begin{aligned}\tilde{Q} &= T^4 + (2/3 + 5/3x_1)T^3 + (1/3 + 2/3x_1 + 7/6x_1^2)T^2 \\ &\quad + (1/3x_1 + 1/3x_1^2 + 1/3x_1^3)T + 1/6x_1^2, \\ \tilde{W}_2 &= (-2/3 - 5/3x_1)T^3 - (2/3 + 4/3x_1 + 7/3x_1^2)T^2 \\ &\quad - (x_1 + x_1^2 + x_1^3)T - 2/3x_1^2, \\ \tilde{W}_3 &= (-2/3 + 1/3x_1)T^3 + (2/3 - 4/3x_1 + 1/3x_1^2)T^2 \\ &\quad + (x_1 - x_1^2 - 1/3x_1^3)T + 2/3x_1^2 - 2/3x_1^3 - 1/3x_1^4.\end{aligned}$$

Then we compute the following irreducible factorization of χ_0 as defined in Proposition 4.9:

$$\chi_0 = 2/9x_1^4(5x_1^4 - 8x_1^3 + 16x_1^2 - 8x_1 + 12).$$

This way, we obtain that $(0, 0, 0)$ is a solution of multiplicity 4, and that there are 4 other simple solutions.

Appendix A. Proof of Theorem 2.9

We carry on with the notation and conventions used in Section 2.4, and we introduce the following block notation:

$$M = \begin{pmatrix} M_{1,1} & M_{1,2} \\ M_{2,1} & M_{2,2} \end{pmatrix},$$

with $M_{1,1}$ of size $r \times r$; Id_r will represent the $r \times r$ identity matrix.

Lemma A.1. *Assume that $\mathcal{I}$ is unmixed and that M is in one of the following three forms:*

$$\begin{pmatrix} \mathrm{Id}_r & 0 \\ M_{2,1} & \mathrm{Id}_{n-r} \end{pmatrix}, \begin{pmatrix} M_{1,1} & 0 \\ 0 & \mathrm{Id}_{n-r} \end{pmatrix}, \text{ or } \begin{pmatrix} \mathrm{Id}_r & 0 \\ 0 & M_{2,2} \end{pmatrix}.$$

(a) *$\mathcal{I}$ is in Noether position (respectively, general Noether position) if, and only if, $\mathcal{I}_M$ is in Noether position (respectively, general Noether position).*
(b) *$\delta_M = \delta$.*

Proof. In the first two cases, part (a) can be straightforwardly verified from the definitions of the Noether positions, whereas the third case follows from Proposition 1.3 (respectively, Proposition 1.17). Since, in the three cases, M defines an isomorphism of $\mathbb{K}[x_1, \ldots, x_n]$ that leaves $\mathbb{A}$ globally unchanged and that sends $\mathcal{I}$ to $\mathcal{I}_M$, we clearly have that $\delta_M = \delta$. □

Remark that δ is finite and positive. If $x_1, \ldots, x_r$ are algebraically dependent modulo $\mathcal{I}_M$ then $\mathcal{I}'_M = (1)$, whence $\mathbb{B}'_M = 0$ and $\delta_M = 0$. In this situation, the theorem trivially holds, so that we can assume from now that $x_1, \ldots, x_r$ are algebraically independent modulo $\mathcal{I}_M$. In this situation δ_M is finite since $x_{r+1}, \ldots, x_n$ are necessarily algebraic over $\mathbb{A}$ modulo $\mathcal{I}_M$ thanks to Theorem 1.12(b).

Claim A.2. *Without loss of generality, we can assume from the outset that*

$$M = \begin{pmatrix} M_{1,1} & M_{1,2} \\ 0 & \mathrm{Id}_{n-r} \end{pmatrix}.$$

Proof. Since M is invertible, the rank of the submatrix $\begin{pmatrix} M_{1,1} & M_{1,2} \end{pmatrix}$ is r, so that there exists a $(n-r) \times r$ matrix N such that $M_{1,1} - M_{1,2}N$ is invertible. Then a straightforward calculation gives us that

$$M = \begin{pmatrix} M_{1,1} - M_{1,2}N & M_{1,2} \\ M_{2,1} - M_{2,2}N & M_{2,2} \end{pmatrix} \begin{pmatrix} \mathrm{Id}_r & 0 \\ N & \mathrm{Id}_{n-r} \end{pmatrix}.$$

Thanks to Lemma A.1, we can assume from the outset that $M_{1,1}$ is invertible. And since we have that

$$M = \begin{pmatrix} \mathrm{Id}_r & 0 \\ M_{2,1}M_{1,1}^{-1} & \mathrm{Id}_{n-r} \end{pmatrix} \begin{pmatrix} M_{1,1} & M_{1,2} \\ 0 & M_{2,2} - M_{2,1}M_{1,1}^{-1}M_{2,1} \end{pmatrix},$$

we can now assume that $M_{2,1} = 0$, thanks to Lemma A.1 again. Finally the claim follows by using Lemma A.1 once more time in order to reach $M_{2,2} = \mathrm{Id}_{n-r}$. □

Let $y_1, \ldots, y_r$ be new variables, and let

$$\mathbb{A}_y = \mathbb{K}[y_1, \ldots, y_r], \quad \mathbb{A}'_y = \mathbb{K}(y_1, \ldots, y_r).$$

For each $i \in \{1, \ldots, r\}$, we introduce the linear form

$$l_i = y_i - (\omega_{i,1}x_1 + \cdots + \omega_{i,n}x_n) \in \mathbb{K}[y_1, \ldots, y_r, x_1, \ldots, x_n],$$

where $\omega_{i,j}$ stands for the (i,j)th entry of M^{-1}. For each $i \in \{0, \ldots, r\}$, we write $\mathcal{I}_i$ for the ideal $\mathcal{I} + (l_1, \ldots, l_i)$ of $\mathbb{K}[y_1, \ldots, y_r, x_1, \ldots, x_n]$. We define $\mathcal{I}'_i$ as the extension of $\mathcal{I}_i$ to $\mathbb{A}'_y[x_1, \ldots, x_n]$, and let:

$$\mathbb{B}_i = \mathbb{K}[y_1, \ldots, y_r, x_1, \ldots, x_n]/\mathcal{I}_i \text{ and } \mathbb{B}'_i = \mathbb{A}'_y[x_1, \ldots, x_n]/\mathcal{I}'_i.$$

We define δ_i as the dimension of the $\mathbb{A}'_y(x_1, \ldots, x_{r-i})$-vector space

$$\mathbb{B}''_i = \mathbb{A}'_y(x_1, \ldots, x_{r-i})[x_{r-i+1}, \ldots, x_n]/\mathcal{I}''_i,$$

where $\mathcal{I}''_i$ represents the extension of $\mathcal{I}'_i$ to $\mathbb{A}'_y(x_1, \ldots, x_{r-i})[x_{r-i+1}, \ldots, x_n]$.

It is straightforward to check that $x_1, \ldots, x_r, y_{i+1}, \ldots, y_r$ are algebraically independent modulo $\mathcal{I}_i$, and that $x_{r+1}, \ldots, x_n, y_1, \ldots, y_i$ are generally integral over

$$\mathbb{K}[x_1, \ldots, x_r, y_{i+1}, \ldots, y_r]$$

modulo $\mathcal{I}_i$ by Proposition 1.17. From Theorem 1.12(a) we deduce that $\dim(\mathcal{I}_i) = 2r - i$. Furthermore, by means of Proposition 1.22, it can be verified that the unmixedness of $\mathcal{I}$ implies the one of $\mathcal{I}_i$. This way, we obtain from Proposition 2.2(a) that l_{i+1} is a nonzerodivisor $\mathbb{B}_i$.

Claim A.3. *We have $\delta = \delta_0$ and $\delta_M = \delta_r$. The ideal $\mathcal{I}_r$ is in general Noether position if, and only if, $\mathcal{I} \circ M$ is in general Noether position.*

Proof. The former equality is straightforward while the latter equality and the equivalence between the Noether positions both follow from:

$$\begin{aligned} \mathcal{I}_r = (f \circ M(y_1, \ldots, y_r, x_{r+1}, \ldots, x_n) \mid f \in \mathcal{I}) + \\ (x_1 - (m_{1,1}y_1 + \cdots + m_{1,r}y_r + m_{1,r+1}x_{r+1} + \cdots + m_{1,n}x_n), \\ \ldots, \\ x_r - (m_{r,1}y_1 + \cdots + m_{r,r}y_r + m_{r,r+1}x_{r+1} + \cdots + m_{r,n}x_n)), \end{aligned}$$

where $m_{i,j}$ stands for the (i,j)th entry of M. □

Claim A.3 implies that the theorem reformulates into: (a) $\delta_r \leq \delta_0$, and (b) the equality holds if, and only if, $\mathcal{I}_r$ is in general Noether position.

It is a classical fact that the primes associated to $\mathcal{I}'_i$ correspond to the ones of $\mathcal{I}_i$ that properly extend to $\mathbb{A}'_y[x_1, \ldots, x_n]$ (see [18, Chapter 3, Theorem 3.10(d)], for instance). Let $\mathcal{P}$ be a prime associated to $\mathcal{I}_i$ such that its extension $\mathcal{P}'$ to $\mathbb{A}'_y[x_1, \ldots, x_n]$ is proper. Since $y_1, \ldots, y_r$ are algebraically independent modulo $\mathcal{P}$, we can find a subset S of $\{x_1, \ldots, x_n\}$ of cardinality $r - i$ such that $y_1, \ldots, y_r$ and the elements of S are algebraically independent modulo $\mathcal{P}$ by [45, Chapter VIII, Section 1, Theorem 1.1]. The elements of S are algebraically independent over $\mathbb{A}'_y$ modulo $\mathcal{P}'$, and that the variables outside of S are algebraic over $\mathbb{A}'_y(S)$ modulo $\mathcal{P}'$. It follows that $\dim(\mathcal{P}') = r - i$ hence that $\mathcal{I}'_i$ is unmixed of dimension either $r - i$

or -1. But since we have assumed that $\mathcal{I}'_M \neq (1)$, we have that $\mathcal{I}'_r \neq (1)$, whence $\dim(\mathcal{I}'_i) = r - i$ for all $i \in \{1, \ldots, r\}$. This way, we obtain from Proposition 2.2(a) that l_{i+1} is a nonzerodivisor in $\mathbb{B}'_i$.

Claim A.4. *Without loss of generality, we can assume that $\mathcal{I}'_i$ is in general Noether position, for all $i \in \{0, \ldots, r\}$.*

Proof. We are going to exhibit a $\mathbb{K}$-linear change of the variables that preserves δ, and the general Noether position of $\mathcal{I}$. Of course the general Noether position of $\mathcal{I}$ implies the one of $\mathcal{I}'_0$. Since l_{i+1} is a nonzerodivisor in $\mathbb{B}'_i$, we can use Proposition 2.2(b) successively with $f = l_1, \ldots, f = l_r$ in order to construct a matrix

$$M' = \begin{pmatrix} M'_{1,1} & 0 \\ 0 & \mathrm{Id}_{n-r} \end{pmatrix}$$

such that $\mathcal{I}'_i \circ M'$ is in general Noether position for all $i \in \{1, \ldots, r\}$. For each $i \in \{1, \ldots, r\}$, we let

$$l'_i = y_i - (\omega'_{i,1} x_1 + \cdots + \omega'_{i,n} x_n) \in \mathbb{A}[y_1, \ldots, y_r, x_1, \ldots, x_n],$$

where $\omega'_{i,j}$ stands here for the (i,j)th entry of $M^{-1}M'$. By construction we have that $\mathcal{I} \circ M' + (l'_1, \ldots, l'_i) = \mathcal{I}_i \circ M'$ to $\mathbb{A}'_y[x_1, \ldots, x_n]$, so that Claim A.2 allows us to replace $\mathcal{I}$ by $\mathcal{I} \circ M'$ and M by $M'^{-1}M$ from the outset in the theorem. □

In order to prove that $\delta_r \leq \delta_0$, we prove the following stronger statement:

Claim A.5. *For all $i \in \{0, \ldots, r-1\}$, we have that $\delta_{i+1} \leq \delta_i$.*

Proof. Proposition 2.7 applied with $\mathcal{I}'_i$ gives us that δ_{i+1} equals to the degree in x_{r-i} of the constant coefficient of the characteristic polynomial of l_{i+1} modulo $\mathcal{I}'_i$. The conclusion thus follows from Theorem 1.27(b). □

The proof of part (a) is now completed. If $\mathcal{I}_M$ is in general Noether position, then part (a) applied with $\mathcal{I}_M$ and M^{-1} yields $\delta \leq \delta_M$, whence $\delta = \delta_M$. Conversely, if the latter equality holds then we have to prove that $\mathcal{I}_r$ is in general Noether position in order to complete the proof of part (b), and thus the proof of the theorem. To this aim, we are to show the following stronger statement:

Claim A.6. *If $\delta = \delta_M$ then $\mathcal{I}_i$ is in general Noether position, for all $i \in \{0, \ldots, r-1\}$.*

Proof. The general Noether position of $\mathcal{I}$ implies the one of $\mathcal{I}_0$. By induction, assume that $\mathcal{I}_i$ is in general Noether position for some $i \geq 0$. We can use Proposition 2.7 with $\mathcal{I}_i$ and l_{i+1}. Since Claim A.5 implies that $\delta_{i+1} = \delta_i$, we deduce that the constant coefficient χ_0 of the characteristic polynomial of l_{i+1} in $\mathbb{B}''_i$ has degree δ_i in x_{r-i}. Since Theorem 1.27(b) implies that $\deg(\chi_0) \leq \delta_i$, we deduce from Lemma 2.1(a) that x_{r-i} is generally integral over $\mathbb{K}[y_1, \ldots, y_r, x_1, \ldots, x_{r-i-1}]$ modulo $\mathcal{I}_{i+1}$. By Proposition 1.7(b) we finally get that $\mathcal{I}_{i+1}$ is in general Noether position. □

References

1. M.-E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann, *Zeros, multiplicities, and idempotents for zero-dimensional systems*, Algorithms in Algebraic Geometry and Applications. Proceedings of MEGA'94, Progress in Mathematics, vol. 143, Birkhäuser, 1996, pp. 1–15.
2. B. Bank, M. Giusti, J. Heintz, and G. M. Mbakop, *Polar varieties, real equation solving, and data structures: the hypersurface case*, J. Complexity **13** (1997), no. 1, 5–27.
3. ———, *Polar varieties and efficient real elimination*, Math. Z. **238** (2001), no. 1, 115–144.
4. B. Bank, M. Giusti, J. Heintz, and L. M. Pardo, *Generalized polar varieties and an efficient real elimination procedure*, Kybernetika (Prague) **40** (2004), no. 5, 519–550.
5. T. Becker and V. Weispfenning, *Gröbner bases. A computational approach to commutative algebra*, Graduate Texts in Mathematics, vol. 141, Springer-Verlag, 1993.

6. A. Bostan, G. Lecerf, B. Salvy, É. Schost, and B. Wiebelt, *Complexity issues in bivariate polynomial factorization*, Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation, ACM, 2004, pp. 42–49.
7. N. Bruno, J. Heintz, G. Matera, and R. Wachenchauzer, *Functional programming concepts and straight-line programs in computer algebra*, Math. Comput. Simulation **60** (2002), no. 6, 423–473.
8. P. Bürgisser, M. Clausen, and M. A. Shokrollahi, *Algebraic complexity theory*, Springer-Verlag, 1997.
9. B. Castaño, J. Heintz, J. Llovet, and R. Martínez, *On the data structure straight-line program and its implementaion in symbolic computation*, Math. Comput. Simulation **51** (2000), no. 5, 497–528.
10. D. Castro, M. Giusti, J. Heintz, G. Matera, and L. M. Pardo, *The hardness of polynomial equation solving*, Found. Comput. Math. **3** (2003), no. 4, 347–420.
11. D. Castro, J. L. Montaña, L. M. Pardo, and J. San Martín, *The distribution of condition numbers of rational data of bounded bit length*, Found. Comput. Math. **2** (2002), no. 1, 1–52.
12. D. Castro, L. M. Pardo, K. Hägele, and J. E. Morais, *Kronecker's and Newton's approaches to solving: a first comparison*, J. Complexity **17** (2001), no. 1, 212–303.
13. D. Castro, L. M. Pardo, and J. San Martín, *Systems of rational polynomial equations have polynomial size approximate zeros on the average*, J. Complexity **19** (2003), no. 2, 161–209.
14. G. Chèze and G. Lecerf, *Lifting and recombination techniques for absolute factorization*, manuscript, Université de Versailles Saint-Quentin-en-Yvelines, 2005.
15. D. A. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra*, second ed., Undergraduate Texts in Mathematics, Springer-Verlag, 1997.
16. ———, *Using algebraic geometry*, second ed., Graduate Texts in Mathematics, Springer-Verlag, 2005.
17. M. Demazure, *Réécriture et bases standard*, Notes informelles de calcul formel. Centre de Mathématiques, École polytechnique, Palaiseau, France, 1985, `http://www.stix.polytechnique.fr/publications/1984-1994.html`.
18. D. Eisenbud, *Commutative algebra. With a view toward algebraic geometry*, Graduate Texts in Mathematics, Springer-Verlag, 1995.
19. N. Fitchas, M. Giusti, and F. Smietanski, *Sur la complexité du théorème des zéros*, Approximation and optimization in the Caribbean, II (Havana, 1993), Approx. Optim., vol. 8, Lang, Frankfurt am Main, 1995, pp. 274–329.
20. J. von zur Gathen and J. Gerhard, *Modern computer algebra*, second ed., Cambridge University Press, 2003.
21. P. Gaudry and É. Schost, *Modular equations for hyperelliptic curves*, Math. Comp. **74** (2005), no. 249, 429–454.
22. M. Giusti, K. Hägele, J. Heintz, J. L. Montaña, J. E. Morais, and L. M. Pardo, *Lower bounds for Diophantine approximations*, J. Pure Appl. Algebra **117/118** (1997), 277–317.
23. M. Giusti, K. Hägele, G. Lecerf, J. Marchand, and B. Salvy, *The projective Noether Maple package: computing the dimension of a projective variety*, J. Symbolic Comput. **30** (2000), no. 3, 291–307.
24. M. Giusti and J. Heintz, *La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial*, Computational algebraic geometry and commutative algebra (Cortona, 1991), Sympos. Math., XXXIV, Cambridge Univ. Press, 1993, pp. 216–256.
25. ———, *Kronecker's smart, little black boxes*, Foundations of computational mathematics (Oxford, 1999), London Math. Soc. Lecture Note Ser., vol. 284, Cambridge Univ. Press, 2001, pp. 69–104.
26. M. Giusti, J. Heintz, J. E. Morais, J. Morgenstern, and L. M. Pardo, *Straight-line programs in geometric elimination theory*, J. Pure Appl. Algebra **124** (1998), no. 1-3, 101–146.
27. M. Giusti, J. Heintz, J. E. Morais, and L. M. Pardo, *When polynomial equation systems can be "solved" fast?*, Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995), Lecture Notes in Comput. Sci., vol. 948, Springer-Verlag, 1995, pp. 205–231.
28. ———, *Le rôle des structures de données dans les problèmes d'élimination*, C. R. Acad. Sci. Paris Sér. I Math. **325** (1997), no. 11, 1223–1228.
29. M. Giusti, J. Heintz, and J. Sabia, *On the efficiency of effective Nullstellensätze*, Comput. Complexity **3** (1993), no. 1, 56–95.
30. M. Giusti, G. Lecerf, and B. Salvy, *A Gröbner free alternative for polynomial system solving*, Journal of Complexity **17** (2001), no. 1, 154–211.
31. M. Giusti and É. Schost, *Solving some overdetermined polynomial systems*, Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation, ACM, 1999, pp. 1–8.

32. G.-M. Greuel and G. Pfister, *A Singular introduction to commutative algebra*, Springer-Verlag, 2002.
33. K. Hägele, *Intrinsic height estimates for the Nullstellensatz*, Ph.D. thesis, Universidad de Cantabria, Santander, Spain, 1998.
34. K. Hägele, J. E. Morais, L. M. Pardo, and M. Sombra, *On the intrinsic complexity of the arithmetic Nullstellensatz*, J. Pure Appl. Algebra **146** (2000), no. 2, 103–183.
35. J. Heintz, T. Krick, S. Puddu, J. Sabia, and A. Waissbein, *Deformation techniques for efficient polynomial equation solving*, J. Complexity **16** (2000), no. 1, 70–109.
36. J. Heintz, G. Matera, L. M. Pardo, and R. Wachenchauzer, *The intrinsic complexity of parametric elimination methods*, Electronic J. of SADIO **1** (1998), no. 1, 37–51.
37. J. Heintz, G. Matera, and A. Waissbein, *On the time-space complexity of geometric elimination procedures*, Appl. Algebra Engrg. Comm. Comput. **11** (2001), no. 4, 239–296.
38. R. A. Horn and C. R. Johnson, *Topics in matrix analysis*, Cambridge University Press, 1994, Corrected reprint of the 1991 original.
39. G. Jeronimo, T. Krick, J. Sabia, and M. Sombra, *The computational complexity of the Chow form*, Found. Comput. Math. **4** (2004), no. 1, 41–117.
40. G. Jeronimo, S. Puddu, and J. Sabia, *Computing Chow forms and some applications*, J. Algorithms **41** (2001), no. 1, 52–68.
41. G. Jeronimo and J. Sabia, *Probabilistic equidimensional decomposition*, C. R. Acad. Sci. Paris Sér. I Math. **331** (2000), no. 6, 485–490.
42. ———, *Effective equidimensional decomposition of affine varieties*, J. Pure Appl. Algebra **169** (2002), no. 2-3, 229–248.
43. T. Krick and L. M. Pardo, *A computational method for Diophantine approximation*, Algorithms in algebraic geometry and applications (Santander, 1994), Progr. Math., vol. 143, Birkhäuser, 1996, pp. 193–253.
44. L. Kronecker, *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*, J. reine angew. Math. **92** (1882), 1–122.
45. S. Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, 2002.
46. G. Lecerf, *`Kronecker`, a `Magma` package for polynomial system solving*, `http://www.math.uvsq.fr/~lecerf`.
47. G. Lecerf, *Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions*, Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation, ACM, 2000, pp. 209–216.
48. G. Lecerf, *Une alternative aux méthodes de réécriture pour la résolution des systèmes algébriques*, Ph.D. thesis, École polytechnique, Palaiseau, France, 2001.
49. ———, *Quadratic Newton iteration for systems with multiplicity*, Found. Comput. Math. **2** (2002), no. 3, 247–293.
50. G. Lecerf, *Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers*, J. Complexity **19** (2003), no. 4, 564–596.
51. G. Lecerf, *Improved dense multivariate polynomial factorization algorithms*, manuscript, Université de Versailles Saint-Quentin-en-Yvelines, 2005.
52. ———, *Sharp precision in Hensel lifting for bivariate polynomial factorization*, Math. Comp. **75** (2006), 921–933.
53. L. Lehmann, *Polar varieties, real elimination and wavelet design*, 2004, Talk given at Dagstuhl Seminar 04061 on Real Computation and Complexity.
54. S. Mallat, *Foveal detection and approximation for singularities*, Appl. Comput. Harmon. Anal. **14** (2003), no. 2, 133–180.
55. G. Matera, *Probabilistic algorithms for geometric elimination*, Appl. Algebra Engrg. Comm. Comput. **9** (1999), no. 6, 463–520.
56. T. Mora, *Solving polynomial equation systems. I The Kronecker-Duval philosophy*, Encyclopedia of Mathematics and its Applications, vol. 88, Cambridge University Press, 2003.
57. J. E. Morais, *Resolución eficaz de sistemas de ecuaciones polinomiales*, Ph.D. thesis, Universidad de Cantabria, Santander, Spain, 1997.
58. L. M. Pardo, *How lower and upper complexity bounds meet in elimination theory*, Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995), Lecture Notes in Comput. Sci., vol. 948, Springer-Verlag, 1995, pp. 33–69.
59. L. M. Pardo and J. San Martin, *Deformation techniques to solve generalised Pham systems*, Theoret. Comput. Sci. **315** (2004), no. 2-3, 593–625.
60. F. Rouillier, *Solving zero-dimensional systems through the rational univariate representation*, Appl. Algebra Engrg. Comm. Comput. **6** (1996), 353–376.
61. M. Safey El Din, *Finding sampling points on real hypersurfaces is easier in singular situations*, Proceedings of Effective Methods in Algebraic Geometry (MEGA) 2005, 2005.

62. M. Safey El Din and É. Schost, *Properness defects of projections and computation of at least one point in each connected component of a real algebraic set*, Discrete Comput. Geom. **32** (2004), no. 3, 417–430.
63. É. Schost, *Computing parametric geometric resolutions*, Appl. Algebra Engrg. Comm. Comput. **13** (2003), no. 5, 349–393.
64. I. R. Shafarevich, *Basic algebraic geometry. 1 Varieties in projective space*, second ed., Springer-Verlag, 1994.
65. A. J. Sommese, J. Verschelde, and C. W. Wampler, *Solving polynomial systems equation by equation*, manuscript, 2005.
66. D. Wang, *Elimination practice. Software tools and applications*, Imperial College Press, London, 2004.

Clémence Durvye, Laboratoire de Mathématiques (UMR 8100 CNRS), Université de Versailles Saint-Quentin-en-Yvelines, 45 avenue des États-Unis, 78035 Versailles, France

E-mail address: Clemence.Durvye@math.uvsq.fr

Grégoire Lecerf, Poncelet Laboratory (UMI 2615 CNRS), Independent University of Moscow, 11 Bolshoi Vlasievskii per., Moscow 119002, Russia; and, Laboratoire de Mathématiques (UMR 8100 CNRS), Université de Versailles Saint-Quentin-en-Yvelines, 45 avenue des États-Unis, 78035 Versailles, France

E-mail address: Gregoire.Lecerf@math.uvsq.fr