Local Bézout Theorem for Henselian rings

M. Emilia Alonso, Henri Lombardi

Local Bézout Theorem for Henselian rings

M. Emilia Alonso* Henri Lombardi†

November 2016

Abstract

In this paper we prove what we call *Local Bézout Theorem* (Theorem 3.7). It is a formal abstract algebraic version, in the frame of Henselian rings and $\mathfrak{m}$-adic topology, of a well known theorem in the analytic complex case. This classical theorem says that, given an isolated point of multiplicity r as a zero of a local complete intersection, after deforming the coefficients of these equations we find in a sufficiently small neighborhood of this point exactly r isolated zeroes counted with multiplicities. Our main tools are, first the *border bases* [11], which turned out to be an efficient computational tool to deal with deformations of algebras. Second we use an important result of de Smit and Lenstra [7], for which there exists a constructive proof in [13]. Using these tools we find a very simple proof of our theorem, which seems new in the classical literature.

Keywords. Local Bézout Theorem, Henselian rings, Roots continuity, Stable computations, Constructive Algebra.

MSC 2010. primary 13J15; secondary 13P10, 13P15, 14Q20, 03F65

1 Introduction

In this paper we use ideas from computer algebra to prove what we call *Local Bézout Theorem* (Theorem 3.7). It is a formal abstract algebraic version, in the frame of Henselian rings and $\mathfrak{m}$-adic topology, of a well known theorem in the analytic complex case. This classical theorem says that, given an isolated point of multiplicity r as a zero of a local complete intersection, after deforming the coefficients of these equations we find in a sufficiently small neighborhood of this point exactly r isolated zeroes counted with multiplicities.

As far as we know the proofs of this classical result in the literature are essentially: by Arnold using powerfully the topological degree and Weierstrass theorems [4, section I-4.3], and another one that can be deduced from Griffiths-Harris [9, Residue Theorem, p. 656] using the theory of residues and its relationship with multiplicity.

Here we state and prove an *algebraic version* of this theorem in the setting of arbitrary Henselian rings and $\mathfrak{m}$-adic topology. We are somehow inspired by Arnold in [4, section I-4.3], exploiting an abstract version of Weierstrass division (in a Henselian ring) and introducing also an abstract version of which he called the "multilocal ring". Roughly speaking we consider a finitely presented $\mathbf{A}$-algebra, where $(\mathbf{A}, \mathfrak{m}, \mathbf{k})$ is a local Henselian ring such that the special point is a $\mathbf{k}$-algebra with an isolated zero of multiplicity r and we prove that the "multilocal ring" determined by this point is a free $\mathbf{A}$-module of rank r.

Our main tools are, first the *border bases* [11], which turned out to be an efficient computational tool to deal with deformations of algebras. Second we use an important result of de Smit and Lenstra [7], for which there exists a constructive proof in [13].

In Section 2.2 we recall the definition and main properties of border bases.

*Universidad Complutense, Madrid, España. mariemi@mat.ucm.es. http://www.mat.ucm.es/imi/People/Alonso_Garcia_MariaEmilia.htm Supported by Spanish GR MTM-2011-22435 and MTM-2014-55565.

†Univ. Bourgogne Franche-Comté, 25030 Besançon cedex, France. henri.lombardi@univ-fcomte.fr. http://hlombardi.free.fr/ Supported by Spanish GR MTM-2011-22435 and MTM-2014-55565.

We point out that, to obtain a fully algorithmic proof of our results, we rely on the constructive proof of the Multivariate Hensel Lemma (MHL for short) given in [2]. Also, in order to get true algorithms, fields are assumed to be discrete and local rings to be residually discrete.

The pure abstract algebraic form of Local Bézout Theorem is given in Theorems 3.3 and 3.7.

Going futher into details let us explain the form of Local Bézout Theorem we are interested in.

Assume $(\mathbf{A}, \mathfrak{m}, \mathbf{k})$ is a local normal domain, $f_1, \ldots, f_n \in \mathbf{A}[X_1, \ldots, X_n]$ and let

$$\mathbf{B} := \mathbf{A}[X_1, \ldots, X_n]/\langle f_1, \ldots, f_n\rangle \text{ and } \mathbf{C} = \mathbf{B}_{\mathfrak{m}+\langle \underline{x}\rangle} = \mathbf{A}[x_1, \ldots, x_n]_{\mathfrak{m}+\langle \underline{x}\rangle},$$

where $\langle \underline{x}\rangle = \langle x_1, \ldots, x_n\rangle$, x_i is $X_i \mod \langle f_1, \ldots, f_n\rangle$, and $f_i(\underline{0}) \in \mathfrak{m}$ for $i = 1, \ldots, n$. We denote by $\mathbf{K}$ the quotient field of $\mathbf{A}$. We assume $\mathbf{K}$ to be an algebraically closed field and therefore $\mathbf{A}$ to be a Henselian ring.

We assume that the $\mathbf{k}$-algebra

$$\overline{\mathbf{C}} := (\mathbf{k}[X_1, \ldots, X_n]/\langle \overline{f_1}, \ldots, \overline{f_n}\rangle)_{\langle \overline{x_1}, \ldots, \overline{x_n}\rangle} = \mathbf{k}[\overline{x_1}, \ldots, \overline{x_n}]_{\langle \overline{x_1}, \ldots, \overline{x_n}\rangle}$$

is zero-dimensional, where $\overline{f_i}$ (resp. $\overline{x_i}$) is the image of f_i (resp. x_i) by $\otimes_{\mathbf{A}}\mathbf{k}$.

Since $\mathbf{K}$ is algebraically closed it is plausible to speak about the continuity of the roots.

The algebraic form of Local Bézout Theorem (Theorem 3.7) says that there are finitely many zeroes of $(f_1, \ldots, f_n)$ above the residual zero $(0, \ldots, 0)$ (i.e., with coordinates in $\mathfrak{m}$), and the sum of their multiplicities equals the dimension r of $\overline{\mathbf{C}}$ as $\mathbf{k}$-vector space, i.e., the multiplicity of the residual zero. This implies also that the $\mathbf{K}$-algebra $\mathbf{C} \otimes_{\mathbf{A}} \mathbf{K}$ is finite free of rank r.

As application of the precedent sections, in section 4, we obtain, from the abstract theorem, the classical one. Here the characterization of border bases introduced by Bernard Mourrain in [11] reveals to be a crucial tool.

2 Useful tools

2.1 Theorem of de Smit and Lenstra

Theorem 2.1. (Theorem of de Smit & Lenstra, flatness, [7])
Let $\mathbf{A}$ *be an arbitrary commutative ring. If an* $\mathbf{A}$*-algebra*

$$\mathbf{B} = \mathbf{A}[X_1, \ldots, X_n]/\langle f_1, \ldots, f_n\rangle$$

is finite, then it is flat (so, it is free if $\mathbf{A}$ *is local).*

A constructive proof due to Claude Quitté is explained in [13].

2.2 Border bases

In this subsection, $\mathbf{A}$ is an arbitrary commutative ring.

(2.2.1) In the sequel we shall identify the semi-groups $X_1^{\mathbb{N}} \cdots X_n^{\mathbb{N}}$ and $\mathbb{N}^n$. A nonempty finite subset $\mathcal{B} \subset \mathbb{N}^n$ is called *closed by division* if for every X^γ, $X^{\gamma'}$, if $X^\gamma \in \mathcal{B}$ and $X^{\gamma'} \mid X^\gamma$ then $X^{\gamma'} \in \mathcal{B}$.
In the sequel any finite subset $\mathbb{N}^n$ denoted by $\mathcal{B}$ will be assumed nonempty and closed by division.
We call *border of* $\mathcal{B}$ the following finite subset of $\mathbb{N}^n$,

$$\partial\mathcal{B} := (X_1\mathcal{B} \cup \cdots \cup X_n\mathcal{B}) \setminus \mathcal{B}$$

(2.2.2) Let $\mathbf{A}$ be a ring, I a finitely generated ideal of $\mathbf{A}[X_1, \ldots, X_n] = \mathbf{A}[\underline{X}]$ and

$$\mathbf{B} := \mathbf{A}[\underline{X}]/I = \mathbf{A}'[x_1, \ldots, x_n]$$

(x_i the image of X_i in $\mathbf{B}$ and $\mathbf{A}'$ the image of $\mathbf{A}$). Given a finite subset $\mathcal{B} \subset \mathbb{N}^n$ as above, we call *rewriting rules for* $\mathbf{B}$ *w.r.t.* $\mathcal{B}$ a set of equalities in $\mathbf{B}$ as follows,

$$\left\{ x^\beta = \sum\nolimits_{\alpha\in\mathcal{B}} h_{\beta,\alpha} x^\alpha : \beta \in \partial\mathcal{B} \right\} \text{ where } h_{\beta,\alpha} \in \mathbf{A} \tag{1}$$

Formally, we define the rewriting rules as being the polynomials $h_\beta(\underline{X}) = X^\beta - \sum_{\alpha\in\mathcal{B}} h_{\beta,\alpha} x^\alpha$. The equalities (1) mean precisely that the $h_\beta(\underline{X})$'s belong to the ideal I.
If $\mathbf{B}$ defined as above has rewriting rules w.r.t. to $\mathcal{B}$, then the set $\{ x^\alpha : \alpha \in \mathcal{B} \}$ generate $\mathbf{B}$ as $\mathbf{A}$-module. In particular $\mathbf{B}$ is a finite $\mathbf{A}$-module.

(2.2.3) We call $(\mathcal{B}, (h_\beta)_{\beta\in\partial\mathcal{B}})$ a *border basis* of $\mathbf{B}/\mathbf{A}$ if

- $\mathcal{B}$ is closed by division.
- the $h_\beta(\underline{X})$'s are rewriting rules in $\mathbf{B}$ w.r.t. $\mathcal{B}$ and
- $(x^\alpha)_{\alpha\in\mathcal{B}}$ is a basis of $\mathbf{B}$ as an $\mathbf{A}$-module.

This implies in particular that $\mathbf{A}' = \mathbf{A}$.
Given any morphism $\rho : \mathbf{A} \to \mathbf{C}$ of rings a border basis $(\mathcal{B}, (h_\beta)_{\beta\in\partial\mathcal{B}})$ of $\mathbf{B}/\mathbf{A}$ is transformed by ρ in a border basis $(\mathcal{B}, (\rho(h_\beta))_{\beta\in\partial\mathcal{B}})$ of $(\mathbf{B}\otimes_{\mathbf{A}}\mathbf{C})/\mathbf{C}$.

(2.2.4) Given a ring $\mathbf{A}$ and $\mathcal{B} \subset \mathbb{N}^n$ (nonempty and closed by division as in (2.2.1)), assume be given a set of "abstract" rewriting rules (1) (without $\mathbf{B}$). Define $I := \left\langle X^\beta - \sum_{\alpha\in\mathcal{B}} h_{\beta,\alpha} X^\alpha : \beta \in \partial\mathcal{B} \right\rangle$ and $\mathbf{B} := \mathbf{A}[\underline{X}]/I$. We can ask wether $\mathbf{B}$ is a free $\mathbf{A}$-module of basis $\{x^\alpha : \alpha \in \mathcal{B}\}$. I.e., do we get a border basis of $\mathbf{B}$? For this, let us denote by $\mathrm{Span}_{\mathbf{A}}(\mathcal{B})$ the free $\mathbf{A}$-module generated by the terms of $\mathcal{B}$, and for every i

$$\mu_{X_i} : \mathrm{Span}_{\mathbf{A}}(\mathcal{B}) \to \mathrm{Span}_{\mathbf{A}}(\mathcal{B})$$

the linear map given by

$$\mu_{X_i}(X^\alpha) = \begin{cases} X_i X^\alpha & \text{if } X_i X^\alpha \in \mathcal{B}, \\ \sum_{\alpha\in\mathcal{B}} h_{\beta,\alpha} X^\alpha & \text{if } X_i X^\alpha = X^\beta \in \partial\mathcal{B}. \end{cases}$$

Now let Λ_i denote the matrix of μ_{X_i} w.r.t. the basis $\mathcal{B}$ of the free $\mathbf{A}$-module $\mathrm{Span}_{\mathbf{A}}(\mathcal{B})$, then, see [6] and [11]

Theorem 2.2. $\mathbf{B}$ *is a free* $\mathbf{A}$*-module with basis* $\{x^\alpha : \alpha \in \mathcal{B}\}$ *iff*

$$\Lambda_i \Lambda_j = \Lambda_j \Lambda_i \ \textit{for } i, j = 1, \ldots, n.$$

(2.2.5) In the particular case in which $\mathbf{A}$ is a discrete field $\mathbf{k}$ and $\mathbf{B}$ is an Artinian $\mathbf{k}$-algebra, the Gröbner basis algorithm provides a border basis of $\mathbf{B}$. Indeed, it is well known that, w.r.t. to an admissible monomial ordering, the monomials "under the staircase" form a $\mathbf{k}$-basis $\mathcal{B}$ of $\mathbf{B}$, and the rewriting rules are given by computing the remainder of the division of X^β by the Gröbner basis (for $\beta \in \partial\mathcal{B}$). Mourrain in [11] introduced an algorithm to compute a border basis of an Artinian $\mathbf{k}$-algebra without using the theory of Gröbner basis and requiring for $\mathcal{B}$ a weaker property than to be closed by division.

(2.2.6) One important fact with border bases is that they are more suitable for computational purposes specially when data is given by approximate values. Another one is that they can be useful in more general cases when Gröbner bases over rings are not available or not easy to manage.

3 The Bézout local theorem

Let us recall two theorems in [3].

Theorem 3.1. ([3, Theorem 1]) *Let $(\mathbf{A}, \mathfrak{m}, \mathbf{k})$ be a local Henselian ring.*
Let $f_1, \ldots, f_m \in \mathbf{A}[X_1, \ldots, X_n] = \mathbf{A}[\underline{X}]$, $\overline{f_1}, \ldots, \overline{f_m}$ their images in $\mathbf{k}[\underline{X}]$,

$$\mathbf{B} := \mathbf{A}[\underline{X}]/\langle f_1, \ldots, f_m\rangle = \mathbf{A}[x_1, \ldots, x_n]$$

and

$$\overline{\mathbf{B}} := \mathbf{B}/\mathfrak{m}\mathbf{B} = \mathbf{k}[X_1, \ldots, X_n]/\langle \overline{f_1}, \ldots, \overline{f_m}\rangle = \mathbf{k}[\overline{x_1}, \ldots, \overline{x_n}].$$

Let $\mathbf{B}_1 := \mathbf{B}_{\mathfrak{m}+\langle \underline{x}\rangle}$, $\overline{\mathbf{B}_1} := \overline{\mathbf{B}}_{\langle \overline{x_1}, \ldots, \overline{x_n}\rangle}$ and assume $1 \leq \dim_{\mathbf{k}}(\overline{\mathbf{B}_1}) < \infty$.
Then the $\mathbf{A}$-algebra $\mathbf{B}_1$ is a finitely generated $\mathbf{A}$-module.

A domain $\mathbf{A}$ is called a DVR with uniformizing parameter p when every nonzero element of $\mathbf{A}$ is uniquely expressed in the form up^m for some $m > 0$ and $u \in \mathbf{A}^\times$. In this case $\mathbf{A}$ is local with radical $p\mathbf{A}$.

Theorem 3.2. ([3, Theorem 5]) *Let $(\mathbf{A}, \mathfrak{m}, \mathbf{k})$ be a Henselian DVR.*
Let $f_1, \ldots, f_n \in \mathbf{A}[X_1, \ldots, X_n] = \mathbf{A}[\underline{X}]$, $\overline{f_1}, \ldots, \overline{f_n}$ their images in $\mathbf{k}[\underline{X}]$,

$$\mathbf{B} := \mathbf{A}[\underline{X}]/\langle f_1, \ldots, f_n\rangle = \mathbf{A}[x_1, \ldots, x_n]$$

and

$$\overline{\mathbf{B}} := \mathbf{B}/\mathfrak{m}\mathbf{B} = \mathbf{k}[X_1, \ldots, X_n]/\langle \overline{f_1}, \ldots, \overline{f_n}\rangle = \mathbf{k}[\overline{x_1}, \ldots, \overline{x_n}].$$

Let $\mathbf{B}_1 := \mathbf{B}_{\mathfrak{m}+\langle \underline{x}\rangle}$, $\overline{\mathbf{B}_1} := \overline{\mathbf{B}}_{\langle \overline{x_1}, \ldots, \overline{x_n}\rangle}$ and assume $\dim_{\mathbf{k}}(\overline{\mathbf{B}_1}) = r \geq 1$.
Then the $\mathbf{A}$-algebra $\mathbf{B}_1$ is a free $\mathbf{A}$-module of rank r, whose basis is given by lifting any $\mathbf{k}$-basis of $\overline{\mathbf{B}}_1$.

We give first a result that implies a generalization and an important precision in Theorems 3.1 and 3.2 in case of a residually finite global complete intersection ($m = n$ and the residual algebra is finite): see corollary 3.5.

In the sequel we use the notation $\mathfrak{m}[\underline{X}]$ for the ideal of $\mathbf{A}[\underline{X}]$ generated by $\mathfrak{m}$ (the polynomials with coefficients in $\mathfrak{m}$) and $\mathfrak{m}+\langle \underline{X}\rangle$ for the ideal $\mathfrak{m}[\underline{X}]+\langle \underline{X}\rangle$ (the polynomials $\in \mathbf{A}[\underline{X}]$ with constant coefficient in $\mathfrak{m}$).

Theorem 3.3. *Let $(\mathbf{A}, \mathfrak{m}, \mathbf{k})$ be a local Henselian ring, $\mathbf{B} := \mathbf{A}[x_1, \ldots, x_n]$ be a finitely generated $\mathbf{A}$-algebra and set $\overline{\mathbf{B}} := \mathbf{B}/\mathfrak{m}\mathbf{B} = \mathbf{B} \otimes_A \mathbf{k}$ the residual algebra. Assume that $\overline{\mathbf{B}}$ is a nonzero finitely generated $\mathbf{k}$-vector space. Then it holds:*

1. *(a) There exists $s \in 1 + \mathfrak{m}\mathbf{B}$ s.t. the $\mathbf{A}$-algebra $\mathbf{B}[1/s]$ is a finitely generated $\mathbf{A}$-module.*
   (b) In case we know a border basis of $\overline{\mathbf{B}}$ as $\mathbf{k}$-algebra, its rewriting rules can be lifted, to provide, for a suitable $s \in 1 + \mathfrak{m}\mathbf{B}$, a system of generators of $\mathbf{B}[1/s]$ as an $\mathbf{A}$-module.
2. *Assume in addition that the $\mathbf{A}$-algebra $\mathbf{B}$ is presented with an equal number of generators and relations, that is $\mathbf{B} := \mathbf{A}[X_1, \ldots, X_n]/\langle f_1, \ldots, f_n\rangle = \mathbf{A}[x_1, \ldots, x_n]$.*
   (a) If $\dim_{\mathbf{k}}(\overline{\mathbf{B}}) = r \geq 1$, there exists $S \in 1+\mathfrak{m}[\underline{X}]$ s.t. letting $s = S(\underline{x})$, $\mathbf{B}[1/s]$ is a free $\mathbf{A}$-module of rank r.
   (b) More precisely, any border basis of the residual algebra $\overline{\mathbf{B}} = \overline{\mathbf{B}[1/s]}$ can be lifted with its rewriting rules to a border basis of $\mathbf{B}[1/s]$ with its rewriting rules.

Note. In order to be able to compute a $\mathbf{k}$-basis of $\overline{\mathbf{B}}$, we need a priori that $\mathbf{B}$ is finitely presented as an $\mathbf{A}$-algebra. So, in item *1 (a)* we do not assume that $\overline{\mathbf{B}}$ has a $\mathbf{k}$-basis, and in item *2* the hypothesis implies that we are able to compute a border basis of $\overline{\mathbf{B}}$.

An intuitive meaning of the first part of the statement of the theorem is that, when $\mathbf{A}$ is a domain with quotient field $\mathbf{K}$ and the polynomial system is residually zero-dimensional, inverting s "maps at infinity" all zeroes of I in $\mathbf{K}$ which are not integral over $\mathbf{A}$. We explain this intuition through Corollary 3.4. An $\mathbf{A}$-algebra is a commutative unital ring $\mathbf{E}$ with a ring morphism $\rho : \mathbf{A} \to \mathbf{E}$, in the sequel we use in this case the terminology "an $\mathbf{A}$-algebra $\rho : \mathbf{A} \to \mathbf{E}$".

Corollary 3.4. *Same hypotheses and notations as in Theorem 3.3 1. Assume moreover that* $\mathbf{B} := \mathbf{A}[X_1,\dots,X_n]/\langle f_1,\dots,f_m\rangle = \mathbf{A}[x_1,\dots,x_n]$ *and we are given an* $\mathbf{A}$*-algebra* $\rho : \mathbf{A} \to \mathbf{E}$ *and a zero* $(\xi_1,\dots,\xi_n,\zeta)$ *of* $\{f_1,\dots,f_m,ZS(\underline{X})-1\}$ *in* $\mathbf{E}$*. Then each* ξ_i *is integral over* $\rho(\mathbf{A})$*.*

Proof. Since $\mathbf{B}[1/s]$ is a finite $\mathbf{A}$-module, each x_i is integral over $\mathbf{A}$ in $\mathbf{B}[1/s]$: in fact x_i annihilates the characteristic polynomial of the matrix of multiplication by x_i with respect to a system of generators of $\mathbf{B}[1/s]$ as $\mathbf{A}$-module. The morphism ρ gives by factorization a morphism of $\mathbf{A}$-algebras $\mathbf{B}[1/s] \to \mathbf{E}$ mapping $(x_1,\dots,x_n,z)$ to $(\xi_1,\dots,\xi_n,\zeta)$. So each ξ_i annihilates a monic polynomial with coefficients in $\rho(\mathbf{A})$. □

Corollary 3.5. *Same hypotheses and notations as in Theorem 3.3 1, and in addition assume that the* $\mathbf{k}$*-algebra* $\overline{\mathbf{B}}$ *is local, more precisely that* $\overline{\mathbf{B}} = \overline{\mathbf{B}}_{\langle\overline{x_1},\dots,\overline{x_n}\rangle}$ *(this means that each* $\overline{x_i}$ *is nilpotent, or also that* $(0,\dots,0)$ *is the unique zero of* $\{\overline{f_1},\dots,\overline{f_m}\}$ *in an algebraic closure of* $\mathbf{k}$*).*

1. *There exists an* $s \in 1+\mathfrak{m}\mathbf{B}$ *such that* $\mathbf{B}[1/s] = \mathbf{B}_{\mathfrak{m}+\langle\underline{x}\rangle}$ *is a finitely generated* $\mathbf{A}$*-module.*
2. *If in addition* $\mathbf{B} := \mathbf{A}[X_1,\dots,X_n]/\langle f_1,\dots,f_n\rangle = \mathbf{A}[x_1,\dots,x_n]$*, then the* $\mathbf{A}$*-algebra* $\mathbf{B}_{\mathfrak{m}+\langle\underline{x}\rangle}$ *is a free* $\mathbf{A}$*-module of rank* r*, whose basis is given by lifting any* $\mathbf{k}$*-basis of* $\overline{\mathbf{B}}$ *with its rewriting rules.*

Proof. 1. First we note that $\overline{\mathbf{B}_{\mathfrak{m}+\langle\underline{x}\rangle}} = \overline{\mathbf{B}}_{\langle\overline{x_1},\dots,\overline{x_n}\rangle} = \overline{\mathbf{B}}$. We apply Theorem 3.3. We get an $s \in 1+\mathfrak{m}\mathbf{B}$ such that $\mathbf{B}[1/s]$ is a finitely generated $\mathbf{A}$-module. Since s is invertible in $\mathbf{B}_{\mathfrak{m}+\langle\underline{x}\rangle}$, we get an $\mathbf{A}$-morphism $\varphi : \mathbf{B}[1/s] \to \mathbf{B}_{\mathfrak{m}+\langle\underline{x}\rangle}$. We show that "$\varphi$ is a canonical isomorphism": the two localizations of $\mathbf{B}$ are the same one. This means that any element $c \in 1+\mathfrak{m}\mathbf{B}+\langle\underline{x}\rangle$ is invertible in $\mathbf{B}[1/s]$. Since $\overline{c}=1$ in $\overline{\mathbf{B}}_{\langle\overline{x_1},\dots,\overline{x_n}\rangle}$ and $\overline{\mathbf{B}} = \overline{\mathbf{B}}_{\langle\overline{x_1},\dots,\overline{x_n}\rangle}$, we get $\overline{c}=1$ in $\overline{\mathbf{B}[1/s]}$ and the result follows from Nakayama: the multiplication by c in $\mathbf{B}[1/s]$ is an $\mathbf{A}$-endomorphism which is residually onto, hence itself is onto and c is invertible in $\mathbf{B}[1/s]$.

2. We have the hypothesis of Theorem 3.3 *2* and $\mathbf{B}[1/s] = \mathbf{B}_{\mathfrak{m}+\langle\underline{x}\rangle}$. □

Corollary 3.6. *Same hypotheses and notation as in Corollary 3.4. Assume moreover that* $\overline{\mathbf{B}} = \overline{\mathbf{B}}_{\langle\overline{x_1},\dots,\overline{x_n}\rangle}$ *(as in Corollary 3.5 1). Then each* ξ_i *is "integral over* $\mathfrak{m}$*" (see the precise meaning in the proof).*

Proof. Since $\overline{x_i}$ is nilpotent, the multiplication $\mu_{\overline{x_i}}$ by $\overline{x_i}$ in $\overline{\mathbf{B}}$ is given by a lower triangular matrix M_i with zeroes on the diagonal (after a suitable change of basis as a $\mathbf{k}$-vector space). Since we have a generator system B of $\mathbf{B}[1/s]$ as an $\mathbf{A}$-module which is lifted from a border basis $\mathcal{B}$ of $\overline{\mathbf{B}}$, and since the rewriting rules are also lifted, the multiplication by x_i in $\mathbf{B}[1/s]$ can be expressed w.r.t. a generator system B' (obtained from B by lifting the above change of vector space basis) by a lifting of the above matrix M_i and the characteristic polynomial of this lifted matrix has the form $T^r + \sum_{j=0}^{r-1}\mu_{i,j}T^{r-j}$ with $\mu_{i,j} \in \mathfrak{m}^j$.
So, we get an equality in $\mathbf{E}$: $\xi_i^r + \sum_{j=0}^{r-1}\rho(\mu_{i,j})\xi_i^{r-j} = 0$ and $\mu_{i,j} \in \mathfrak{m}^j$. □

Proof of Theorem 3.3.
1. We set $\mathbf{B} = \mathbf{A}[X_1,\dots,X_n]/I$ for some ideal $I \subseteq \mathbf{A}[\underline{X}]$. As $\overline{\mathbf{B}}$ is a finitely generated nonzero $\mathbf{k}$-vector space, we can represent it as a quotient of some finitely presented nonzero $\mathbf{k}$-algebra

$$\mathbf{k}[X_1,\dots,X_n]/\langle\overline{f_1},\dots,\overline{f_m}\rangle$$

for some $f_i \in I$. So $\mathbf{B}$ is a quotient of the finitely presented $\mathbf{A}$-algebra

$$\mathbf{B}_0 = \mathbf{k}[X_1,\dots,X_n]/\langle f_1,\dots,f_m\rangle$$

whose residual $\mathbf{k}$-algebra $\overline{\mathbf{B}_0}$ is a $\mathbf{k}$-vector space with a finite $\mathbf{k}$-basis.
Hence w.l.o.g. we can assume that $\mathbf{B}$ is finitely presented. Hence $\overline{\mathbf{B}}$ has a border basis. There exists a finite set of monomials $\mathcal{B} \subset \mathbb{N}^n$ containing 1 and closed by division, such that $\{x^\alpha : \alpha \in \mathcal{B}\}$ is a $\mathbf{k}$-basis of $\overline{\mathbf{B}}$, and for $\beta \in \partial\mathcal{B}$

$$h_\beta^0(X) := X^\beta - \sum\nolimits_{\alpha\in\mathcal{B}} u_{\beta,\alpha}^0 X^\alpha \qquad (\text{with } u_{\beta,\alpha}^0 \in \mathbf{k})$$

are the corresponding rewriting rules.

Now we follow the constructions in the proof of [3, Theorem 1] (see Claim 4 in [3]). As $\langle \overline{f_1}, \dots, \overline{f_m} \rangle = \left\langle h^0_\beta : \beta \in \partial\mathcal{B} \right\rangle \subseteq \mathbf{k}[X_1, \dots, X_n]$, we have $h^0_\beta = \sum_{i=1}^m \overline{p_{i,\beta}}\ \overline{f_i}$, with some $p_{i,\beta} \in \mathbf{A}[\underline{X}]$. For $\beta \in \partial\mathcal{B}$ we put

$$H_\beta(\underline{X}) := \sum\nolimits_{i=1}^m p_{i,\beta} f_i \qquad (\text{so } \overline{H_\beta} = h^0_\beta).$$

Next we reduce these polynomials H_β with the following "formal rewriting rules"

$$\widetilde{h_\beta} := X^\beta - \sum\nolimits_{\alpha\in\mathcal{B}} \widetilde{u_{\beta,\alpha}} X^\alpha,$$

where $\widetilde{u_{\beta,\alpha}}$ are variables, whose suitable values in $\mathbf{A}$ we are looking for.

Following [3] and [1] we get

$$H_\beta = \sum\nolimits_{\beta'\in\partial\mathcal{B}} \widetilde{Q_{\beta,\beta'}} \widetilde{h_{\beta'}} + \widetilde{R_\beta} \tag{2}$$

for polynomials $\widetilde{Q_{\beta,\beta'}}((\widetilde{u_{\beta,\alpha}}), \underline{X}) \in \mathbf{A}[(\widetilde{u_{\beta,\alpha}})_{\beta\in\partial\mathcal{B},\alpha\in\mathcal{B}}, \underline{X}]$ and

$$\widetilde{R_\beta} = \sum\nolimits_{\alpha\in\mathcal{B}} \widetilde{R_{\beta,\alpha}} X^\alpha \qquad \text{with } \widetilde{R_{\beta,\alpha}}((\widetilde{u_{\beta,\alpha}})) \in \mathbf{A}[(\widetilde{u_{\beta,\alpha}})].$$

Moreover

$$\widetilde{\Delta}((\widetilde{u_{\beta,\alpha}}), \underline{X}) := \det((\widetilde{Q_{\beta,\beta'}})_{\beta,\beta'\in\partial\mathcal{B}}) \in 1 + \mathfrak{m}[(\widetilde{u_{\beta,\alpha}}), \underline{X}].$$

In [3] and [1] we proved that $(u^0_{\beta,\alpha})$ is an isolated simple zero of the system $\left\{\widetilde{R_{\beta,\alpha}} = 0\right\}$. Since $\mathbf{A}$ is Henselian, by MHL, there exists a unique solution $(u_{\beta,\alpha}) \in \mathbf{A}^{\partial\mathcal{B}\times\mathcal{B}}$ of the system $\left\{\widetilde{R_{\beta,\alpha}} = 0\right\}$ lifting the solution $(u^0_{\beta,\alpha}) \in \mathbf{k}^{\partial\mathcal{B}\times\mathcal{B}}$.

For $\beta \in \partial\mathcal{B}$, we define

$$\begin{aligned} h_\beta &:= X^\beta - \textstyle\sum_{\alpha\in\mathcal{B}} u_{\beta,\alpha} X^\alpha, \\ Q_{\beta,\beta'}(\underline{X}) &:= \widetilde{Q_{\beta,\beta'}}((u_{\beta,\alpha}), \underline{X}) \in \mathbf{A}[\underline{X}], \\ S(\underline{X}) &:= \widetilde{\Delta}((u_{\beta,\alpha}), \underline{X}) = \det((Q_{\beta,\beta'})_{\beta,\beta'\in\partial\mathcal{B}}) \in 1 + \mathfrak{m}[\underline{X}]. \end{aligned}$$

Equalities (2) give

$$H_\beta = \sum\nolimits_{\beta'\in\partial\mathcal{B}} Q_{\beta,\beta'} h_{\beta'}. \tag{3}$$

Let $s = S(\underline{x}) \in \mathbf{A}[\underline{x}] = \mathbf{B}$. The ideal $\langle f_1, \dots, f_m, SZ - 1\rangle \subseteq I \subseteq \mathbf{A}[\underline{X}, Z]$ contains polynomials h_β's for $\beta \in \mathcal{B}$ since $h_\beta \equiv ZSh_\beta$ and Sh_β is expressed from the $H_{\beta'}$'s using the cotransposed matrix of $(Q_{\beta,\beta'})_{\beta,\beta'\in\partial\mathcal{B}}$. As f_i belong to the ideal I, we get a well defined $\mathbf{A}$-algebra morphism

$$\begin{aligned} \Phi : \mathbf{C} = \mathbf{A}[\underline{X}]/\langle (h_\beta)_{\beta\in\partial\mathcal{B}}\rangle &\longrightarrow \mathbf{A}[\underline{X}, Z]/\langle I, SZ - 1\rangle = \mathbf{B}[1/s] \\ X_i &\longmapsto X_i \end{aligned}$$

As an $\mathbf{A}$-module, $\mathbf{C}$ is generated by the classes $X^\alpha \bmod J = \langle (h_\beta)_{\beta\in\partial\mathcal{B}}\rangle$ (for $\alpha \in \mathcal{B}$).

Moreover Φ is surjective because S has an inverse in $\Phi(\mathbf{C})$. Indeed $\Phi(\mathbf{C})$ is a finitely generated $\mathbf{A}$ module and the multiplication by S in $\Phi(\mathbf{C})$ is residually onto (it is the identity), therefore by Nakayama lemma the multiplication by S is itself onto on $\Phi(\mathbf{C})$.

As we get $\Phi(\mathbf{C}) = \mathbf{B}[1/s]$, $\mathbf{B}[1/s]$ is generated as $\mathbf{A}$-module by the lifting $\{x^\alpha; \alpha \in \mathcal{B}\}$ of $\mathcal{B}$ and the h_β's are rewriting rules for this generator system.

2. We have $\mathbf{B} = \mathbf{A}[X_1, \dots, X_n]/\langle f_1, \dots, f_n\rangle$. By item *1* we know that $\mathbf{B}[1/s]$ is a finitely generated $\mathbf{A}$-module for some $S(X) \in 1 + \mathfrak{m}[\underline{X}]$. We can apply the theorem of de Smit & Lenstra 2.1 to conclude that $\mathbf{B}[1/s]$ is a finite free $\mathbf{A}$-module. Clearly its rank is the same after $\otimes_{\mathbf{A}}\mathbf{k}$, so it is equal to the dimension

$r = \#\mathcal{B}$ of the $\mathbf{k}$-vector space $\overline{\mathbf{B}[1/s]} = \overline{\mathbf{B}}$. Since $\mathbf{B}[1/s]$ is generated by a lifting of $\mathcal{B}$, we conclude by saying that in a free module of rank r, any generator system of r elements is a basis.

On the other hand, since the generator system $\{x^\alpha : \alpha \in \mathcal{B}\}$ of the $\mathbf{A}$-module $\mathbf{C}$ is mapped by Φ to a basis of the $\mathbf{A}$-module $\mathbf{B}[1/s]$ with the same number of elements, we have that Φ is injective and therefore it is an isomorphism. This fact will be used in Section 4. In consequence we have finished the proof of the theorem. □

Our main concern is the following result in which item *3* generalizes [3, Theorem 11]. We point out that in [3, Theorem 11] we forgot to give as an hypothesis the fact that $\mathbf{A}$ is integrally closed in $\mathbf{K}$: the proof was given only for the case of a valuation domain and used implicitely the normality hypothesis in the general case.

Theorem 3.7. (Bézout local) *Let $(\mathbf{A}, \mathfrak{m}, \mathbf{k})$ be a Henselian local ring and $\mathbf{B} := \mathbf{A}[x_1, \ldots, x_n]$ a finitely generated $\mathbf{A}$-algebra. Let $\overline{\mathbf{B}} := \mathbf{B}/\mathfrak{m}\mathbf{B} = \mathbf{k}[\overline{x_1}, \ldots, \overline{x_n}]$ be the residual algebra. Assume that $\overline{\mathbf{B}}$ is finitely presented*[1] *as a $\mathbf{k}$-algebra and that $\dim_{\mathbf{k}} \overline{\mathbf{B}}_{\langle \overline{x_1}, \ldots, \overline{x_n}\rangle} = r \geq 1$ (this means that $(\underline{0})$ is an isolated residual zero of multiplicity r). Then $\mathfrak{m}\mathbf{B} + \langle x_1, \ldots, x_n\rangle$ (denoted as $\mathfrak{m} + \langle \underline{x}\rangle$) is a maximal ideal of $\mathbf{B}$ and we have:*

1. *(Pure algebraic form, without zeroes)*
   The $\mathbf{A}$-algebra $\mathbf{B}_{\mathfrak{m}+\langle \underline{x}\rangle}$ is a finitely generated $\mathbf{A}$-module: there exists an $u \in 1 + \mathfrak{m}\mathbf{B} + \langle \underline{x}\rangle$ such that
   $$\mathbf{B}[1/u] = \mathbf{B}_{\mathfrak{m}+\langle \underline{x}\rangle},\ \overline{\mathbf{B}}[1/\overline{u}] = \overline{\mathbf{B}}_{\langle \overline{x_1}, \ldots, \overline{x_n}\rangle},$$
   and we get a generator system of the $\mathbf{A}$-module $\mathbf{B}_{\mathfrak{m}+\langle \underline{x}\rangle}$ by lifting a $\mathbf{k}$-border basis of $\overline{\mathbf{B}}[1/\overline{u}]$.

2. *(Local complete intersection case, without zeroes)*
   If in addition $\mathbf{B}$ is finitely presented as $\mathbf{B} := \mathbf{A}[X_1, \ldots, X_n]/\langle f_1, \ldots, f_n\rangle = \mathbf{A}[x_1, \ldots, x_n]$, then $\mathbf{B}_{\mathfrak{m}+\langle \underline{x}\rangle}$ is a free $\mathbf{A}$-module of rank r, whose basis is given by lifting any $\mathbf{k}$-border basis of $\overline{\mathbf{B}}_{\langle \overline{x_1}, \ldots, \overline{x_n}\rangle}$ with its rewriting rules.

3. *(Local complete intersection case, usual form, with zeroes)*
   Assume that $(\mathbf{A}, \mathfrak{m}, \mathbf{k})$ is a local normal domain with algebraically closed quotient field $\mathbf{K}$ and let $\mathbf{B}$ as in item 2. Then, there are finitely many zeroes of $(f_1, \ldots, f_n)$ above the residual zero $(\underline{0})$ (i.e., zeroes with coordinates in $\mathfrak{m}$) and the sum of their multiplicities equals r.

Proof. 1. Let $\mathbf{B}_1 := \mathbf{B}_{\mathfrak{m}+\langle \underline{x}\rangle}$, $\overline{\mathbf{B}_1} := \overline{\mathbf{B}}_{\langle \overline{x_1}, \ldots, \overline{x_n}\rangle}$. The hypothesis $\dim_{\mathbf{k}}(\overline{\mathbf{B}_1}) = r \geq 1$ means that $(\underline{0})$ is residually an isolated zero of multiplicity r. So, we can construct an $e \in \mathbf{B}$ with $\overline{e} \in \overline{\mathbf{B}}$ such that

- $\overline{e}$ is an idempotent in $\overline{\mathbf{B}}$,
- for a suitable integer N, $\langle 1 - \overline{e}\rangle = \langle \overline{x_1}, \ldots, \overline{x_n}\rangle^N$ in $\overline{\mathbf{B}}$,
- $\overline{\mathbf{B}}[1/\overline{e}] = \overline{\mathbf{B}_1}$.

(See [10, Theorem IX-4.7].) In particular

$$e \in 1 + \mathfrak{m}\mathbf{B} + \langle \underline{x}\rangle \quad \text{and} \quad e^2 - e \in \mathfrak{m}\mathbf{B}$$

Let $\mathbf{C} := \mathbf{B}[1/e]$. Since $e \in 1 + \mathfrak{m}\mathbf{B} + \langle \underline{x}\rangle$, we have $\mathbf{C}_{\mathfrak{m}+\langle \underline{x}\rangle} = \mathbf{B}_{\mathfrak{m}+\langle \underline{x}\rangle}$, and

$$\overline{\mathbf{C}} = \overline{\mathbf{B}}[1/\overline{e}] = \overline{\mathbf{B}}_{\langle \overline{x_1}, \ldots, \overline{x_n}\rangle} = \overline{\mathbf{C}}_{\langle \overline{x_1}, \ldots, \overline{x_n}\rangle}.$$

So $\mathbf{C}$ is a finitely presented $\mathbf{A}$-algebra to which we can apply Corollary 3.5 *1*. There exists $s \in 1 + \mathfrak{m}\mathbf{C}$ such that $\mathbf{C}[1/s] = \mathbf{C}_{\mathfrak{m}+\langle \underline{x}\rangle}$. Since $e \in 1 + \mathfrak{m}\mathbf{B} + \langle \underline{x}\rangle$ we see that s is written as $v(x)/e^m$ for a $v \in 1 + \mathfrak{m}\mathbf{B} + \langle \underline{x}\rangle$ and a suitable exponent m. Finally we see that

$$\mathbf{C}[1/s] = \mathbf{B}[1/u] = \mathbf{B}_{\mathfrak{m}+\langle \underline{x}\rangle}$$

[1] From a constructive point of view we cannot deduce that $\overline{\mathbf{B}}$ is finitely presented from the fact it is finitely generated.

where $u = sv \in 1 + \mathfrak{m}\mathbf{B} + \langle \underline{x} \rangle$. This finishes the proof of item *1*.

2. Now we give some details for describing $\mathbf{C}$ and $\mathbf{C}[1/s]$ when $\mathbf{C}$ is presented with an equal number of generators and relations. Let $E(\underline{X}) \in \mathbf{A}[\underline{X}]$ s.t. $e = E(\underline{x})$, we have

$$1 - E \in \mathfrak{m} + \langle \underline{X} \rangle + \langle f_1, \ldots, f_n \rangle \quad \text{and} \quad E^2 - E \in \mathfrak{m}[\underline{X}] + \langle f_1, \ldots, f_n \rangle \quad \text{(inside } \mathbf{A}[\underline{X}])$$

Therefore

$$\mathbf{C} := \mathbf{B}[1/e] = \mathbf{A}[\underline{x}, 1/e] = \mathbf{A}[\underline{X}, T]/\langle f_1, \ldots, f_n, E(\underline{X})(T+1) - 1 \rangle = \mathbf{A}[\underline{x}, t]$$

Now we write $s = S(\underline{x}, t)$ where $S(\underline{X}, T) \in 1 + \mathfrak{m}[\underline{X}, T]$ and Corollary 3.5 *2* says us that

$$\mathbf{D} := \mathbf{C}[1/s] = \mathbf{A}[\underline{X}, T, Z]/\langle f_1, \ldots, f_n, E(\underline{X})(T+1) - 1, S(\underline{X}, T)(Z+1) - 1 \rangle$$

is a free $\mathbf{A}$-module of rank r, whose basis is given by lifting any $\mathbf{k}$-border basis of $\overline{\mathbf{B}}[1/\overline{e}] = \overline{\mathbf{B}}_{\langle \overline{x_1}, \ldots, \overline{x_n} \rangle}$ with its rewriting rules. This finishes the proof of item *2*.

3. First of all notice that under the hypothesis of *3*, $\mathbf{A}$ is a Henselian local ring and item *2* applies. Let

$$\Sigma := \{f_1, \ldots, f_n, E(\underline{X})(T+1) - 1, S(\underline{X}, T)(Z+1) - 1\}$$

Since $\mathbf{D}$ is a free $\mathbf{A}$-module of rank r, $\mathbf{D} \otimes_{\mathbf{A}} \mathbf{K}$ is a finite $\mathbf{K}$-vector space of dimension r.
Since $\mathbf{K}$ is an algebraically closed field, by Stickelberger's theorem (see [10, Theorem IV-8.17]), we can decompose $\mathbf{D} \otimes_{\mathbf{A}} \mathbf{K}$ as

$$\prod_{(\xi_1, \ldots, \xi_{n+2}) \in \mathcal{Z}_{\mathbf{K}}(\Sigma)} \mathbf{K}[\underline{X}, T, Z]_{(\underline{X} - \underline{\xi}, T - \xi_{n+1}, Z - \xi_{n+2})}/\langle \Sigma \rangle \tag{4}$$

In each $(\xi_1, \ldots, \xi_{n+2}) \in \mathcal{Z}_{\mathbf{K}}(\Sigma)$ the corresponding local $\mathbf{K}$-algebra is zero-dimensional and the sum of multiplicities is equal to r.

It remains to prove that the points of $\mathcal{Z}_{\mathbf{K}}(\Sigma)$ correspond exactly to the zeroes of $(f_1, \ldots, f_n)$ in $\mathbf{K}$ having their coordinates in $\mathfrak{m}$, and that the corresponding local $\mathbf{K}$-algebras are isomorphic.
First let $(\xi_1, \ldots, \xi_{n+2}) \in \mathcal{Z}_{\mathbf{K}}(\Sigma)$ where $\xi_1, \ldots, \xi_n \in \mathfrak{m}$. Since $E(\underline{x}) \in 1 + \mathfrak{m} + \langle \underline{x} \rangle$, we get $\varepsilon := E(\xi_1, \ldots, \xi_n) \in 1 + \mathfrak{m}$. This ε has a unique inverse in $\mathbf{K}$, and this inverse is written $1 + \mu$ with $\mu \in \mathfrak{m}$. This forces $\xi_{n+1} = \mu$. Morevover the two local algebras at $(\xi_1, \ldots, \xi_n)$ and $(\xi_1, \ldots, \xi_{n+1})$ are "equal"

$$\mathbf{K}[x_1, \ldots, x_n]_{\langle x_1 - \xi_1, \ldots, x_n - \xi_n \rangle} \simeq \mathbf{K}[x_1, \ldots, , x_{n+1}]_{\langle x_1 - \xi_1, \ldots, x_{n+1} - \xi_{n+1} \rangle}.$$

This follows from the facts that $\mathbf{K}[x_1, \ldots, , x_{n+1}] = \mathbf{K}[x_1, \ldots, x_n][1/E(\underline{x})]$ and that $E(\underline{x})$ is invertible in $\mathbf{K}[x_1, \ldots, x_n]_{(x_1 - \xi_1, \ldots, x_n - \xi_n)}$. Indeed

$$E(x_1, \ldots, x_n) \equiv E(\xi_1, \ldots, \xi_n) = \varepsilon \bmod \langle x_1 - \xi_1, \ldots, x_n - \xi_n \rangle \text{ in } \mathbf{K}[x_1, \ldots, x_n],$$

so $\langle E(x_1, \ldots, x_n), x_1 - \xi_1, \ldots, x_n - \xi_n \rangle = \langle 1 \rangle$ in $\mathbf{K}[x_1, \ldots, x_n]$.
Similarly $S(\xi_1, \ldots, \xi_n, \mu) \in 1 + \mathfrak{m}$, it has a unique inverse in $\mathbf{K}$, and this inverse is written $1 + \nu$ with $\nu \in \mathfrak{m}$. This forces $\xi_{n+2} = \nu$ and the equality

$$\mathbf{K}[x_1, \ldots, x_n]_{(x_1 - \xi_1, \ldots, x_{n+1} - \xi_{n+1})} \simeq \mathbf{K}[x_1, \ldots, , x_{n+1}]_{(x_1 - \xi_1, \ldots, x_{n+2} - \xi_{n+2})}.$$

It remains to see that any zero $(\xi_1, \ldots, \xi_{n+2}) \in \mathcal{Z}_{\mathbf{K}}(\Sigma)$ has its first n coordinates in $\mathfrak{m}$. Corollary 3.4 (with $\mathbf{E} = \mathbf{K}$ and $\rho : \mathbf{A} \to \mathbf{K}$ the inclusion morphism) shows that $\xi_1, \ldots, \xi_{n+1}$ are in $\mathbf{A}$ (recall that $\mathbf{A}$ is assumed to be integrally closed). Then Corollary 3.6 shows that $\xi_1, \ldots, \xi_{n+1}$ are in $\mathfrak{m}$. □

Remark 3.1. Theorem 3.7 1. can be seen as a generalization of the Mather-Weierstrass division theorem. In fact let $\mathbf{k}$ be a field,

$$\mathbf{A}_n = \mathbf{k}[[X_1, \ldots, X_n]]_{\text{alg}} \text{ (with maximal ideal } \mathfrak{m}_n), \mathbf{A}_m = \mathbf{k}[[X_1, \ldots, X_n, Y_1, \ldots, Y_\ell]]_{\text{alg}},$$

$I = \langle F_1, \ldots, F_q \rangle$ an ideal of $\mathbf{A}_m$, and assume that the morphism $\mathbf{A}_n \to \mathbf{C} = \mathbf{A}_m/I$ is quasi-finite (i.e. $\mathbf{C}/\mathfrak{m}_n\mathbf{C}$ is a finite dimensional $\mathbf{k}$-vector space). We will see that $\mathbf{C}$ is a finite $\mathbf{A}$-module.
As $\mathbf{A}_m$ is the henselization of $(\mathbf{A}_n[Y_1, \ldots, Y_\ell])_{\mathfrak{m}_n + \langle Y_1, \ldots, Y_\ell \rangle}$, we can assume that I is contained in some

$$(\mathbf{A}_n[\underline{Y}, t])_{\mathfrak{m}_n + \langle \underline{Y}, t \rangle} \quad \text{where} \quad \begin{array}{l} \mathbf{A}_n[\underline{Y}, t] = \mathbf{A}_n[\underline{Y}, T]/\langle f(\underline{Y}, T) \rangle\,, \\ f(\underline{Y}, T) \in \mathbf{A}_n[\underline{Y}, T],\ f(\underline{0}, 0) \in \mathfrak{m}_n,\ f_T(\underline{0}, 0) \in 1 + \mathfrak{m}_n, \\ t \in \mathbf{A}_m \ \text{ and } \ f(\underline{Y}, t) = 0. \end{array}$$

W.l.o.g. we assume that $F_i = P_i(\underline{Y}, t)$ where $P_i(\underline{Y}, T) \in \mathbf{A}_n[\underline{Y}, T]$. We apply the theorem with $\mathbf{A} = \mathbf{A}_n$, $\mathbf{B} = (\mathbf{A}_n[\underline{Y}, T]/\langle P_1, \ldots, P_q \rangle)_{\mathfrak{m} + \langle \underline{Y} \rangle}$. Finally we get that $\mathbf{B}$ is a finite $\mathbf{A}$-module. So, it is Henselian and $\mathbf{C} = \mathbf{B}$. And $\mathbf{C}$ is a finite $\mathbf{A}$-module. This is the Mather Theorem.
In the case of $q = 1$, we get the Weierstrass division theorem applying 3.7 2.

4 Application

This section is written in classical mathematics, allowing us to deal with $\mathbb{C}$ as if it were a discrete field (i.e. assuming we have an equality test for complex numbers).

E.g., Theorem 4.1 is not written in a constructive form because, since there is no zero test for elements of $\mathbb{C}$, it is impossible to know in the general situation what are exactly the distinct zeroes and their multiplicities for the perturbed polynomial. E.g., it is a priori impossible to know if a monic univariate polynomial of degree two has one double root or two distinct roots. A constructive and continuous form of the FTA has a slightly different formulation, the best one being [14], where the zeroes of a complex polynomial are seen as forming a multiset that varies continuously in a suitable complete metric space. See also [5, Chapter 5] for another constructive formulation, and [12, Appendix A, page 276] for an optimal modulus of continuity. We think that Theorem 4.2 would need a subtle constructive reformulation, with a more precise proof than that we give here.

Finally we would like to point out that, in the spirit of the proof of [8, Eisermann] which is an analogous to Theorem 4.1 for the algebraic closure $\mathbf{R}[i]$ of a real closed field $\mathbf{R}$, one could prove the classical multivariate version of Theorem 4.2 for $\mathbf{R}[i]$, taking into account the usual manipulation of semialgebraic continuous functions w.r.t. the topology in $\mathbf{C}^n \cong \mathbf{R}^{2n}$ defined by the order of the real closed field $\mathbf{R}$.

We start with a classical result of complex analysis, about the continuity of roots of a univariate polynomial defined over $\mathbb{C}$ (the field of complex numbers), with respect to its coefficients. By $\Omega(\xi, \epsilon)$ we denote the polydisc of $\mathbb{C}^n$ centered at $\xi \in \mathbb{C}^n$: that is

$$\Omega(\xi, \epsilon) = \left\{ \xi' \in \mathbb{C}^n \mid \left|\xi_j - \xi'_j\right| < \epsilon,\ j \in [\![1..n]\!] \right\}.$$

The statement is the following easy consequence of Rouché's Theorem.

Theorem 4.1. *Let be $P(Y) = Y^d + \sum_{i \in [\![0..d-1]\!]} a_i Y^i \in \mathbb{C}[Y]$ a nonzero polynomial of degree $d \geq 1$, and let $P(Y) = \prod_{i \in [\![1..s]\!]} (Y - \xi_i)^{m_i}$ where $\xi_i \in \mathbb{C}$, $i \in [\![1..s]\!]$ are the distinct roots of P. Let $\epsilon > 0$ be s.t. $\Omega(\xi_i, \epsilon) \cap \Omega(\xi_j, \epsilon) = \emptyset$ for every $i \neq j$. Then, there exists $\delta > 0$ s.t. for every $(\widehat{a}_1, \ldots, \widehat{a}_d) \in \Omega((a_1, \ldots, a_d), \delta)$, the polynomial $\widehat{P}(Y) = Y^d + \sum_{i \in [\![0..d-1]\!]} \widehat{a}_i Y^i$ has exactly m_j roots counting with multiplicities in $\Omega(\xi_j, \epsilon)$, for every $j \in [\![1..s]\!]$.*

This section consists in giving a clear proof of the following theorem, which is a classical result about the continuity of the points in a 0-dimensional complete intersection $\mathbb{C}$-algebra, as in [4, 9].

Theorem 4.2. *Let $g_1, \ldots, g_n \in \mathbb{C}[X_1, \ldots, X_n]$ be polynomials of degrees $d_1, \ldots, d_n$ respectively and let $p \in \mathcal{Z}_{\mathbb{C}}(g_1, \ldots, g_n)$ be an isolated zero of multiplicity r. Let $N_1, \ldots, N_n$ be the number of monomials of degree respectively $d_1, \ldots, d_n$ in the variables in $X_1, \ldots, X_n$, and let $N = \sum_i N_{d_i}$. We can see $(g_1, \ldots, g_n)$ as an element $(\underline{a}) \in \mathbb{C}^N$. Let us consider a "slightly perturbed system" $(\widehat{g_1}, \ldots, \widehat{g_n})$ corresponding to an element $(\underline{\widehat{a}}) \in \mathbb{C}^N$. Then for all $\epsilon > 0$ there exists ϵ_1 with $0 < \epsilon_1 < \epsilon$ and $\delta_1 > 0$ such that for all $(\underline{\widehat{a}}) \in \Omega(\underline{a}, \delta_1)$, the perturbed system has only finitely many zeroes in $\Omega(p, \epsilon_1)$; moreover the sum of multiplicities of these zeroes equals r.*

Proof. For sake of simplicity we assume $p = (0, \ldots, 0)$, that is $r = \dim_{\mathbb{C}} \mathbb{C}[\underline{x}]_{(\underline{x})}$ where $\mathbb{C}[\underline{x}] = \mathbb{C}[x_1, \ldots, x_n] = \mathbb{C}[X_1, \ldots, X_n]/\langle g_1, \ldots, g_n \rangle$. We consider a family of new indeterminates:

$$\widetilde{a}^{(i)} = (\widetilde{a}_j^{(i)})_{j=1,\ldots,N_i}.$$

Let us denote by $G_1(\widetilde{a}^{(1)}, \underline{X}), \ldots, G_n(\widetilde{a}^{(n)}, \underline{X})$ the generic polynomials of degrees $d_1, \ldots, d_n$ respectively. So, $g_i = G_i(a^{(i)}, \underline{X})$ for some $a^{(i)} \in \mathbb{C}^{N_i}$. We set now

$$\widetilde{v}_j^{(i)} = \widetilde{a}_j^{(i)} - a_j^{(i)}.$$

We can see the $\widetilde{v}_j^{(i)}$'s as indeterminate perturbations of the $a_j^{(i)}$'s, letting $\widetilde{a}_j^{(i)} = a_j^{(i)} + \widetilde{v}_j^{(i)}$.

We set $\boxed{\mathbf{A} = \mathbb{C}[[(\widetilde{v}_j^{(i)})_{i=1,\ldots,n;j=1,\ldots,N_i}]]_{\mathrm{alg}}}$ the ring of algebraic formal power series (or the ring $\boxed{\mathbf{A} = \mathbb{C}\{(\widetilde{v}_j^{(i)})_{i=1,\ldots,n;j=1,\ldots,N_i}\}}$ of analytic power series) with coefficients in $\mathbb{C}$ in the variables $\widetilde{v}_j^{(i)}$. In the second case this ring can be identified with the ring of germs of analytic functions in a neighborhood of $\underline{a} = (a_j^{(i)})_{i,j}$. In both cases the ring is Henselian with residue field $\mathbb{C}$.

Then, we apply Theorem 3.7 *2* taking as f_i's the G_i's, hence $\mathbf{B} = \mathbf{A}[\underline{x}] = \mathbf{A}[\underline{X}]/\langle G_1, \ldots, G_n \rangle$. Let us recall some elements in the proof of 3.7 *2*.

We have $\mathbf{A}$-algebras $\mathbf{C} = \mathbf{B}[1/e]$ and $\mathbf{D} = \mathbf{C}[1/s] = \mathbf{B}_{\mathfrak{m}+\langle \underline{x} \rangle}$, and $\mathbf{D}$ is a free $\mathbf{A}$-module of rank r, with

$$\overline{\mathbf{D}} = \overline{\mathbf{C}} = \overline{\mathbf{B}}[1/\overline{e}] = \overline{\mathbf{B}}_{\langle \overline{x_1}, \ldots, \overline{x_n} \rangle} = \overline{\mathbf{C}}_{\langle \overline{x_1}, \ldots, \overline{x_n} \rangle} = \overline{\mathbf{D}}_{\langle \overline{x_1}, \ldots, \overline{x_n} \rangle}.$$

In this situation a $\mathbb{C}$-border basis $\mathcal{B}$ of $\overline{\mathbf{B}_1} := \overline{\mathbf{B}}_{\langle \overline{x_1}, \ldots, \overline{x_n} \rangle}$ (with $r = \#\partial\mathcal{B}$) lifts with its rewriting rules to an $\mathbf{A}$-basis of $\mathbf{D}$. So we get in $\mathbf{D}$ for every $\beta \in \partial\mathcal{B}$ an equation

$$x^\beta - \sum\nolimits_{\alpha \in \mathcal{B}} U_{\beta,\alpha} x^\alpha = 0 \quad (\text{for some } U_{\beta,\alpha} \in \mathbf{A}) \tag{5}$$

These $U_{\beta,\alpha}$ are algebraic power series in the formal coefficients $\widetilde{v}$'s and they give analytic functions in a neighborhood of $(\underline{a}) = (a_j^{(i)})_{i,j}$.

Let us denote by Λ_i the multiplication matrix by x_i in the free $\mathbf{A}$-module $\mathbf{D} = \mathrm{Span}_{\mathbf{A}}(\mathcal{B})$, w.r.t. the basis $\mathcal{B}$ using (5). Notice that the entries of Λ_i are either 0 or 1 or one of the $U_{\beta,\alpha}$'s and, since $\mathcal{B}$ is a border basis, one has

$$\Lambda_i \Lambda_j - \Lambda_j \Lambda_i = 0 \tag{6}$$

in $\mathbf{A}^{r \times r}$ for $i \neq j$.

Now we remark that in the proof of 3.7 *2* we have seen that the following ideals of $\mathbf{A}[X_1, ..., X_n]$ coincide.

$$\langle X^\beta - \sum\nolimits_{\alpha \in \mathcal{B}} U_{\beta,\alpha} X^\alpha : \beta \in \partial\mathcal{B} \rangle = \langle G_1, \ldots, G_n, (T+1)E - 1, (Z+1)S - 1 \rangle \mathbf{A}[\underline{X}, T, Z] \cap \mathbf{A}[\underline{X}] \tag{7}$$

Hence one gets equalities ($\beta \in \partial\mathcal{B}$):

$$X^\beta - \sum\nolimits_{\alpha \in \mathcal{B}} U_{\beta,\alpha} X^\alpha = \sum\nolimits_{i \in [\![1..n]\!]} W_i G_i + ((T+1)E - 1)M + ((Z+1)S - 1)R \tag{8}$$

for some $W_i, M, R \in \mathbf{A}[\underline{X}, T, Z]$, and on the other side ($i = 1, \ldots, n$)

$$G_i(\underline{X}) = \textstyle\sum_{\beta \in \partial\mathcal{B}} Q_{i,\beta}(\underline{X}) \cdot (X^\beta - \sum_{\alpha \in \mathcal{B}} U_{\beta,\alpha} X^\alpha) \tag{9}$$

for some $Q_{i,\beta} \in \mathbf{A}[\underline{X}]$. We know that identities (8) and (9) hold in the smallest sub-$\mathbb{C}$-algebra of $\mathbf{A}$ containing the $U_{\beta,\alpha}$'s.

We recall that $\mathfrak{m} = \langle \widetilde{v}_j^{(i)}; i, j \rangle$, $E(\underline{X}) \in 1 + \mathfrak{m} + \langle \underline{X} \rangle$ and $S(\underline{X}, T) \in 1 + \mathfrak{m}[\underline{X}, T]$. To stress the (analytic) dependence of E and S on the $\widetilde{v}_j^{(i)}$'s we shall write $E(\underline{\widetilde{v}}, \underline{X})$ and $S(\underline{\widetilde{v}}, \underline{X}, T)$.

Now let $P_i \in \mathbf{A}[Y]$ denote the characteristic polynomial of the multiplication by the image of x_i in $\mathbf{D}$ (i.e. the characteristic polynomial of Λ_i). Its coefficients are $\mathbb{Z}$-polynomials in the $U_{\beta,\alpha}$'s. By change of ring, $\overline{P_i} \in \mathbb{C}[Y]$ is the characteristic polynomial of the multiplication by $\overline{x_i}$ in $\overline{\mathbf{D}} = \overline{\mathbf{B}}_1$.

From ϵ, by usual arguments of Taylor calculus for convergent series we can find δ and $\epsilon' < \epsilon$ such that the following properties hold:

i) All the $U_{\beta,\alpha}$ are convergent and also the coefficients in (8) and (9) are convergent for any $\widehat{a}^{(i)} \in \Omega(a^{(i)}, \delta)$. Therefore the same will hold for the coefficients of P_i.

ii) The polynomial $E(\underline{\widetilde{v}}, \underline{X})$ as a polynomial with coefficients which are analytic functions in a neighborhood of $a^{(i)}$'s verifies that for every $(\widehat{a}^{(i)}, \underline{x}) \in \Omega(a^{(i)}; \delta) \times \Omega(\underline{0}; \epsilon')$, $|E(\widehat{\underline{a}}, \underline{x}) - 1| < \epsilon'$.

In particular for those points $(\widehat{\underline{a}}, \underline{x})$ we have $E(\widehat{\underline{a}}, \underline{x}) \neq 0$ and we may also ask that $\left|1 - \frac{1}{E(\widehat{\underline{a}}, \underline{x})}\right| < \epsilon'$.

iii) In the same way for $(\widehat{a}^{(i)}, \underline{x}, t) \in \Omega(a^{(i)}; \delta) \times \Omega(\underline{0}; \epsilon') \times \Omega(0; \epsilon')$, $S(\widehat{\underline{a}}, \underline{x}, t)$ does not vanish and $\left|1 - \frac{1}{S(\widehat{\underline{a}}, \underline{x}, t)}\right| < \epsilon'$.

We apply Theorem 4.1 with ϵ' and $P = Y^r = \overline{P_i} \in \mathbb{C}[Y]$, there exists $\delta' \in \mathbb{R}^+$, $\delta' < \delta$, such that if $Q \in \mathbb{C}[Y]$ is a monic polynomial of degree r, whose coefficients belong to a neighborhood $\Omega(\underline{0}; \delta')$, then, the distance of each of the r complex roots of Q to 0 is less than ϵ'. Notice that Q can be considered as a perturbation of $\overline{P_i}$.

Then, for every $\widehat{a}^{(i)} \in \Omega(a^{(i)}; \delta')$; we consider $\widehat{g_i} := G_i(\widehat{a}^{(i)}, X)$, which is "a perturbation" of the g_j, and we denote by $\widehat{U}_{\beta,\alpha}$ the result of specializing $U_{\beta,\alpha}$ in the values of $\widehat{a}^{(i)}$'s.

Then the following facts hold true and alltogether prove the theorem taking the value δ_1 as δ' and ϵ_1 as ϵ':

1. $\{x^\beta : \beta \in \mathcal{B}\}$ is a basis of the $\mathbb{C}$-vector space, because the relations of commutations (6) still hold under specialization at $\widehat{a}^{(i)}$ (see **2.2.4** in section 2 on border bases). Consequently the ideal of $\mathbb{C}[\underline{X}]$ $\widehat{I} = I(\widehat{a}^{(i)}) := \langle X^\alpha - \sum_{\beta \in \mathcal{B}} \widehat{U}_{\beta,\alpha} X^\beta \rangle$ has r zeroes in $\mathbb{C}^n$ counted with multiplicity.

2. The characteristic polynomial of the multiplication by X_i in the ring $\mathbb{C}[\underline{X}]/\widehat{I}$ is $\widehat{P}_i$. For every $(\underline{\xi}) \in \mathbb{C}^n$ which is a zero of $\widehat{I}$ its coordinates ξ_i's are roots of the polynomials $\widehat{P}_i(T)$. We know that these roots belong to $\Omega(\underline{0}; \epsilon')$. On the other hand these zeroes are zeroes of the ideal $J(\widehat{a}^{(i)}) := \langle (\widehat{g}_i)_{i=1,\ldots,n} \rangle \mathbb{C}[\underline{X}]$, because of the specialization of (9).

3. Conversely given $(\underline{\xi}) \in \mathbb{C}^n$ which is a zero of the ideal $J(\widehat{a}^{(i)})$ and such that $(\underline{\xi}) \in \Omega(\underline{0}; \epsilon')$ we are going to prove that $(\underline{\xi})$ is a zero of $I(\widehat{a}^{(i)})$. As $\widehat{a}^{(i)} \in$ and $(\underline{\xi}) \in \Omega(\underline{0}; \epsilon')$, by ii) above we have that $t := 1 - \frac{1}{E(\widehat{a}^{(i)}, \underline{\xi})} \in \Omega(0, \epsilon')$. Consequently it makes sense to substitute in (8), $(\widehat{a}^{(i)}, \underline{\xi}, t)$. since the right hand side vanishes, the same happen for the left hand side.

4. Given $(\underline{\xi}) \in \Omega(\underline{0}; \epsilon')$, zero of $J(\widehat{a}^{(i)})$ and hence of $I(\widehat{a}^{(i)})$ the local rings $\mathbb{C}[\underline{X}]/I(\widehat{a}^{(i)})_{(\underline{X}-\underline{\xi})}$ and $\mathbb{C}[\underline{X}]/J(\widehat{a}^{(i)})_{(\underline{X}-\underline{\xi})}$ coincide. In fact this comes from (9), and by substituting in (8) T by $1 - \frac{1}{E(\widehat{a}^{(i)}, \underline{X})}$ and Z by $1 - \frac{1}{S(\widehat{a}^{(i)}, \underline{X}, T)}$, which is allowed since both expressions are rational regular at the point $(\underline{\xi})$. □

References

[1] Maria Emilia Alonso, Jean Brachat, and Bernard Mourrain. Stable Deformation of Zero-Dimensional Quotient Algebras. Technical report, 2009. 6

[2] Maria Emilia Alonso, Thierry Coquand, and Henri Lombardi. Revisiting Zariski main theorem from a constructive point of view. *J. Algebra*, 406:46–68, 2014. 2

[3] Maria Emilia Alonso and Henri Lombardi. Local Bézout theorem. *J. Symbolic Comput.*, 45(10):975–985, 2010. 4, 6, 7

[4] V.I. Arnold, S.M. Gusein-Zade, and A.N. Varchenko. *Singularities of differentiable maps, Volume 1. Classification of critical points, caustics and wave fronts. Transl. from the Russian by Ian Porteous, edited by V. I. Arnold.* Boston, MA: Birkhäuser, reprint of the 1985 hardback edition, 2012. 1, 9

[5] Errett Bishop. *Foundations of constructive analysis*. McGraw-Hill Book Co., New York-Toronto, Ont.-London, 1967. 9

[6] Jean Brachat. *Schémas de Hilbert et Décomposition de tenseurs*. PhD thesis, 2011. 3

[7] B. de Smit and H. W. Lenstra. Finite complete intersection algebras and the completeness radical. *J. Algebra*, 196(2):520–531, 1997. 1, 2

[8] Michael Eisermann. The fundamental theorem of algebra made effective: an elementary real-algebraic proof via Sturm chains. *Amer. Math. Monthly*, 119(9):715–752, 2012. 9

[9] Phillip Griffiths and Joseph Harris. *Principles of algebraic geometry*. Wiley Classics Library. John Wiley & Sons, Inc., New York, 1994. Reprint of the 1978 original. 1, 9

[10] Henri Lombardi and Claude Quitté. *Commutative Algebra. Constructive Methods*. Algebra and Applications, Vol. 20. Berlin, New-York: Springer, 2015. 7, 8

[11] Bernard Mourrain. A new criterion for normal form algorithms. In *Applied algebra, algebraic algorithms and error correcting codes. 13th international symposium, AAECC-13, Honolulu, HI, USA, November 15–19, 1999. Proceedings*, pages 430–443. Berlin: Springer, 1999. 1, 2, 3

[12] A. M. Ostrowski. *Solution of equations in Euclidean and Banach spaces*. Academic Press [A Subsidiary of Harcourt Brace Jovanovich, Publishers], New York-London, 1973. Third edition of ıt Solution of equations and systems of equations, Pure and Applied Mathematics, Vol. 9. 9

[13] Claude Quitté and Henri Lombardi. Le théorème de de Smit et Lenstra, démonstration élémentaire. http://arxiv.org/abs/1508.05589. 2015. 1, 2

[14] Fred Richman. The fundamental theorem of algebra: a constructive development without choice. *Pacific J. Math.*, 196(1):213–230, 2000. 9