Revisiting Zariski Main Theorem from a constructive point of view

Alonso M., Coquand T., Lombardi H.

March 10, 2014

Abstract

This paper deals with the Peskine version of Zariski Main Theorem published in 1965 and discusses some applications. It is written in the style of Bishop's constructive mathematics. Being constructive, each proof in this paper can be interpreted as an algorithm for constructing explicitly the conclusion from the hypothesis. The main non-constructive argument in the proof of Peskine is the use of minimal prime ideals. Essentially we substitute this point by two dynamical arguments; one about gcd's, using subresultants, and another using our notion of strong transcendence. In particular we obtain algorithmic versions for the Multivariate Hensel Lemma and the structure theorem of quasi-finite algebras.

Keywords. Zariski Main Theorem, Multivariate Hensel Lemma, Quasi finite algebras, Constructive Mathematics

Contents

1 Introduction

The paper is written in the style of Bishop's constructive mathematics, i.e. mathematics with intuitionistic logic (see [4, 5, 14, 16]).

A partial realization of Hilbert's program has recently proved successful in commutative algebra, see e.g., [1, 6, 7, 8, 9, 11, 14, 19] and [10] with references therein, and this paper is a new piece of realization of this program.

We were mainly interested in an algorithm for the Multivariate Hensel Lemma (MHL for short). Let us see what is the aim of the computation on a simple example.

We consider the local ring $A = \mathbb{Q}[a,b]_S$, $S = 1 + \langle a,b\rangle A$. We take the equations

$$-a + x + bxy + 2bx^2 = 0, \qquad -b + y + ax^2 + axy + by^2 = 0$$

and we want to compute a solution of the system $(\xi,\zeta) \equiv 0 \bmod \mathfrak{M}$ in the henselization of A. In other words, we have to find a Hensel equation $f(U) \in A[U]$ (i.e. f monic, $f(0) \in \langle a,b\rangle$ and $f'(0) \notin \langle a,b\rangle$) such that, when adding the Hensel zero u of f to A we are able to compute ξ and $\zeta \in A[u]_{1+\langle a,b,u\rangle A[u]}$.

Surprinsingly there is no direct proof of the result. Moreover elementary elimination techniques do not work on the above example. So we have to rely on the proof of MHL via the so called Zariski Main Theorem (ZMT for short), as for example in [15]. Note that there are many versions of ZMT (e.g. [13, 20]) and we are interested in the ZMT à la Peskine as in [15].

We will give a solution of the above example in section 4.4.

This paper deals with the Peskine proof of ZMT published in 1965 [17] and discusses some applications. Peskine statement is purely algebraic avoiding any hypothesis of noetherianity. The argument we give for Theorem 1.3 follows rather closely Peskine's proof. The main non-constructive argument in the proof of Peskine is the use of minimal prime ideals. Note that the existence of minimal prime ideals in commutative rings is known to be equivalent to Choice Axiom. Essentially we substitute this point by two dynamical arguments; one about gcd's, using *subresultants*, section 2.3, proof of Proposition 2.18, and another using our notion of *strong transcendence*, section 2.2 (in classical mathematics: to be transcendent over all residual fields).

In sections 4 and 5, we give a constructive treatment of two classical applications of ZMT: the Multivariate Hensel Lemma, and structure theorem of quasi finite algebras.

Being constructive, each proof in this paper can be interpreted as an algorithm for constructing explicitly the conclusion from the hypothesis.

Theorem 1.1 (ZMT à la Peskine, particular case)
Let A be a ring, $\mathfrak{M}$ a detachable maximal ideal of A and $k = A/\mathfrak{M}$. If $B = A[x_1,\ldots,x_n]$ is an extension of A such that $B/\mathfrak{M}B$ is a finite k-algebra then there exists $s \in 1+\mathfrak{M}B$ such that s, sx_1, ..., sx_n are integral over A.

In [18] an equivalent formulation (Proposition 13.4) of Peskine version of the Zariski Main Theorem can be written as the following lemma.

Proposition. *Let $(A,\mathfrak{M})$ be a residually discrete local ring and $k = A/\mathfrak{M}$. If $B = A[x_1,\ldots,x_n]$ is an extension of A such that $\mathfrak{M}B \cap A = \mathfrak{M}$, A is integrally* *closed in B and $B/\mathfrak{M}B$ has a nontrivial zero-dimensional component as a k-algebra, then $B = A$.*

The last hypothesis can be given in a concrete way: there exists an idempotent e of $B/\mathfrak{M}B$ such that $(B/\mathfrak{M}B)[1/e]$ is a nontrivial finite k-algebra. This means that the residual variety has at least one isolated point.

The following corollary of Theorem 1.1 is a weakened form of the previous proposition.

Corollary 1.2 *Let $(A, \mathfrak{M})$ be a residually discrete local ring and $k = A/\mathfrak{M}$. If $B = A[x_1, \dots, x_n]$ is an extension of A such that $\mathfrak{M}B \cap A = \mathfrak{M}$, A is integrally closed in B and $B/\mathfrak{M}B$ is a finite k-algebra then $B = A$.*

Proof. By Theorem 1.1 we find $s \in A$ such that $s \in 1 + \mathfrak{M}B$ and $sx_1, \dots, sx_n \in A$. We have then $s - 1 \in A \cap \mathfrak{M}B = \mathfrak{M}$ and hence s is invertible in A. Hence $x_1, \dots, x_n$ are in A and $B = A$. □

Remark. The hypothesis that A is integrally closed in B is necessary, even if we weaken the conclusion to "B is finite over A". Let A be a DVR with $\mathfrak{M} = pA$, the ring $B = A \times A[1/p]$ is finitely generated over A, $\mathfrak{M}B = \langle (p, 1) \rangle$ and $B/\mathfrak{M}B = A/\mathfrak{M}$, but B is not finite over A. If A' is the integral closure of A in B, we cannot apply Corollary 1.2 with $(A', \mathfrak{M}A')$ replacing $(A, \mathfrak{M})$ because $\mathfrak{M}A'$ is not a maximal ideal of A' (in fact $A' \simeq A \times A$).

In fact we shall prove a slightly more general version of Theorem 1.1, without assuming $\mathfrak{M}$ to be a detachable maximal ideal.

Theorem 1.3 (ZMT à la Peskine, variant)
Let A be a ring with an ideal $\mathfrak{I}$ and $B = A[x_1, \dots, x_n]$ be an extension of A such that $B/\mathfrak{I}B$ is a finite $A/\mathfrak{I}$-algebra, then there exists $s \in 1 + \mathfrak{I}B$ such that s, sx_1, $\dots$, sx_n are integral over A.

Remark. In fact, the hypothesis that the morphism $A \to B$ is injective is not necessary: it is always possible to replace A and $\mathfrak{I}$ by their images in B, and the conclusion remains the same.

Corollary 1.4 *Let A be a ring with an ideal $\mathfrak{I}$ and $B = A[x_1, \dots, x_n]$ be an extension of A such that $B/\mathfrak{I}B$ is a finite $A/\mathfrak{I}$-algebra, then there exists a finite extension C of A inside B and $s \in C \cap 1 + \mathfrak{I}B$ such that $C[1/s] = B[1/s]$.*

Proof. Take $C = A[s, sx_1, \dots, sx_n]$. □

We shall also give a proof of the following "global form" of Zariski Main Theorem.

Theorem 5.3 (ZMT à la Raynaud, [15])
Let $A \subseteq B = A[x_1, \dots, x_n]$ be rings such that the inclusion morphism $A \to B$ is zero dimensional (in other words, B is quasi-finite over A). Let C be the integral closure of A in B. Then there exist elements $s_1, \dots, s_m$ in C, comaximal in B, such that all $s_i x_j \in C$.
In particular for each i, $C[1/s_i] = B[1/s_i]$. Moreover letting $C' = A[(s_i), (s_i x_j)]$, which is finite over A, we get also $C'[1/s_i] = B[1/s_i]$ for each i.

We give now the plan of the paper.

In section 2 we give some preliminary results and the proof of a Peskine "crucial lemma".

In section 3 we give the constructive proof for Theorem 1.3.

In section 4 we give a constructive proof for the Multivariate Hensel Lemma (Theorem 4.4). A usual variant is the following corollary.

Corollary 4.5 *Let $(A, \mathfrak{m})$ be a Henselian local ring. Assume that a polynomial system $(f_1, \ldots, f_n)$ in $A[X_1, \ldots, X_n]$ has residually a simple zero at $(0, \ldots, 0)$. Then the system has a (unique) solution in A^n with coordinates in $\mathfrak{m}$.*

Section 5 is devoted to structure theorem of quasi-finite algebras: we give a proof of Theorem 5.3, moreover Proposition 5.2 explains the constructive content of the hypothesis in Theorem 5.3.

Acknowledgements. First and third authors are partially supported by Spanish GR MTM2011-22435. Third author thanks the Computer Science and Engineering Department at University of Gothenburg for several invitations. This article has been discussed in the course of a researching stay of the first author at the Department of Mathematics of the University of Franche-Comté. She thanks the Department for its kind invitation.

2 Peskine crucial lemma

In this section we give a constructive proof of a crucial lemma in the proof of Peskine. This is Proposition 2.18 in the following.

2.1 Basic tools for computing integral elements

Let $R \subseteq S$ be rings and let $\mathfrak{I}$ be an ideal of R. We say that $t \in S$ is *integral over* $\mathfrak{I}$ if and only if it satisfies a relation $t^n + a_1 t^{n-1} + \cdots + a_n = 0$ with $a_1, \ldots, a_n$ in $\mathfrak{I}$. The *integral closure* of $\mathfrak{I}$ in S is the ideal of elements of S that are integral over $\mathfrak{I}$.

Lemma 2.1 *(Lying Over, concrete form)*

1. *If S is integral over R then the integral closure of $\mathfrak{I}$ in S is $\sqrt{\mathfrak{I}S}$.*

   As a consequence $\sqrt{\mathfrak{I}S} \cap R = \sqrt{\mathfrak{I}}$.

2. *If S is integral over R and $1 \in \langle b_1, \ldots, b_m \rangle S$ then $1 \in \langle b_1, \ldots, b_m \rangle R[b_1, \ldots, b_m]$.*

Proof. *1.* See [2] Lemma 5.14.
2. Use item *1* with $R' = R[b_1, \ldots, b_m]$ and $\mathfrak{I} = \langle b_1, \ldots, b_m \rangle R[b_1, \ldots, b_m]$. □

Algorithm: Let x be in $\sqrt{\mathfrak{I}S}$: $x^n = \sum_{k=1}^{p} a_k s_k$, with $a_k \in \mathfrak{I}$ and $s_k \in S$. Let $1 = s_1, \ldots, s_m$ be generators of $R_1 = R[s_1, \ldots, s_p]$ as an R-module. The multiplication by x^n in R_1 is expressed on $s_1, \ldots, s_m$ by a matrix M_{x^n} with coefficients in $\mathfrak{I}$. The characteristic polynomial of M_{x^n} is $P(T) = T^m + \sum_{k=0}^{m-1} b_k T^k$ with b_k's $\in \mathfrak{I}$, and $P(x^n) = P(M_{x^n})(1, 0, \ldots, 0) = 0$.

Definition 2.2 We denote $\mathrm{c}_X(g)$ (or $\mathrm{c}(g)$) the ideal of R generated by the coefficients of $g \in R[X]$ ($\mathrm{c}_X(g)$ is called the X-content ideal of g in R).

Lemma 2.3 (Kronecker)
Let $Z \subseteq R$ where Z is the subring generated by 1.

1. *(simple form) If $f(X) = X^k + a_1 X^{k-1} + \cdots + a_k$ divides $X^n + b_1 X^{n-1} + \cdots + b_n$ in $R[X]$ then $a_1, \ldots, a_k$ are integral over $b_1, \ldots, b_n$ (more precisely they are integral over the ideal generated by $b_1, \ldots, b_n$ in $Z[b_1, \ldots, b_n]$).*

2. *(general form) If $fg = h = \sum_{j=0}^{n} c_j X^j$ in $R[X]$, a a coefficient of f and b a coefficient of g then ab is integral over the ideal generated by $c_0, \ldots, c_n$ in $Z[c_0, \ldots, c_n]$.*

3. *(Gauss-Joyal) If $fg = h = \sum_{j=0}^{n} c_j X^j$ in $R[X]$ then $\mathrm{c}(f)\mathrm{c}(g) \subseteq \sqrt{\mathrm{c}(h)}$.*

Proof. *1.* Considering the splitting algebra of f over R, we can assume $X^k + a_1 X^{k-1} + \cdots + a_k = (X - t_1) \ldots (X - t_k)$. We have then $t_1, \ldots, t_k$ integral over $b_1, \ldots, b_n$ and hence also $a_1, \ldots, a_k$ since they are (symmetric) polynomials in $t_1, \ldots, t_k$.
2. This is deduced from *1* by homogeneization arguments.
3. This is an immediate consequence of *2.* □

Lemma 2.4 *If $R \subseteq S$ and $t \in S$ satisfies an equation $a_n t^n + \cdots + a_0 = 0$ with $a_0, \ldots, a_n \in R$ then $a_n t$ is integral over R.*

Lemma 2.5 (see [12]) *Let $R \subseteq S$ and $x \in S$ satisfies an equation $P(x) = a_n x^n + \cdots + a_0 = 0$ with $a_0, \ldots, a_n \in R$. We take*

$$u_n = a_n, \; u_{n-1} = u_n x + a_{n-1}, \; \ldots\ldots \; , \; u_0 = u_1 x + a_0 = 0$$

We get the following results.

1. *$u_n, \ldots, u_0$ and $u_n x, \ldots, u_0 x$ are integral over R and $\langle u_0, \ldots, u_n \rangle = \langle a_0, \ldots, a_n \rangle$ as ideals of $R[x]$.*

2. *Let $\mathfrak{I}$ be an ideal of R s.t. $1 \in \langle a_0, \ldots, a_n \rangle R[x] \bmod \mathfrak{I}R[x]$ and $x \bmod \mathfrak{I}$ is integral over $R/\mathfrak{I}$ then there exists $w \in 1 + R[x]$ s.t. w and wx are integral over R.*

Proof. *1.* Lemma 2.4 shows that $a_n x = u_n x$ is integral over R. It follows that $u_{n-1} = u_n x + a_{n-1}$ is integral over R. We have then

$$u_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \cdots + a_0 = 0$$

so that, again by Lemma 2.4, $u_{n-1} x$ is integral over $R[u_{n-1}]$ and so over R. In this way, we get that u_n, $u_n x$, u_{n-1}, $u_{n-1} x$, …, $u_1 x$, $u_0 = 0$ are all integral over R.
2. Let R' be the image of $R[\underline{u}] = R[u_0, \ldots, u_n]$ in $R[x]/\mathfrak{I}R[x]$. So $R' \subseteq R[x]/\mathfrak{I}R[x]$ with $R[x]/\mathfrak{I}R[x]$ integral over R'. Item *1.* shows that $1 \in \langle u_0, \ldots, u_n \rangle \bmod \mathfrak{I}R[x]$. Lying Over item *2* gives $1 = \sum_{i=0}^{n} u_i g_i(\underline{u}) \bmod \mathfrak{I}R[x]$ with $g_i(\underline{u})$'s $\in R[\underline{u}]$. Let $w = \sum_{i=0}^{n} u_i g_i(\underline{u})$, then w and wx are clearly integral over R. □

Lemma 2.6

1. *If t is integral over $R[x]$ and $p(x)$ is a monic polynomial in $R[x]$ such that $tp(x)$ is in $R[x]$ then there exists q in $R[x]$ such that $t - q$ is integral over R.*

2. *If t is integral over $R[x]$ and $p(x) = a_k x^k + \cdots + a_0$ is a polynomial in $R[x]$ such that $tp(x)$ is in $R[x]$ then there exists q in $R[x]$ and m such that $a_k^m t - q$ is integral over R.*

Proof. 1. We write $tp = r(x)$ in $R[x]$. We do the Euclidian division of $r(X)$ by $p(X)$ and get $r = pq + r_1$. We can then write $(t - q)p = r_1$. This shows that we have $p = (t-q)^{-1}r_1$ in $R[(t-q)^{-1}][x]$ and hence that x is integral over $R[(t-q)^{-1}]$. Since $t - q$ is integral over $R[x]$ we get that $t - q$ is integral over $R[(t - q)^{-1}]$ and hence over R.
2. We have an equation for t of the form $t^n + p_1(x)t^{n-1} + \cdots + p_n(x) = 0$. Let ℓ be the greatest exponent of x in this expression. By multiplying by a^ℓ we get an equality of the form

$$a^\ell t^n + q_1(ax)t^{n-1} + \cdots + q_n(ax) = 0$$

and hence, by Lemma 2.4, $a^\ell t$ is integral over $R[ax]$. Sowe we have ℓ such that $a^\ell t$ is integral over $R[ax]$ for all $a \in R$.
We write $tp(x) = r(x)$ and by multiplying by a suitable power of a_k we get an $ta_k^m P(a_k x) \in R[a_k x]$ with $m \geq \ell$ and P monic. We can then apply item *1.* □

Corollary 2.7 *If t is integral over $R[x]$ and R is integrally closed in $R[x,t]$ and $t(a_k x^k + \cdots + a_0) \in R[x]$ then there exists m such that $a_k^m t \in R[x]$.*

Next lemma is a kind of glueing of integral extensions.

Lemma 2.8 *Let $R \subseteq S$ and $x, t, y, s \in S$. If t, ty are integral over $R[x]$ and s, sx integral over R then for N big enough and $w = s^N t$ the elements w, wx, wy are integral over R.*

Proof. We write $t^k + a_1(x)t^{k-1} + \cdots + a_k(x) = 0$ and $t^\ell y^\ell + b_1(x)t^{\ell-1}y^{\ell-1} + \cdots + b_\ell = 0$. Let x^d be the highest power of x that appears in these expressions. We have that $s^d t$ and $s^d ty$ are integral over s, sx and so over R, and we take $N = d + 1$. □

2.2 Strong transcendence

Let D be a C-algebra and $x \in D$. We say that x *is strongly transcendent over C in D* if for all $u \in D$ and $c_0, \ldots, c_k \in C$ such that $u(c_0 + \cdots + c_k x^k) = 0$, we have $uc_0 = \cdots = uc_k = 0$ (each time it is needed, c_i stands for the image of c_i in D).

Note that the definition strongly depends on C **and** D. Moreover from an equality $c_0 + \cdots + c_k x^k = 0$ in D we deduce only that $c_0 = \cdots = c_k = 0$ in D.

Lemma 2.9

1. *If D is a C-algebra, x strongly transcendent over C in D and V a monoid of D, then x is strongly transcendent over C in D_V.*

2. *If D is a C-algebra and x is strongly transcendent over C in D and $a \in C$, then x is strongly transcendent over $C[1/a]$ in $D[1/a]$.*

Lemma 2.10 *If $u, x \in D$, D a reduced C-algebra, x strongly transcendent over C in D and u, ux are integral over C then $u = 0$.*

Proof. We have $Q(ux) = (ux)^\ell + c_1(ux)^{\ell-1} + \cdots + c_\ell = 0$ and $P(u) = u^m + a_1 u^{m_1} + \cdots + a_m = 0$ for some $c_1, \ldots, c_\ell, a_1, \ldots, a_m$ in C. So $\mathrm{Res}_U(P(U), Q(Ux)) = V(x)$ is a polynomial with constant coefficient c_ℓ^m and leading coefficient $\pm a_m^\ell$. Since $V(x) = 0$, x is transcendent over C in D, and D is reduced, it follows that we have $c_\ell = a_m = 0$ in D. We get in D

$$(ux)Q_1(ux) = 0 \quad \text{with} \quad Q_1(T) = (Q(T) - c_\ell)/T.$$

Now we consider the reduced ring $D_1 = D[1/(ux)]$. In this ring x is strongly transcendent over C. We have in D_1

$$Q_1(ux) = 0 \text{ with } Q_1(0) = c_{\ell-1} \quad \text{and} \quad P(u) = 0.$$

So $c_{\ell-1} = 0$ in D_1. Similarly we deduce $c_{\ell-2} = \cdots = c_1 = 0$ in D_1. So $ux = 0$ in D_1 and finally $ux = u = 0$ in D. □

Lemma 2.11 *If D is a reduced C-algebra and x is strongly transcendent over C in D and $C_1 \subseteq D$ and C_1 is integral over C then x is strongly transcendent over C_1 in D.*

Proof. Assume an equality $u(c_0 x^k + \cdots + c_k) = 0$ with $u \in D$ and c_i's in C_1. Passing to $D' = D[1/u]$ we get $c_0 x^k + \cdots + c_k = 0$ with c_i's integral over C. So $c_0 x$ is integral over C_1, and thus over C too. So c_0 and $c_0 x$ are integral over C. By Lemma 2.10 $c_0 = 0$ in D', so $c_0 u = 0$ in D. We finish by induction on k. □

2.3 Crucial lemma

Context 2.12 We fix now the following context, which comes from Corollary 2.7: t integral over $R[x]$ of degree n and R integrally closed in $S = R[x, t]$. We define $J = (R[x] : S)$.

Lemma 2.13 (Context 2.12)
If $u \in S$ we have $u \in J$ if and only if $u, ut, \ldots, ut^{n-1} \in R[x]$.

Proof. This is clear since all elements of S can be written $q_{n-1}(x)t^{n-1} + \cdots + q_0(x)$. □

Lemma 2.14 (Context 2.12)
If $u \in S$ and $a_0, \ldots, a_k \in R$ and $u(a_0 + \cdots + a_k x^k) \in J$, then there exists m such that $u a_k^m \in J$.

Proof. We have by Lemma 2.13

$$(a_0 + \cdots + a_k x^k)u, (a_0 + \cdots + a_k x^k)ut, \ldots, (a_0 + \cdots + a_k x^k)ut^{n-1} \in R[x].$$

All elements ut^j are integral over $R[x]$ and R is integrally closed in $R[x, ut^j]$. Hence by Corollary 2.7 we find m such that $a_k^m ut^j \in A[x]$. $\square$

We consider now the radical $\sqrt{JS}$ of J *in* S.

Corollary 2.15 (Context 2.12)
If $u \in S$ *and* $a_0, \ldots, a_k \in R$ *and* $u(a_0+\cdots+a_k x^k) \in \sqrt{JS}$, *then* $ua_0, \ldots, ua_k \in \sqrt{JS}$.

Proof. We have ℓ such that $u^\ell(a_0 + \cdots + a_k x^k)^\ell \in J$. By Lemma 2.14 we have m such that $u^\ell(a_k^\ell)^m \in J$ and hence $ua_k \in \sqrt{JS}$. It follows that $ua_k x^k \in \sqrt{JS}$ and so $u(a_0 + \cdots + a_{k-1}x^{k-1}) \in \sqrt{JS}$ and we get successively $ua_{k-1}, \ldots, ua_0 \in \sqrt{JS}$. $\square$

Summing up previous results in Context 2.12 and using the notion of strong transcendence.

Proposition 2.16 *Assume* $S = R[x, t]$ *with* t *integral over* $R[x]$ *and* R *is integrally closed in* S. *We take* $J = (R[x] : S)$. *If we take* $D = S/\sqrt{JS}$ *and* $C = R/R \cap \sqrt{JS}$, *then* $D = C[x, t]$ *is a reduced ring with a subring* C *such that* t *is integral over* $C[x]$ *and* x *is strongly transcendent over* C *in* D.

Proof. Clear. The last assertion comes from Corollary 2.15. $\square$

Proposition 2.17 *Assume that* $D = C[x, t]$ *is a reduced ring with a subring* C *such that* t *is integral over* $C[x]$ *and* x *is strongly transcendent over* C *in* D. *Let* $\mathfrak{I}$ *be an ideal of* C *such that* $tx \in \sqrt{\mathfrak{I}D}$. *Then* $t \in \sqrt{\mathfrak{I}D}$.
Equivalently, if D_U *is the localization of* D *at the monoid* $U = t^{\mathbb{N}} + \mathfrak{I}D$, *then* D_U *is a trivial ring.*

The proof is given after the crucial lemma.

Proposition 2.18 (crucial lemma)
If $S = R[x, t]$ *and* R *is integrally closed in* S *and* t *is integral over* $R[x]$ *and* $\mathfrak{I}$ *ideal of* R *such that* $tx \in \sqrt{\mathfrak{I}S}$ *then* $t \in \sqrt{\mathfrak{I}S}$ *mod.* $\sqrt{JS}$ *where* $J = (R[x] : S)$.

Proof. This follows from Propositions 2.16 and 2.17. $\square$

Here begins the proof of Proposition 2.17.
Since t is integral over C we get a T-monic polynomial $P(x, T)$ in $C[x][T]$ s.t. $P(x, t) = 0$. As $tx \in \sqrt{\mathfrak{I}D}$ by Lying Over we get a polynomial

$$Q(X, T) = X^n T^n + \mu_1(X) X^{n-1} T^{n-1} + \cdots + \mu_n(X) \text{ with } \in \mu_i(X) \in \mathfrak{I}C[X]$$

s.t. $Q(x, t) = 0$. We need now to prove Lemma 2.19.

Lemma 2.19 *Assume* $C_1 \subseteq D_U$, *that* x *is transcendent over* C_1 *and that* $G(x, T) = T^k + b_1(x)T^{k-1} + \cdots + b_k(x)$ *divides* $Q(x, T)$, *with* $b_1(x), \ldots, b_k(x) \in C_1[x]$ *and* $G(x, t) = 0$. *Then* D_U *is a trivial ring.*

Proof. Since x is transcendent over C_1 we have that $G(X,T) = T^k + b_1(X)T^{k-1} + \cdots + b_k(X)$ divides $Q(X,T)$. By taking $T = X^N$ we see that $X^{Nk} + b_1(X)X^{N(k-1)} + \cdots + b_k(X)$ divides $X^n X^{Nn} + \mu_1(X)X^{n-1}X^{N(n-1)} + \cdots + \mu_n(X)$. If N is big enough we can apply Lemma 2.3 and conclude that all coefficients of $b_1(X), \ldots, b_k(X)$ are integral over $\mathfrak{I}$. Since $G(x,t) = t^k + b_1(x)t^{k-1} + \cdots + b_k(x) = 0$ it follows that t is integral over $\mathfrak{I}C[x]$, and so D_U is a trivial ring. □

We consider the ring D_U, we compute the subresultants of $P(x,T)$ and $Q(x,T)$ in $C[x][T]$ and we show that they are all 0 in D_U, i.e. $P(x,T)$ has to divide $Q(x,T)$ in $D_U[T]$.
The conclusion follows then from Lemma 2.19 with C_1 the image of C in D_U and $G = P$.
We use results about subresultants given in Lemma 2.20 (for the general theory of subresultants, see [3, Chapter 4]) We consider one such subresultant $s_0(x)T^\ell + c_1(x)T^{\ell-1} + \cdots + c_\ell(x)$ assuming that all previous subresultants have been shown to be 0. We can assume $s_0(x)$ to be invertible, replacing D_U by $D_U[1/s_0]$. We let a be the leading coefficient of $s_0(x)$ and we show $a = 0$. We write $b_i(x) = c_i(x)/s_0(x)$. Since $T^\ell + b_1(x)T^{\ell-1} + \cdots + b_\ell(x)$ divides $P(x,T)$ we have that $b_1(x), \ldots, b_\ell(x)$ are integral over $C[x]$ by Lemma 2.3. By Lemma 2.6, $b_1(x), \ldots, b_\ell(x)$ are in $C_1[1/a][x]$ with C_1 integral over C. By Corollary 2.11 and Lemmas 2.19 and 2.9, we have $1 = 0$ in $D_U[1/a]$ and hence $a = 0$ in D_U.

Here the proof of Proposition 2.17 is finished.

Lemma 2.20 *Let A be a reduced ring, $f \in A[X]$ a monic polynomial of degree d, $g \in A[X]$ and δ a bound for the degree of g. Let $j < d$ a nonnegative integer. The subresultant of f and g in degree j, denoted* $\mathrm{Sres}_{j,X,d,\delta}(f,g) = Sr_j(X)$ *is a well defined polynomial of degree $\leq j$: it does not depend on δ. We let $Sr_d = f$. Let us denote s_j the coefficient of X^j in $Sr_j(X)$. Then we have:*

1. *$Sr_j(X)$ belongs to the ideal $\langle f, g\rangle$ of $A[X]$ $(0 \leq j \leq d)$.*
2. *Let $\ell > 0$, $\ell \leq d$. If $s_k = 0$ for $k < \ell$ and s_ℓ is invertible, then:*
   - *$Sr_k(X) = 0$ for $k < \ell$.*
   - *$Sr_\ell(X)$ divides $f(X)$ and $g(X)$ in $A[X]$.*

Proof. 1. This is a classical result.
2. Since the results are well known when A is a field, the lemma follows by using the formal Nullstellensatz. □

3 Proof of ZMT

It is more convenient for a proof "by induction on n" to use the following version 3.1.

Theorem 3.1 (ZMT à la Peskine, general form, variant)
Let A be a ring with an ideal $\mathfrak{I}$ and B be a finite extension of $A[x_1, \ldots, x_n]$ such that $B/\mathfrak{I}B$ is a finite $A/\mathfrak{I}$-algebra, then there exists $s \in 1 + \mathfrak{I}B$ such that $s, sx_1, \ldots, sx_n$ are integral over A.

Here, the precise hypothesis is $A \subseteq A[x_1, \dots, x_n] \subseteq B$, with B finite over $A[x_1, \dots, x_n]$. Clearly Theorems 1.3 and 3.1 are equivalent.

Case $n = 1$

Proposition 3.2 *Let A be a ring with an ideal $\mathfrak{J}$ and B be a finite extension of $A[x]$ such that $B/\mathfrak{J}B$ is a finite $A/\mathfrak{J}$-algebra, then there exists $s \in 1 + \mathfrak{J}B$ such that s, sx are integral over A.*

Proof. Let $f(X) \in A[X]$ a monic polynomial s.t. $f(x) \in \mathfrak{J}B$. By Lying Over $f(x)^m \in \mathfrak{J}A[x]$. This provides $P(X) = \sum_{i=0} a_i X^i \in A[X]$ such that $P(x) = 0$ and $1 \in \langle a_0, \dots, a_n \rangle \mod \mathfrak{J}A[x]$. Apply Lemma 2.5, item *2* with $R = A$. □

The induction step

Proposition 3.3 *Let A be a ring with an ideal $\mathfrak{J}$, B an extension of A with x in B such that B is integral over $A[x]$ and t in B such that xt is in $\sqrt{\mathfrak{J}B}$. There exist $b_0, \dots, b_n$ such that $\langle b_0, \dots, b_n \rangle$ meets $t^{\mathbb{N}} + \mathfrak{J}B$ and $b_0, \dots, b_n, b_0 x, \dots, b_n x$ are integral over A.*

Proof. By Lying Over $xt \in \sqrt{\mathfrak{J}A[x,t]}$ and we can assume as well that $B = A[x,t]$.
We apply Proposition 2.18 with R the integral closure of A in B, $S = R[x,t] = B$, $J = (R[x] : S)$. We get an $a \in J \subseteq R[x]$ with $a = t^m + y$, $y \in \mathfrak{J}S$. We have $at = t^{m+1} + yt \in R[x]$. Since $tx \in \sqrt{\mathfrak{J}S}$, $atx \in R[x] \cap \sqrt{\mathfrak{J}S}$ and by Lying Over $\exists e \in \mathbb{N}$, $(at)^e x^e = \sum_i \mu_i x^i$ with μ_i's in $\mathfrak{J}R$.
We write $at = p(x)$ with $p(X) \in R[X]$, $q(X) = p(X)^e X^e - \sum_i \mu_i x^i$ written as $\sum_{i=0}^{\ell} a_i X^i$ in $R[x][X]$ and $Q(X) = p(X)^e X^e - \sum_i \mu_i X^i \in R[X]$. We have $Q(x) = q(x) = 0$ and $\mathrm{c}_X(p^e) = \mathrm{c}_X(q) = \mathrm{c}_X(Q) \mod \mathfrak{J}R[x]$.
Let $R' = R[x]/\mathfrak{J}R[x]$. In R' we have $at = p(x) \in \mathrm{c}_X(p)$ and $\sqrt{\mathrm{c}_X(p)} = \sqrt{\mathrm{c}_X(Q)}$ by Gauss-Joyal. Remark that $t^{m+1} = at - yt$ implies that $t \in \sqrt{\mathrm{c}_X(p)} + \mathfrak{J}S$.
If n is a bound for the degree of Q, by Lemma 2.5 we get $b_0, \dots, b_n \in R[x]$ integral over R s.t. $b_0 x, \dots, b_n x$ avec integral over R and $\langle b_0, \dots, b_n \rangle = \mathrm{c}_X(Q)$.
Finally we get $t \in \sqrt{\mathrm{c}_X(p)} + \mathfrak{J}S = \sqrt{\langle b_0, \dots, b_n \rangle} + \mathfrak{J}S$ □

Corollary 3.4 *Let A be a ring with an ideal $\mathfrak{J}$, B an extension of A with x in B such that B is integral over $A[x]$, $p(X) \in A[X]$ a monic polynomial and t in B such that $p(x)t$ is in $\sqrt{\mathfrak{J}B}$. There exist $b_0, \dots, b_n$ such that $\langle b_0, \dots, b_n \rangle$ meets $t^{\mathbb{N}} + \mathfrak{J}B$ and $b_0, \dots, b_n, b_0 x, \dots, b_n x$ are integral over A.*

Proof. Let $y = p(x)$, then x is integral over $A[y]$. Applying Proposition 3.3 with y instead of x, we get $b_0, \dots, b_n$ such that $\langle b_0, \dots, b_n \rangle$ meets $t^{\mathbb{N}} + \mathfrak{J}B$ and $b_0, \dots, b_n, b_0 y, \dots, b_n y$ are integral over A. We say that this implies $b_j x$'s are integral over A. If the integral dependance of $b_j y$ over A is given by a polynomial of degree d and p is of degree m, multiplying the equation by $b_j^{(m-1)d}$, one gets an integral dependance equation of $b_j x$ over $A[b_j]$. □

Now we can prove Theorem 3.1.

Proof. We give the proof for $n = 2$, $x_1 = x$ and $x_2 = y$.
The induction from $n-1$ to n follows the same lines as the induction from 1 to 2.
First we apply Proposition 3.2 with $A' = A[x]$ instead of A, y replacing x. We get $s \in 1 + \mathfrak{I}B$ with s and sy integral over A'.
Let $p(X) \in A[X]$ be a monic polynomial such that $p(x) \in \mathfrak{I}B$. By Lying Over $p(x)$ is integral over $\mathfrak{I}A[x, y]$. We take $t = s^N$ for N big enough such that $tp(x)$ is integral over $\mathfrak{I}A[x, s, sy]$. By Lying Over again $tp(x)$ is in $\sqrt{\mathfrak{I}A[x, s]}$.
We apply Corollary 3.4 with A, x, t, replacing B by $A[x, s]$. We get $b_0, \ldots, b_n \in A[x, s]$ such that $\langle b_0, \ldots, b_n \rangle A[x, s]$ meets $t^{\mathbb{N}} + \mathfrak{I}A[x, s]$ and $b_0, \ldots, b_n, b_0x, \ldots, b_nx$ are integral over A. Since $t \in 1 + \mathfrak{I}B$, $1 \in \langle b_0, \ldots, b_n \rangle B/\mathfrak{I}B$. As $B/\mathfrak{I}B$ is finite over $A/\mathfrak{I}$, by Lying Over item *2* we have that $1 = \sum_{i=0}^{n} b_i g_i(\underline{b}) \bmod \mathfrak{I}B$ for some polynomials g_i with coefficients in A. Let $w = \sum_{i=0}^{n} b_i g_i(\underline{b})$. Clearly w and wx are integral over A. Applying lemma 2.8 with $R = A$, $S = B$ gives $u = w^M s$ such that u, ux and uy integral over A, and we see that $w \in 1 + \mathfrak{I}B$. □

4 Henselian local rings

Remark. Section 5 is independant of section 4.

4.1 Simple zeroes in commutative rings

We consider an arbitrary commutative ring k, $\mathfrak{I} = \mathrm{Rad}(k)$ its Jacobson radical (so $1 + \mathfrak{I} \subseteq k^\times$) and a polynomial system

$$f_1(X_1, \ldots, X_n) = \cdots = f_n(X_1, \ldots, X_n) = 0 \qquad (*)$$

which has a simple zero at $(a_1, \ldots, a_n) = (\underline{a}) \in k^n$. This means

$$f_1(\underline{a}) = \cdots = f_n(\underline{a}) = 0 \ \text{ and } \ J_{\underline{f}}(\underline{a}) \in k^\times,$$

where $J_{\underline{f}}(\underline{X})$ is the Jacobian of the system, i.e. the determinant of the Jacobian matrix $\mathrm{Jac}_{\underline{f}}(\underline{X}) = (\partial f_j / \partial X_i)_{1 \le i,j \le n}$.

Then this zero is unique modulo $\mathfrak{I} = \mathrm{Rad}(k)$ and can be isolated in a pure algebraic way as shown by the next lemma.

Lemma 4.1 *Let us consider the above polynomial system* $(*)$*.*
Let $L = k[X_1, \ldots, X_n]/\langle f_1, \ldots, f_n \rangle = k[x_1, \ldots, x_n]$*,* $S = 1 + \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ *and* L_S *the corresponding "local algebra".*

1. *For* $i = 1, \ldots, n$*,* $x_i = a_i$ *in* L_S*, the natural morphism* $k \to L_S$ *is an isomorphism. Identifying* k *with its images in* L *and* L_S*, we have* $L = k \oplus \langle x_1 - a_1, \ldots, x_n - a_n \rangle L$ *and* $L_S = k = L/\langle x_1 - a_1, \ldots, x_n - a_n \rangle$*.*

2. *There exists an idempotent* e *in* S *such that* $ex_i = a_i$ $(i = 1, \ldots, n)$ *and* $L_S = L[1/e]$*.*

3. $(\underline{a})$ *is the unique zero of* $(*)$ *equal to* $(\underline{a})$ *modulo* $\mathfrak{I}$*.*

Proof. Making a translation we can replace $(a_1, \ldots, a_n)$ by $(0, \ldots, 0)$. The evaluation $g \mapsto g(\underline{0})$ defined on $k[\underline{X}]$ gives morphisms $L \to k$ and $L_S \to k$, which we shall note again $g \mapsto g(\underline{0})$. By composing $k \to L_S \to k$ or $k \to L \to k$ we get the identity map. So $L = k \oplus \langle x_1, \dots, x_n \rangle L$.

1 and *2*. After a linear change of variables using $\mathrm{Jac}(\underline{0})^{-1}$ we can assume that $\mathrm{Jac}(\underline{0}) = \mathrm{I}_n$, and we write $f_i(\underline{X}) = X_i - g_i(\underline{X})$ with $g_i(\underline{X}) \in \langle X_1, \dots, X_n \rangle^2$. So in L we have a matrix $M = M(\underline{x}) \in \mathbb{M}_n(\langle x_1, \dots, x_n \rangle)$ satisfying

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = M \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

Writing $e(\underline{x}) = \det(\mathrm{I}_n - M)$ we get $e \in 1 + \langle x_1, \dots, x_n \rangle = S$ and $ex_i = 0$, which implies $eg = eg(\underline{0})$ for all $g \in L$. In particular $e^2 = e$ and $eh = e$ for $h \in S$, so $L_S = L[1/e]$. Also $x_i = 0$ in L_S and $g = g(\underline{0})$ for all $g \in L_S$.

3. Let $(y_1, \dots, y_n)$ be a zero with coordinates in $\mathfrak{I}$. So we have a k-morphism

$$L \to k, \quad g \mapsto g(y_1, \dots, y_n).$$

We can view it as a specialization $x_i \to y_i$. Item *2* gives $e(x_1, \dots, x_n) \in 1 + \langle x_1, \dots, x_n \rangle$ with $ex_i = 0$. Specialising x_i to y_i we obtain $e(y_1, \dots, y_n)y_i = 0$ with $e(y_1, \dots, y_n) \in 1 + \langle y_1, \dots, y_n \rangle \subseteq 1 + \mathfrak{I} \subseteq k^\times$. □

Remark. Viewing L as the ring of polynomial functions on the variety defined by the polynomial system $(*)$, the idempotent e defines a clopen Zariski subset, it gives two ways of isolating the zero $(\underline{a})$, either by considering the closed subset defined by $e = 1$ or by considering the open subset defined by making e invertible (the two subsets are identical). Moreover point *3* gives a third way of understanding the fact that the zero is isolated: it is the unique zero in the "infinitesimal neighborhood of $(\underline{a})$".

Approximate simple zeroes and Newton process

Here A is a commutative ring with an ideal $\mathfrak{I}$ and we consider a polynomial system with coefficients in A

$$f_1(X_1, \dots, X_n) = \cdots = f_n(X_1, \dots, X_n) = 0 \qquad (*)$$

Theorem 4.2 (Newton process, see e.g. [14, Section III-10])
Let $(\underline{a}) = (a_1, \dots, a_n) \in A^n$ be an approximate simple zero of $(*)$ modulo $\mathfrak{I}$: it gives a zero of $(*)$ in $A/\mathfrak{I}$ and the Jacobian $J_{\underline{f}}(\underline{a})$ of the system is invertible in $A/\mathfrak{I}$. So the Jacobian matrix $\mathrm{Jac}_{\underline{f}}(\underline{a})$ is invertible modulo $\mathfrak{I}$; let $U(\underline{a}) \in \mathbb{M}_n(A)$ be such an inverse modulo $\mathfrak{I}$. Compute

$$\begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} - U(\underline{a}) \begin{bmatrix} f_1(\underline{a}) \\ \vdots \\ f_n(\underline{a}) \end{bmatrix}.$$

Then $(b_1, \dots, b_n)$ is a zero of $(*)$ modulo $\mathfrak{I}^2$ and $\mathrm{Jac}(\underline{b})$ is invertible modulo $\mathfrak{I}^2$: one can take $U(\underline{b}) = U(\underline{a})(2\mathrm{I}_n - \mathrm{Jac}(\underline{b})U(\underline{a}))$.

Let $\mathfrak{J}$ be the Jacobson radical of the ideal $\mathfrak{I}$, i.e. the ideal of elements x such that each $y \in 1 + xA$ is invertible modulo $\mathfrak{I}$. Then Lemma 4.1 *3* tells us that $(\underline{a})$ is the unique zero modulo $\mathfrak{I}$ of $(*)$ equal to $(\underline{a})$ modulo $\mathfrak{J}$. Since $\mathfrak{J}$ is also the Jacobson radical of $\mathfrak{I}^2$, $(\underline{b})$ is the unique zero modulo $\mathfrak{I}^2$ of $(*)$ which is equal to $(\underline{b})$ modulo $\mathfrak{J}$. A fortiori $(\underline{b})$ is the unique zero modulo $\mathfrak{I}^2$ of $(*)$ which is equal to $(\underline{a})$ modulo $\mathfrak{I}$.

Remark. Newton process is used for constructing a zero of an Hensel system (see Context 4.3) when the Henselian local ring is a ring of formal power series. Nevertheless, this does not prove that the coordinates of the zero are inside the Henselization of the ring generated by the coefficients of the Hensel system. So the MHL can be seen an improved version of Newton process for the existence of the zero. On the other hand, Newton process is used in the proof of MHL (see the proof of Lemma 4.9).

4.2 Simple residual zeroes, Henselian rings

We fix the following context for sections 4.2 and 4.3.

Context 4.3 Let A be a local ring with detachable maximal ideal $\mathfrak{M}$, and $k = A/\mathfrak{M}$ its residual field (it is a discrete field). We consider a polynomial system

$$f_1(X_1, \ldots, X_n) = \cdots = f_n(X_1, \ldots, X_n) = 0 \qquad (*)$$

which has a residually simple zero at $(0, \ldots, 0)$: we have $f_i(0, \ldots, 0) = 0$ residually and the Jacobian of this system $J_{\underline{f}}(0, \ldots, 0)$ is in $A^\times$. In this case we will say that we have a *Hensel system*.

First we remark that if $(C, \mathfrak{M}_C)$ is a local A-algebra such that the system $(*)$ has a solution $(y_1, \ldots, y_n)$ with the y_i's in $\mathfrak{M}_C$, then this solution is unique by Lemma 4.1 *3*.

To this polynomial system we associate

the quotient ring	$B = A[X_1, \ldots, X_n]/\langle f_1, \ldots, f_n\rangle = A[x_1, \ldots, x_n]$
a maximal ideal of B	$\mathfrak{M}_B = \mathfrak{M} + \langle x_1, \ldots, x_n\rangle B \quad (\mathfrak{M}_B \supseteq \mathfrak{M}B)$
and the local ring	$B_{1+\mathfrak{M}_B}$ (usually denoted as $B_{\mathfrak{M}_B}$).

The ideal $\mathfrak{M}_B$ is maximal because it is the kernel of the morphism $B \to k$ sending $g(\underline{x})$ to $\overline{g}(\underline{0})$. This shows also that $B/\mathfrak{M}_B = A/\mathfrak{M}$ and hence the natural morphism $A \to B$ is injective. So we can identify A with its image in B and we have $B = A \oplus \langle x_1, \ldots, x_n\rangle B$. Nevertheless it is not at all evident that the morphism from A to $B_{1+\mathfrak{M}B}$ is injective (this fact will be proved in Corollary 4.6), so if we speak of $A \subseteq B_{1+\mathfrak{M}B}$ before the proof of Corollary 4.6 is complete, it is an *abus de langage* and it is needed to replace A by its image in $B_{1+\mathfrak{M}B}$.

It can be easily seen that the natural morphism $\varphi : A \to B_{1+\mathfrak{M}_B}$ satisfies the following *universal property*:
φ is a *local morphism* (i.e., $\varphi(x) \in (B_{1+\mathfrak{M}_B})^\times$ implies $x \in A^\times$) and for every local morphism $\psi : A \to C$ such that $(y_1, \ldots, y_n)$ is a solution of $(*)$ with the y_i's in the maximal ideal of C, there exists a unique local morphism $\theta : B \to C$ such that $\theta \circ \varphi = \psi$.

Since $B_{1+\mathfrak{M}_B}$ satisfies this universal property w.r.t. the system $(*)$ we introduce the notation

$$B_{1+\mathfrak{M}_B} = A_{[\![f_1,\ldots,f_n]\!]}.$$

The following version of MHL is a kind of "primitive element theorem".

Theorem 4.4 (Multivariate Hensel Lemma)
We consider a Hensel system as in Context 4.3 and we use preceeding notations. Then the local ring $A_{[\![f_1,\ldots,f_n]\!]} = B_{1+\mathfrak{M}_B}$ can also be described with only one polynomial equation $f(X)$ such that $f(0) \in \mathfrak{M}$ and $f'(0)$ invertible. More precisely there exist

– an $y \in \mathfrak{M}_B$,

– a monic polynomial $f(X) \in A[X]$ with $f(y) = 0$ and $f'(0) \in 1 + \mathfrak{M}$ (thus $f'(y) \in 1 + \mathfrak{M}_B$),

such that

– each x_i belongs to $A[y]_{1+\mathfrak{M}+yA[y]}$,

– the natural morphism $A_{[\![f]\!]} \to B_{1+\mathfrak{M}_B}$ sending x to y is an isomorphism (x is X viewed in $A_{[\![f]\!]}$).

In short $A_{[\![f_1,\ldots,f_n]\!]} = A_{[\![f]\!]}$.

Before proving Theorem 4.4 we state some corollaries.

A local ring where each equation of the preceeding form (a monic polynomial with a simple residual zero) has a solution residually 0 is said to be *Henselian*.

As immediate consequence of the MHL one has the following.

Corollary 4.5 *Let $(A, \mathfrak{m})$ be a Henselian local ring. Assume that a polynomial system $(f_1, \ldots, f_n)$ in $A[X_1, \ldots, X_n]$ has a residually simple zero at $(0, \ldots, 0)$. Then the system has a (unique) solution in A^n with coordinates in $\mathfrak{m}$.*

Corollary 4.6 *The morphism $A \to A_{[\![f_1,\ldots,f_n]\!]}$ is faithfully flat. In particular it is injective and the divisibility relation is faithfully extended from A to $A_{[\![f_1,\ldots,f_n]\!]}$.*

Proof. It is sufficient to prove the assertions for $A_{[\![f]\!]}$ with a monic polynomial f. Since $A_{[\![f]\!]}$ is a localization of a free A-algebra, it is flat over A. As $A_{[\![f]\!]}/\mathfrak{M}_{A_{[\![f]\!]}} = A/\mathfrak{M}$ the morphism $A \to A_{[\![f]\!]}$ is local, hence faithfully flat. So for $a, b \in A$, a divides b in A iff a divides b in $A_{[\![f]\!]}$. □

4.3 Proof of the Multivariate Hensel Lemma

We begin by a slight transformation or our polynomial system in order to being able to get the hypotheses of ZMT for the ring associated to the new system.

Proposition 4.7 *Let a polynomial system*

$$f_1(X_1, \ldots, X_n) = \cdots = f_n(X_1, \ldots, X_n) = 0 \qquad (*)$$

which has a residually simple zero at $(0, \ldots, 0)$. We use preceeding notations for B and $\mathfrak{M}_B$.

One can find $f_{n+1}(X_1,\dots,X_n,X_{n+1}) \in A[X_1,\dots,X_{n+1}]$ such that for the new system

$$f_1(X_1,\dots,X_n) = \cdots = f_n(X_1,\dots,X_n) = f_{n+1}(X_1,\dots,X_n,X_{n+1}) = 0 \qquad (**)$$

we have again $f_{n+1}(0,\dots,0) \in \mathfrak{M}$, with Jacobian $J'(0,\dots,0)$ invertible and if we call

$$B' = A[x_1,\dots,x_n,x_{n+1}] = A[X_1,\dots,X_n,X_{n+1}]/\langle f_1,\dots,f_{n+1}\rangle$$

then $x_1,\dots,x_n,x_{n+1} \in \mathfrak{M}B'$ (this means $\mathfrak{M}B' = \mathfrak{M}_{B'}$), and the natural morphism $B_{\mathfrak{M}_B} \to B'_{\mathfrak{M}B'}$ is an isomorphism.
In short with the new system we have $x_1,\dots,x_{n+1} \in \mathfrak{M}A[x_1,\dots,x_{n+1}]$ and $A_{[\![f_1,\dots,f_n]\!]} = A_{[\![f_1,\dots,f_{n+1}]\!]}$.

Proof. Applying Lemma 4.1 to the residual system we get $e(X_1,\dots,X_n)$ such that in $k[x_1,\dots,x_n]$ we have $e^2 = e$, $ex_i = 0$. So if we consider the localization $B[1/e]$ we get residually $k[x_1,\dots,x_n,1/e] = k$, more precisely $e = 1$ and $x_i = 0$ in $k[x_1,\dots,x_n,1/e]$. In other words if we introduce a new variable T and the equation $Te(X_1,\dots,X_n) = 1$ we get a new polynomial system which has residually only one zero $(0,\dots,0,1)$. In order to get a Hensel system we introduce the variable X_{n+1} $(= 1-T)$ with the equation $1-(1-X_{n+1})e(X_1,\dots,X_n)$, and $(0,\dots,0)$ is the unique residual zero. Moreover if we call $J'(x_1,\dots,x_{n+1})$ the Jacobian of the new system in B' then $J'(x_1,\dots,x_{n+1}) = J_{\underline{f}}(x_1,\dots,x_n)e(x_1,\dots,x_n)$ and $J'(0,\dots,0) = J_{\underline{f}}(0,\dots,0)$ mod $\mathfrak{M}$ is invertible.
NB: Let us note that there is a little abuse of notations: we have $e(x_1,\dots,x_n) = 1$ in $k[x_1,\dots,x_{n+1}] = B'/\mathfrak{M}_{B'}$ but in general $e(x_1,\dots,x_n) \neq 1$ in $k[x_1,\dots,x_n] = B/\mathfrak{M}_B$, meaning that the morphism $k[x_1,\dots,x_n] \to k[x_1,\dots,x_{n+1}]$ is not injective. It would be necessary to change the names of the x_i's when changing the ring! □

In the following we assume w.l.o.g. that the system $(*)$ satisfies $x_1,\dots,x_n \in \mathfrak{M}B$.

Applying Theorem 1.3 to $B = A[x_1,\dots,x_n]$, $\mathfrak{M} \subseteq A$ and $x_1,\dots,x_n \in \mathfrak{M}B$ (so $B/\mathfrak{M}B = A/\mathfrak{M}$) we get an $s \in 1+\mathfrak{M}B$ such that $s, sx_1,\dots,sx_n$ are integral over A. So $s = S(x_1,\dots,x_n)$, where $S \in 1+\mathfrak{M}A[X_1,\dots,X_n]$). We are going to prove the following proposition, which clearly implies Theorem 4.4 if the given polynomial f is monic.

Proposition 4.8 *We can construct a polynomial $h(T) \in A[T]$ such that $h(s) = 0$, $h'(s) \in 1+\mathfrak{M}B$ (more precisely, $h(T) = T^N(T-1)$ modulo $\mathfrak{M}A[T]$), the x_i are expressed as rational fractions in s with denominator in $1+\mathfrak{M}+(s-1)A[s]$, and letting $f(X) = h(1+X)$, the natural morphism $A_{[\![f]\!]} \to B_{1+\mathfrak{M}B} = A_{[\![f_1,\dots,f_n]\!]}$ sending x to $s-1$ is an isomorphism.*

Proof. Let $D = A[s, sx_1,\dots,sx_n]$ and therefore we have $A \subseteq A[s] \subseteq D \subseteq B$. We call $m_0 = 1$, m_1, …, m_ℓ monomials in the (sx_i)'s such that $m_0,\dots,m_\ell$ generate D as an $A[s]$-module and we can also assume that $m_i = sx_i$ for $i = 1,\dots,n$. We have $D = A[s] + m_1D + \cdots + m_\ell D$.
Let $\mathfrak{M}_D = \mathfrak{M}B \cap D$ and $\mathfrak{M}_{A[s]} = \mathfrak{M}B \cap A[s]$.

Since $m_1, \dots, m_\ell \in \mathfrak{M}_D$ we have $\mathfrak{M}_D = \mathfrak{M}_{A[s]} + m_1 D + \cdots + m_\ell D$.
As $s-1 \in \mathfrak{M}_{A[s]}$ and $A[s] = A[s-1] = A+(s-1)A[s]$ we have $\mathfrak{M}_{A[s]} = \mathfrak{M}+(s-1)A[s]$.
Notice that for all $v \in B$ there exists an exponent r such that $s^r v \in D$. Moreover if $v \in \mathfrak{M}B$, there exists an exponent r such that $s^r v \in \mathfrak{M}D$. In particular, since $m_j \in \mathfrak{M}B$ there exists an exponent r_0 such that all $s^{r_0} m_j \in \mathfrak{M}D$ ($j = 1, \dots, \ell$).
We write this fact as

$$s^{r_0} m_j = \left(\sum\nolimits_{i=1}^{\ell} \mu_{ij}(s) m_i\right) + \mu_{0j}(s)$$

where $\mu_{ij}(s) \in \mathfrak{M}A[s]$ for all i, j.
Let $M(s) = (\mu_{ij}(s))_{1 \le i,j \le \ell}$. We have then

$$s^{r_0} \begin{bmatrix} m_1 \\ \vdots \\ m_\ell \end{bmatrix} = M(s) \begin{bmatrix} m_1 \\ \vdots \\ m_\ell \end{bmatrix} + \begin{bmatrix} \mu_{01}(s) \\ \vdots \\ \mu_{0\ell}(s) \end{bmatrix}.$$

Let $d(T) = \det(T^{r_0}\, \mathrm{I}_\ell - M(T))$, multiplying by the adjoint matrix $P(s)$ we get

$$d(s) \begin{bmatrix} m_1 \\ \vdots \\ m_\ell \end{bmatrix} = P(s) \begin{bmatrix} \mu_{01}(s) \\ \vdots \\ \mu_{0\ell}(s) \end{bmatrix} \in \mathbb{M}_{\ell,1}(\mathfrak{M}A[s]).$$

Summing up. We have found a polynomial $d(T) \in A[T]$ such that:

i) $d(T) = T^N$ modulo $\mathfrak{M}A[T]$ for some N, and so $d(s)s^r \in 1 + \mathfrak{M}_{A[s]}$ for all $r \ge 0$,

ii) one has $d(s)m_j = \nu_j(s) \in \mathfrak{M}A[s]$, this implies $d(s)\mathfrak{M}_D \subseteq \mathfrak{M}_{A[s]}$,

iii) given an arbitrary $v \in \mathfrak{M}B$ one has an exponent r such that $s^r d(s) v \in \mathfrak{M}A[s]$,

Let q be an exponent such that $s^q d(s)(s-1) \in \mathfrak{M}A[s]$ and let us define $h(T) = d(T)T^q(T-1) - \mu(T) \in A[T]$. So $h(s) = 0$ and $h(T) = T^{N+q}(T-1)$ modulo $\mathfrak{M}A[T]$. Notice that $h'(1) \in 1 + \mathfrak{M}$, which implies that s is a root of $h(T)$ which is residually simple.

Now we finish the proof of Proposition 4.8 using the following general lemma. □

Lemma 4.9 *Let $h(T) \in A[T]$ such that $h(s) = 0$ and $h'(1) \in 1 + \mathfrak{M}$.*
Let us set $f(X) = h(1+X)$, $A[x] = A[X]/\langle f(X) \rangle$, $t = 1+x$, $A_{[\![f]\!]} = A[x]_{1+\mathfrak{M}+xA[x]}$.
Let $\theta : A_{[\![f]\!]} \to B_{1+\mathfrak{M}B} = A_{[\![f_1,\dots,f_n]\!]}$ be the natural morphism sending x to $s-1$ (and t to s) given by the universal property of $A_{[\![f]\!]}$.
Then θ is in fact an isomorphism.

Proof. In order to prove that θ is an isomorphism, it is sufficient to find a zero $(z_1, \dots, z_n)$ of the system $(*)$ in $A_{[\![f]\!]}$ with coordinates z_i in the maximal, and such that

– $\theta(z_i) = x_i$ for each i,

– the natural morphism $B_{1+\mathfrak{M}B} \to A_{[\![f]\!]}$ sending $(x_1, \dots, x_n)$ to $(z_1, \dots, z_n)$ sends s to t.

We have $d(s)sx_i = \nu_i(s)$ where $\nu_i(T) \in \mathfrak{M}A[T]$. We let $q(T) = Td(T)$.

We have $q(T) \in T^{N+1}(T-1) + \mathfrak{M}A[T]$, $t \in 1 + \mathfrak{M}A_{[\![f]\!]}$ and $q(t) \in 1 + \mathfrak{M}A_{[\![f]\!]}$. We let

$$z_i = \nu_i(t)/q(t) \in \mathfrak{M}A_{[\![f]\!]}$$

and we get $\theta(z_i) = \nu_i(s)/q(s) = x_i$ for each i.
Let

$$\mathfrak{I} = \langle f_1(z_1, \ldots, z_n), \ldots, f_n(z_1, \ldots, z_n)\rangle$$

as ideal of $A_{[\![f]\!]}$. We get $\mathfrak{I} \subseteq \mathfrak{M}A_{[\![f]\!]}$.
We are going to show that $\mathfrak{I} = \mathfrak{I}^2$, so $\mathfrak{I} \subseteq \mathfrak{I}\,\mathfrak{M}'$, where $\mathfrak{M}' = \mathfrak{M}A_{[\![f]\!]} + xA_{[\![f]\!]}$ is the maximal ideal of $A_{[\![f]\!]}$. This implies $\mathfrak{I} = 0$ by Nakayama's Lemma. This will show that $(z_1, \ldots, z_n)$ is a zero of $(*)$ with coordinates in $\mathfrak{M}'$.
By Newton process we can construct a zero modulo $\mathfrak{I}^2$, let us call it $(y_1, \ldots, y_n)$. The system $(*)$ has the zero $(y_1, \ldots, y_n)$ residually null in the local ring $A_{[\![f]\!]}/\mathfrak{I}^2$. By the universal property of $A_{[\![f_1,\ldots,f_n]\!]}$ there is a morphism $\lambda : A_{[\![f_1,\ldots,f_n]\!]} \to A_{[\![f]\!]}/\mathfrak{I}^2$ sending x_i to y_i.
We let $y = S(y_1, \ldots, y_n)$, so $\lambda(s) = y \bmod \mathfrak{I}^2$, $h(y) = \lambda(h(s)) \bmod \mathfrak{I}^2$, i.e. $h(y) = 0 \bmod \mathfrak{I}^2$.
Since $h(t) = 0$, $h'(t) \in A_{[\![f]\!]}{}^{\times}$, $t = y = 1 \bmod \mathfrak{M}'$ we write

$$h(y) = h(t) + (t-y)(h'(t) + (t-y)h_1(t,y)),$$

we have $h'(t) + (t-y)h_1(t,y) \in A_{[\![f]\!]}{}^{\times}$ and we get $t - y \in \mathfrak{I}^2$.
We have $0 = \lambda(q(s)x_i - \nu_i(s)) = q(y)y_i - \nu_i(y)$ in $A_{[\![f]\!]}/\mathfrak{I}^2$, $q(y)y_i - q(t)y_i \in \mathfrak{I}^2$ and $\nu_i(t) - \nu_i(y) \in \mathfrak{I}^2$, so $q(t)y_i - \nu_i(t) \in \mathfrak{I}^2$, i.e. $y_i = z_i \bmod \mathfrak{I}^2$. Finally

$$0 = \lambda(f_i(x_1, \ldots, x_n)) = f_i(y_1, \ldots, y_n) = f_i(z_1, \ldots, z_n) \bmod \mathfrak{I}^2.$$

This shows that $\mathfrak{I} \subseteq \mathfrak{I}^2$, so $\mathfrak{I} = 0$. Now, since $(z_1, \ldots, z_n)$ is a zero of $(*)$ residually null in $A_{[\![f]\!]}$, by the universal property of $A_{[\![f_1,\ldots,f_n]\!]}$ we can see λ as a morphism from $A_{[\![f_1,\ldots,f_n]\!]}$ to $A_{[\![f]\!]}$ sending x_i to $y_i = z_i$.
Finally, we show that $\lambda(s) = t$. This follows from $h(\lambda(s)) = \lambda(h(s)) = 0$ and $s \in 1 + \mathfrak{M}A[x_1, \ldots, x_n]$ in B which implies $\lambda(s) \in 1 + \mathfrak{M}A[y_1, \ldots, y_n] \subseteq 1 + \mathfrak{M}A_{[\![f]\!]}$ so $h'(\lambda(s)) \in 1 + \mathfrak{M}A_{[\![f]\!]}$. □

In order to get Theorem 4.4 from Proposition 4.8 we use the following lemma.

Lemma 4.10 (see [1, Lemma 5.3])
Let $(A, \mathfrak{M})$ be a local ring, $f(X) = a_nX^n + \cdots + a_1X + a_0$, with $a_1 \in A^{\times}$ and $a_0 \in \mathfrak{M}$. There exists a monic polynomial $g(X) \in A[X]$, $g(X) = X^n + \cdots + b_1X + b_0$, with $b_1 \in A^{\times}$ and $b_0 \in \mathfrak{M}$, such that the following equality holds in $A(X)$ (the Nagata localization of $A[X]$):

$$a_0 \cdot g(X) = (X+1)^n f\left(\frac{-a_0a_1^{-1}}{X+1}\right).$$

Moreover $A_{[\![f]\!]}$ is isomorphic to $A_{[\![g]\!]}$.

Proof. We have

$$\begin{aligned} X^n f\left(\tfrac{-a_0a_1^{-1}}{X}\right) &= a_0 \cdot \left(X^n - X^{n-1} + a_0 \textstyle\sum_{j=2}^{n}(-1)^j a_j a_0^{j-2} a_1^{-j} X^{n-j}\right) \\ &= a_0 h(X) \end{aligned}$$

with

$$h(X) = X^n - X^{n-1} + a_0 \sum_{j=2}^{n} (-1)^j a_j a_0^{j-2} a_1^{-j} X^{n-j} = X^n - X^{n-1} + a_0 \ell(X)$$

We let $g(X) = h(X+1) = X^n + \cdots + b_1 X + b_0$. It is a monic polynomial, with constant term $b_0 = g(0) = h(1) = a_0 \ell(1) \in \mathfrak{M}$, and linear term $b_1 = g'(0) = h'(1) = 1 + a_0 \ell'(1) \in 1 + \mathfrak{M}$. □

4.4 An example of Multivariate Hensel Lemma

In this section we analyse an example where A is the local ring $\mathbb{Q}[a,b]_S$, S being the monoid of elements $p(a,b) \in \mathbb{Q}[a,b]$ such that $p(0,0) \neq 0$. We take next $B = A[x,y]$ where x, y are defined by the equations

$$-a + x + bxy + 2bx^2 = 0, \qquad -b + y + ax^2 + axy + by^2 = 0$$

We shall compute $s \in B$ integral over A such that sx, sy integral over B and $s = 1$ mod. $\mathfrak{M}B$.

Following the proof we apply Proposition 3.2 and we take $t = 1 + ax + by$. We have that $t = 1$ mod. $\mathfrak{M}B$ and t, ty integral over $A[x]$. We have even $ty = y + axy + by^2 = b - ax^2$ in $A[x]$. The equation for t is

$$t^2 - (1+ax)t - b + ax^2$$

We have then

$$tx = x + ax^2 + bxy = a + (a-2b)x^2.$$

Notice that we are now in the situation of the proof of Proposition 2.17 with $Q(X,T) = TX - (a + (a-2b)X^2)$. Since Q has degree 1 we get without extra work and so

$$(t - (a-2b)x)x = a$$

If we take $w = t - (a-2b)x = 1 + 2bx + by$ we have $w = 1$ mod. $\mathfrak{M}B$ and wx in A and w is integral over A. Indeed w is integral over $A[1/w]$ since x is in $A[1/w]$ and w is integral over $A[x]$.

If we take $u = tw^2$ we have u, ux, uy integral over A. Indeed, wx is in A and since $t^2 - (1+ax)t - b + ax^2 = 0$ we have tw and hence u integral over A. Since $ty = b - ax^2$ we have $uy = bw^2 - a(wx)^2$ integral over A. Finally $ux = (tw)(wx)$ is integral over A.

It can be checked that u is a root of a monic polynomial f of degree 4 of the form $U^3(U-1)$ residually.

$$\begin{gathered}
-u^4 + (1 + 4\,a\,b + a^2 + 3\,b^2)\,u^3 \\
+b\,(b^5 + 8\,a\,b^4 + 7\,a^2\,b^3 - a^3\,b^2 - 4\,b\,a^4 + a^5 - 6\,a^2\,b - a^3 + 4\,a\,b^2)\,u^2 \\
-a^2\,b^2\,(a-b)\,(a+2\,b)\,(2\,b^2 - 9\,a\,b + a^2)\,u + a^4\,b^3\,(a-4\,b)\,(a+2\,b)^2\,(a-b)^2 = 0
\end{gathered}$$

5 Structure of quasi finite algebras

Let us recall that in classical mathematics an A-algebra B is said to be quasi-finite if it is of finite type and if prime ideals of B lying over any prime ideal of A are incomparable.

This last requirement means that the morphism $A \to B$ is zero-dimensional. A constructive characterization of zero-dimensional morphisms uses the zero-dimensional reduced ring $A^\bullet$ generated by A.

A zero-dimensional reduced ring is characterized by the fact that every element a possesses a quasi inverse: an element b such that $a^2b = a$ and $b^2a = b$. Such a ring is also said to be Von Neuman regular or absolutely flat. The element ab is an idemptent e_a. In the component $A[1/e_a]$, a is invertible, and $a = 0$ in the other component $A/\langle e_a\rangle$.

From an algorithmic point of view this implies that algorithms for discrete fields are easily transformed in algorithms for zero-dimensional reduced rings (for more details see [14, Chapter 4]).

The ring $A^\bullet$ can be obtained as a direct limit of rings

$$A[a_1^\bullet, a_2^\bullet, \dots, a_n^\bullet] \simeq (A[T_1, T_2, \dots, T_n]/\mathfrak{a})_{\mathrm{red}}$$

with $\mathfrak{a} = \langle (a_iT_i^2 - T_i)_{i=1}^n, (T_ia_i^2 - a_i)_{i=1}^n \rangle$ (for more details see [14, section 11.4]). The direct limit is along the p.o. set of finite sequences of elements of A, ordered by $(a_1, \dots, a_n) \preceq (b_1, \dots, b_m)$ iff one has (for each i) $b_{k_i} = a_i$ for some map $\{1, \dots, n\} \xrightarrow{k} \{1, \dots, m\}$.

In classical mathematics we obtain the following equivalence.

Proposition 5.1 *Let $\varphi : A \to B$ a morphism of commutative rings.*

1. *Prime ideals of B lying over any prime ideal of A are incomparable.*
2. *The ring $A^\bullet \otimes_A B$ is a zero-dimensional ring.*

The morphism $A \to B$ is not required to be injective, but the proposition involves only the structure of B as $\varphi(A)$-algebra.

The second item is taken to be the correct definition of zero-dimensional morphisms in constructive mathematics.

This gives also a good definition of *quasi-finite morphisms* in constructive mathematics: indeed a *quasi-finite A-algebra* is an algebra B of finite type such that the structure morphism $A \to B$ is zero-dimensional.

We have the following concrete characterization of zero-dimensional morphisms for algebras of finite type.

Proposition 5.2 *Let B be an A-algebra of finite type. The following are equivalent.*

1. *The structure map $A \to B$ is a zero dimensional morphism.*
2. *There exist $a_1, \dots, a_p \in A$ such that for each $I \subseteq \{1, \dots, p\}$, if we let $I' = \{1, \dots, p\} \setminus I$, $\mathfrak{a}_{\underline{a},I} = \langle a_i,\ i \in I\rangle$, $\alpha_{\underline{a},I'} = \prod_{i\in I'} a_i$ and $A_{(\underline{a},I)} = \left(A/\mathfrak{a}_{\underline{a},I}\right)\left[\frac{1}{\alpha_{\underline{a},I'}}\right]$ then the ring $B_{(\underline{a},I)}$ is integral over $A_{(\underline{a},I)}$.*

Let us insist here on the fact that the equivalence in Proposition 5.2 has a constructive proof.

Theorem 5.3 (ZMT à la Raynaud, [15])
Let $A \subseteq B = A[x_1, \dots, x_n]$ be rings such that the inclusion morphism $A \to B$ is zero dimensional (in other words, B is quasi-finite over A). Let C be the integral closure of A in B. Then there exist elements $s_1, \dots, s_m$ in C, comaximal in B, such that all $s_i x_j \in C$.
In particular for each i, $C[1/s_i] = B[1/s_i]$. Moreover letting $C' = A[(s_i), (s_i x_j)]$, which is finite over A, we get also $C'[1/s_i] = B[1/s_i]$ for each i.

Proof. The concrete hypothesis is item *2.* in Proposition 5.2. We have to find elements $s_1, \dots, s_m$ integral over A, comaximal in B, such that all $s_i x_j$ are integral over A.
The proof is by induction on p, the case $p = 0$ being trivial (in this case B is finite over A by hypothesis).
Assume we have the conclusion for $p - 1$ and let $a = a_p$. The induction hypothesis is applied to the morphisms $A/aA \to B/aB$ and $A[1/a] \to B[1/a]$.
First we get $s_1, \dots, s_m$ integral over A/aA, comaximal in B/aB with all $s_i x_j$ integral over A/aA. Let $B' = A[(s_i), (s_i x_j)]$ $(1 \leq i \leq m,\ 1 \leq j \leq n)$. Applying Theorem 1.3 to $A \subseteq B'$ and $\mathfrak{I} = aA$ we obtain $w \in 1 + aB'$ such that all ws_i's and $ws_i x_j$'s are integral over A.
Second, we get $t_1, \dots, t_q$ integral over $A[1/a]$, comaximal in $B[1/a]$ with all $t_i x_j$ integral over $A[1/a]$. This gives, for N big enough, $a^N \in \langle t_1, \dots, t_q \rangle B$ and all $a^N t_i$'s and $a^N t_i x_j$'s integral over A.
Since $1 \in \langle s_1, \dots, s_m, a \rangle B$ and $1 \in \langle w, a \rangle B$, we have

$$1 \in \langle ws_1, \dots, ws_m, a^{2N} \rangle B \subseteq \langle ws_1, \dots, ws_m, a^N t_1, \dots, a^N t_q \rangle.$$

So we have our conclusion with the family $(ws_1, \dots, ws_m, a^N t_1, \dots, a^N t_q)$. $\square$

References

[1] M. Alonso, H. Lombardi, H. Perdry. *Elementary Constructive Theory of Henselian Local Rings.* Math. Logic Quarterly **54** (3), (2008), 253–271. 2, 17

[2] M. Atiyah, L. MacDonald. *Introduction to Commutative Algebra.* Addison Wesley series in Mathematics, (1969). 4

[3] S. Basu, R. Pollack & M.-F. Roy *Algorithms in Real Algebraic Geometry.* Springer-Verlag. 2nd edition (2006). 9

[4] E. Bishop, D. Bridges. *Constructive Analysis.* Springer-Verlag (1985). 2

[5] D. Bridges, F. Richman. *Varieties of Constructive Mathematics.* London Math. Soc. LNS 97. Cambridge University Press (1987). 2

[6] T. Coquand. *On seminormality.* J. Algebra, **305**, (2006), 577–584. 2

[7] T. Coquand. *Space of valuations.* Ann. Pure Appl. Logic, **157**, (2009), 97–109. 2

[8] T. Coquand, H. Lombardi, C. Quitté. *Generating non noetherian modules constructively.* Manuscripta Math., **115**, (2004), 513–520. 2

[9] T. Coquand, C. Quitté. *Constructive finite free resolutions.* Manuscripta Math., **137**, (2012), 331–345. 2

[10] T. Coquand, H. Lombardi, P. Schuster *Spectral schemes as ringed lattices.* Ann. Math. Artif. Intell., **56**, (2009), 339–360. 2

[11] L. Ducos, H. Lombardi, C. Quitté , M. Salou. *Théorie algorithmique des anneaux arithmétiques, de Prüfer et de Dedekind.* Journal of Algebra. **281**, (2004), 604–650. 2

[12] E. Hallouin. *Parcours initiatique à travers la théorie des valuations.* technical report. Université de Poitiers, (1997). 5

[13] A. Grothendieck. *Éléments de Géométrie Algébrique IV.* 2

[14] H. Lombardi, C. Quitté. *Algèbre Commutative, Méthodes Constructives.* Calvage & Mounet, (2011). 2, 12, 19

[15] M. Raynaud. *Anneaux locaux henséliens.* Springer Lecture Notes in Mathematics No 169, (1970). 2, 3, 20

[16] R. Mines, F. Richman and W. Ruitenburg. *A Course in Constructive Algebra.* Springer-Verlag, (1988) 2

[17] C. Peskine. *Une généralization du "main theorem" de Zariski.* Bull. Sci. Math. (2) 90 (1966) 119–127. 2

[18] C. Peskine. *An Algebraic Introduction to Complex Projective Geometry: Commutative Algebra.* Cambridge University Press, (1996). 2

[19] I. Yengui. *Making the use of maximal ideals constructive.* Theoret. Comput. Sci., **392**, (2008), 174–178. 2

[20] O. Zariski. *Analytical irreducibility of normal varieties.* Annals of Math. 49 (1948) 352–361. 2