# *A constructive approach to Zariski Main Theorem*

**MAP meeting, Logroño, november 2010**

H. Lombardi, Besançon.
joint work with T. Coquand, Göteborg.
and MariEmi Alonso, Madrid
Henri.Lombardi@univ-fcomte.fr, http://hlombardi.free.fr

A printable version of these slides:

http://hlombardi.free.fr/publis/MAPLogronoDoc.pdf



## Abstract

*Zariski Main Theorem.* We study the constructive formulation and the constructive meaning of ZMT and some consequences.

## Outline

1. Isolated zeroes, field case
2. Isolated zeroes, local case
3. Isolated zeroes, general case
4. Simple zeroes, field case
5. Simple zeroes, local case
6. Multidimensional Hensel Lemma



## *0. Isolated zeroes, preliminaries*

Let $\mathbf{A}$ be a commutative ring, $f_1, \dots, f_s$ polynomials in $\mathbf{A}[X_1, \dots, X_n]$.
To this polynomial system is associated the **quotient algebra**

$$\mathbf{B} = \mathbf{A}[X_1, \dots, X_n]/\langle f_1, \dots, f_s \rangle = \mathbf{A}[x_1, \dots, x_n].$$

This is a general finitely presented $\mathbf{A}$-algebra. We shall speak of a **fp-algebra**.
A zero $\underline{a} = (a_1, \dots, a_n)$ of the polynomial system in an $\mathbf{A}$-algebra $\mathbf{C}$ corresponds to a morphism $\varphi_{\underline{a}} : \mathbf{B} \to \mathbf{C}$ sending $x_i$ to $a_i$ $(i = 1, \dots, n)$.
We are interested in “isolated zeros” of polynomial systems.

**Isolated zeroes, preliminaries**

If $\underline{a} = (a_1, \ldots, a_n)$ is a zero of $\mathbf{B}$ with coordinates in $\mathbf{A}$ we consider:
**the ideal of** $\underline{a}$: $\mathfrak{m}_{\underline{a}} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle \subseteq \mathbf{B}^n$
**the local algebra at** $\underline{a}$: $(1 + \mathfrak{m}_{\underline{a}})^{-1}\mathbf{B} = \mathbf{B}_{1+\mathfrak{m}_{\underline{a}}}$
Recall what is a **local ring**:
a commutative ring for which $x + y$ invertible implies
$x$ invertible *or* $y$ invertible.
In a ring $\mathbf{C}$ the **Jacobson radical** is the ideal

$$\mathrm{Rad}(\mathbf{C}) = \left\{ x \in \mathbf{C} \,|\, 1 + x\mathbf{C} \subseteq \mathbf{C}^\times \right\} \subseteq \mathbf{C}.$$

The quotient $\mathbf{C}/\mathrm{Rad}\mathbf{C}$ is the **residue ring**. When $\mathbf{C}$ is a local ring, the residue algebra is a **field**: a local ring whose Jacobson radical is reduced to 0.



## 1. *Isolated zeroes, field case*

**Discrete field**: commutative ring $\mathbf{k}$ with:
every element is 0 *or* invertible.
**Zerodimensional reduced ring (Von Neuman regular ring)**: commutative ring $\mathbf{k}$ with:
for each element $x$ there is an idempotent $e_x$ such that
$x = 0$ modulo $e_x$ *and* $x$ is invertible modulo $1 - e_x$.
**Zerodimensional ring**: commutative ring $\mathbf{k}$ with:
for each element $x$ there is an idempotent $e_x$ such that
$x$ is nilpotent modulo $e_x$ *and* $x$ is invertible modulo $1 - e_x$.
If $\mathbf{B}$ is a fp $\mathbf{k}$-algebra and $\underline{a} = (a_1, \ldots, a_n)$ is a zero of $\mathbf{B}$ with coordinates in $\mathbf{k}$ the local algebra $\mathbf{B}_{1+\mathfrak{m}_{\underline{a}}}$ is a local ring whose residual ring is isomorphic to $\mathbf{k}$ through the morphism $\varphi_{\underline{a}} : \mathbf{B} \to \mathbf{k}$.



**Isolated zeroes, field case**

First we have a **local theorem**, which allows us to give a good definition of an **isolated zero** when the base ring is a discrete field.

**Theorem 1.** *For a discrete field* $\mathbf{k}$*, a fp-algebra* $\mathbf{B} = \mathbf{k}[x_1, \ldots, x_n]$ *and a zero* $\underline{a} = (a_1, \ldots, a_n)$ *with coordinates in* $\mathbf{k}$*, T.F.A.E.*

1. *The local algebra* $\mathbf{B}_{1+\mathfrak{m}_{\underline{a}}}$ *is zero-dimensional.*
2. *There is an idempotent* $e \in 1 + \mathfrak{m}_{\underline{a}}$ *such that* $\mathbf{B}_{1+\mathfrak{m}_{\underline{a}}} = \mathbf{B}[1/e]$.
3. *There is an element* $s$ *of* $\mathbf{B}$ *such that* $\mathbf{B}_{1+\mathfrak{m}_{\underline{a}}} = \mathbf{B}[1/s]$.

*If* $\mathbf{k}$ *is contained in an algebraically closed field* $\mathbf{K}$*:*

4. *There is an element* $s(\underline{x})$ *of* $\mathbf{B}$ *such that* $\underline{a}$ *is the unique zero of* $\mathbf{B}$ *with coordinates in* $\mathbf{K}$ *and* $s(\underline{a})$ *invertible.*

**Isolated zeroes, field case**

There is a corresponding **global theorem**.

**Theorem 2.** *For a discrete field* $\mathbf{k}$ *and a fp-algebra* $\mathbf{B} = \mathbf{k}[x_1, \ldots, x_n]$*, T.F.A.E.*

1. *The algebra* $\mathbf{B}$ *is a zero-dimensional ring.*
2. *The algebra* $\mathbf{B}$ *is a finite dimensional* $\mathbf{k}$*-vector space.*
3. *The elements* $x_i$ *of* $\mathbf{B}$ *are integral over* $\mathbf{k}$*.*

*If* $\mathbf{k}$ *is contained in an algebraically closed field* $\mathbf{K}$*:*

4. *All zeroes of* $\mathbf{B}$ *with coordinates in* $\mathbf{K}$ *are isolated.*
5. *There are finitely many zeroes of* $\mathbf{B}$ *with coordinates in* $\mathbf{K}$*.*



## 2. Isolated zeroes, local case

Here we consider a polynomial system on a residually discrete local ring $(\mathbf{A}, \mathfrak{M})$ (the residue field $\mathbf{k} = \mathbf{A}/\mathfrak{M}$ is a discrete field).
If $\mathbf{B} = \mathbf{A}[x_1, \ldots, x_n]$ is the corresponding quotient algebra, we have residually $\mathbf{L} = \mathbf{B}/\mathfrak{M}\mathbf{B}$ corresponding to "the same" polynomial system read on $\mathbf{k}$ rather than on $\mathbf{A}$.
A natural problem is: assume $\mathbf{L}$ is finite over $\mathbf{k}$,

1. can we lift the zeroes in $\mathbf{A}$?
2. is $\mathbf{B}$ finite over $\mathbf{A}$? (i.e., is it a finitely generated $\mathbf{A}$-module? or equivalently, are the $x_i$'s integral over $\mathbf{A}$?)

An answer will be given by the Zariski Main Theorem (Grothendieck formulation).



**Isolated zeroes, local case**

We cannot be too optimistic.
Consider e.g., a variety in $\mathbf{k}^2$ which is the union of points on the $y$-axis with equations $x = 0$, $u(y) = 0$ and of two curves of equations $f(x, y) = 0$ (with $f$ monic in $y$) and $g(x, y) = 1 + xy = 0$. This corresponds to the following quotient ring (where $F = fg$)

$$\mathbf{C} = \mathbf{k}[x, y] = \mathbf{k}[X, Y]/\langle XF(X, Y), u(Y)F(X, Y)\rangle \ .$$

We want to examine this variety above the $x$-axis in the neibourhood of $\{0\}$. So we consider the local ring $\mathbf{A} = \mathbf{k}[x]_{1+x\mathbf{k}[x]}$ (with maximal ideal $\mathfrak{M} = x\mathbf{A}$ and residue field $\mathbf{k}$) and the $\mathbf{A}$-algebra $\mathbf{B} = \mathbf{C}_{1+xk[x]}$.
Residually we get taking $x = 0$ the ring $\mathbf{B}/\mathfrak{M}\mathbf{B} = \mathbf{k}[Y]/\langle u(Y)f(0, Y)\rangle$. It is a finite $\mathbf{k}$-vector space. But $y$ viewed in $\mathbf{B}$ is not integral over $\mathbf{A}$. We have to remove the component $g(x, y) = 0$ in order that $y$ becomes integral over $\mathbf{A}$. What we get is we find an element $s \in 1 + \mathfrak{M}\mathbf{B}$ (namely $s = g$) which changes nothing residually (you invert 1!) but we have $\mathbf{B}[1/s]$ is finite over $\mathbf{A}$.

**Isolated zeroes, local case**

**Theorem 3.** (as in Raynaud)
*Let $\mathbf{A}$ be a ring, $\mathfrak{M}$ a maximal ideal of $\mathbf{A}$ and $\mathbf{k} = \mathbf{A}/\mathfrak{M}$. Let $\mathbf{B}$ a finitely generated $\mathbf{A}$-algebra and $\mathfrak{P}$ a prime ideal of $\mathbf{B}$ lying over $\mathfrak{M}$. Let $\mathbf{A}_1$ be the integral closure of $\mathbf{A}$ in $\mathbf{B}$. Let $\mathbf{C} = \mathbf{B}_{\mathfrak{P}}$. If $\mathbf{C}/\mathfrak{M}\mathbf{C}$ is a finite $\mathbf{k}$-algebra then there exists $s \in \mathbf{A}_1 \setminus \mathfrak{P}$ such that $\mathbf{A}_1[1/s] = \mathbf{B}[1/s]$.*

A constructive form of this theorem is the following.

**Theorem 4.**
*Let $\mathbf{A}$ be a ring, $\mathfrak{M}$ a detachable maximal ideal of $\mathbf{A}$ and $\mathbf{k} = \mathbf{A}/\mathfrak{M}$. Let $\mathbf{B} = \mathbf{A}[x_1, \ldots, x_n]$ such that $\mathbf{B}/\mathfrak{M}\mathbf{B}$ is a finite $\mathbf{k}$-algebra. Then there exists $s \in 1 + \mathfrak{M}\mathbf{B}$ such that $s, sx_1, \ldots, sx_n$ are integral over $\mathbf{A}$.*
*So $\mathbf{A}' = \mathbf{A}[s, sx_1, \ldots, sx_n]$ is finite over $\mathbf{A}$, $\mathbf{B}[1/s] = \mathbf{A}'[1/s]$ and residually $\mathbf{A}'/\mathfrak{M}\mathbf{A}' = \mathbf{B}/\mathfrak{M}\mathbf{B}$.*





An abstract proof of Theorem 3 was given by Peskine. The proof uses in an essential way localizations at minimal primes. Deciphering constructively the proof is a rather hard task. This gives a slightly more general theorem.

**Theorem 5.**
*Let $\mathbf{A}$ be a ring, $\mathfrak{I}$ an ideal of $\mathbf{A}$ and $\mathbf{k} = \mathbf{A}/\mathfrak{I}$. Let $\mathbf{B} = \mathbf{A}[x_1, \ldots, x_n]$ such that $\mathbf{B}/\mathfrak{I}\mathbf{B}$ is a finite $\mathbf{k}$-algebra. Then there exists $s \in 1 + \mathfrak{I}B$ such that $s, sx_1, \ldots, sx_n$ are integral over $\mathbf{A}$.*
*So $\mathbf{A}' = \mathbf{A}[s, sx_1, \ldots, sx_n]$ is finite over $\mathbf{A}$, $\mathbf{B}[1/s] = \mathbf{A}'[1/s]$ and residually $\mathbf{A}'/\mathfrak{I}\mathbf{A}' = \mathbf{B}/\mathfrak{I}\mathbf{B}$.*



## *3. Isolated zeroes, general case*

**Quasi-finite algebras**

In classical mathematics an $\mathbf{A}$-algebra $\mathbf{B}$ is said to be **quasi-finite** if it is of finite type and if prime ideals of $\mathbf{B}$ lying over any prime ideal of $\mathbf{A}$ are incomparable. If $\mathfrak{P}$ is a prime ideal of $\mathbf{B}$ lying over the prime ideal $\mathfrak{p}$ of $\mathbf{A}$ this means that the extension $\mathrm{Frac}(\mathbf{B}/\mathfrak{P})$ of $\mathrm{Frac}(\mathbf{A}/\mathfrak{p})$ is finite.
Another way to express this fact is to say that the morphism $\mathbf{A} \to \mathbf{B}$ is **zero-dimensional**. A constructive characterization of zero-dimensional morphisms uses the zero-dimensional reduced ring $\mathbf{A}^\bullet$ generated by $\mathbf{A}$. The ring $\mathbf{A}^\bullet$ can be obtained as a direct limit of rings

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

with $\mathfrak{a} = \langle (a_iT_i^2 - T_i)_{i=1}^n, (T_ia_i^2 - a_i)_{i=1}^n \rangle$

### Isolated zeroes, general case

In classical mathematics we obtain the following equivalence.

***Proposition* 6.** *Let $\varphi : \mathbf{A} \to \mathbf{B}$ a morphism of commutative rings.*

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

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



### Isolated zeroes, general case

As a consequence we have the following characterization of quasi-finite morphisms.

***Proposition* 7.** *Let $\mathbf{B}$ be an $\mathbf{A}$-algebra of finite type. The following are equivalent.*

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

This gives a good definition of quasi-finite morphisms in constructive mathematics. Let us insist here on the fact that the equivalence in Proposition 7 has a constructive proof.



### Isolated zeroes, general case

### Open immersions

The global version of ZMT given in classical mathematics uses also the notion of an "open immersion" from $\mathsf{Spec}\,\mathbf{B}$ to $\mathsf{Spec}\,\mathbf{A}$.
A constructive approach for an open immersion is the following.

***Definition* 8.** *A morphism $\varphi : \mathbf{A} \to \mathbf{B}$ is an* **open immersion** *if there exist $s_1, \dots, s_n$ in $\mathbf{A}$ comaximal in $\mathbf{B}$ such that for each $i$ the natural morphism $\mathbf{A}[1/s_i] \to \mathbf{B}[1/\varphi(s_i)]$ is an isomorphism.*

Open immersions and finite morphisms are particular case of quasi-finite morphisms.

**Theorem 9.** (global ZMT, classical formulation)
*Let $\mathbf{B}$ be quasi-finite over $\mathbf{A}$. Let $\mathbf{C}$ be the integral closure of $\mathbf{A}$ in $\mathbf{B}$. Then the morphism $\mathbf{C} \to \mathbf{B}$ is an open immersion. Moreover there exists a finite subalgebra $\mathbf{C}'$ of $\mathbf{C}$ such that the morphism $\mathbf{C}' \to \mathbf{B}$ is an open immersion.*

**Isolated zeroes, general case**

A more precise formulation is the following.

**Theorem 10.** (global ZMT, constructive formulation)
*Let $\mathbf{A} \subseteq \mathbf{B} = \mathbf{A}[x_1, \ldots, x_n]$ be rings such that the inclusion morphism $\mathbf{A} \to \mathbf{B}$ is zero dimensional (in other words, $\mathbf{B}$ is quasi-finite over $\mathbf{A}$). Let $\mathbf{C}$ be the integral closure of $\mathbf{A}$ in $\mathbf{B}$. Then there exist elements $s_1, \ldots, s_m$ in $\mathbf{C}$, comaximal in $\mathbf{B}$, such that all $s_i x_j \in \mathbf{C}$. In particular for each $i$, $\mathbf{C}[1/s_i] = \mathbf{B}[1/s_i]$. Moreover letting $\mathbf{C}' = \mathbf{A}[(s_i), (s_i x_j)]$, which is finite over $\mathbf{A}$, we get also $\mathbf{C}'[1/s_i] = \mathbf{B}[1/s_i]$ for each $i$.*

The concrete hypothesis is item 2 in proposition 7. The proof is by induction on $p$.
We assume we have the conclusion for $p-1$ and let $a = a_p$. The induction hypothesis is applied to the morphisms $\mathbf{A}/a\mathbf{A} \to \mathbf{B}/a\mathbf{B}$ and $\mathbf{A}[1/a] \to \mathbf{B}[1/a]$, and so on ...



## *4. Simple zeroes, unramified and étale algebras*

We use the terminology of Grothendieck in EGA4. Let us recall that an ideal is called a nilideal if some power of it is zero.

***Definition* 11.** *Let $\mathbf{A}$ be an arbitrary commutative ring and $\mathbf{C}$ an $\mathbf{A}$-algebra.*

1. *The $\mathbf{A}$-algebra $\mathbf{C}$ is said to be* **formally unramified** *(resp.* **formally smooth***) if for each algebra $\mathbf{B}$ and each nilideal $\mathfrak{I}$ of $\mathbf{B}$ the canonical map $\mathrm{Hom}_{\mathbf{A}}(\mathbf{C}, \mathbf{B}) \to \mathrm{Hom}_{\mathbf{A}}(\mathbf{C}, \mathbf{B}/\mathfrak{I})$, $\varphi \mapsto \pi \circ \varphi$, is injective (resp. surjective).*
2. *A morphism which is formally smooth and formally unramified is called* **formally étale**.
3. *An $\mathbf{A}$-algebra is said to be* **étale** *(resp.* **smooth**, *resp.* **unramified***) if it is formally étale (resp. formally smooth, resp. formally unramified) and moreover is a finitely presented $\mathbf{A}$-algebra.*



**Simple zeroes, unramified morphisms**

The following classical result is constructive.

***Proposition* 12.** *An $\mathbf{A}$-algebra $\mathbf{C}$ is formally unramified iff the module of differentials of $\mathbf{C}$ over $\mathbf{A}$, usually denoted as $\Omega_{\mathbf{C}|\mathbf{A}}$ is null.*

We shall use the following notation for finitely presented algebras:

$$\mathbf{A}_{[f_1,\ldots,f_p]} = A[X_1, \ldots, X_n] / \langle f_1, \ldots, f_p \rangle .$$

So an $\mathbf{A}$-algebra $\mathbf{C}$ is unramified iff $\mathbf{C} \simeq \mathbf{A}_{[f_1,\ldots,f_p]}$ with the transpose of the Jacobian matrix $\mathrm{Jac}_{f_1,\ldots,f_p}[\underline{x}]$ surjective:

$$\mathrm{Jac}_{f_1,\ldots,f_p}(\underline{X}) = (\partial f_j / \partial X_i)_{1 \le i \le n, 1 \le j \le p}$$

This means that **the $n$-minors of the Jacobian matrix generate the ideal $\langle 1 \rangle$ of C.**

**Simple zeroes, field case**

A basic theorem of algebraic geometry describes unramified algebras over discrete fields.

**Theorem 13.** *Let* $\mathbf{k}$ *be a discrete field and* $\mathbf{A}$ *an unramified* $\mathbf{k}$*-algebra.*

1. $\mathbf{A}$ *is a finite dimensional* $\mathbf{k}$*-vector space.*
2. $\mathbf{A}$ *is a zero-dimensional reduced ring and can be described as a finite product of monogenic separable algebras, i.e., algebras isomorphic to* $\mathbf{k}_{[h_j]}$ *with* $h_j$ *a separable polynomial.*
3. *Moreover:*

   – *If* $\mathbf{k}$ *is a separably factorial field (see [MRR] for this constructive notion), one can take the* $h_j$*'s irreducible (so the algebra is a finite product of discrete fields* $\mathbf{k}_{[h_j]}$*).*

   – *If* $\mathbf{k}$ *is infinite, the algebra is isomorphic to* $\mathbf{k}_{[h]}$ *for some separable polynomial* $h$*.*



## 5. Simple zeroes, local case

***Proposition* 14.** *An unramified algebra is quasi-finite.*

*Proof.* Let $\mathbf{B} = \mathbf{A}_{[f_1,\ldots,f_s]} = \mathbf{A}[x_1, \ldots, x_n]$ be an unramified $\mathbf{A}$-algebra. We have to show that the ring $\mathbf{A}^{\bullet} \otimes_{\mathbf{A}} \mathbf{B}$ is zero-dimensional. So we have to prove that when $\mathbf{A}_1$ is a zero-dimensional reduced ring any unramified $\mathbf{A}_1$-algebra is finite. The result is classical when $\mathbf{A}_1$ is a discrete field (see Theorem 13). So we can apply the constructive elementary local-global machinery of zero-dimensional reduced rings. □

As a consequence of Zariski Main Theorem (global version, Theorem 10) we obtain structure theorems for unramified algebras.



**Simple zeroes, local case**

**Theorem 15.** (unramified morphisms, local structure theorem)
*Let* $(\mathbf{A}, \mathfrak{M})$ *be a residually discrete local ring. Let* $\mathbf{B}$ *be an unramified* $\mathbf{A}$*-algebra with* $\mathfrak{M}\mathbf{B} \cap \mathbf{A} = \mathfrak{M}$ *and* $C$ *be the integral closure of* $\mathbf{A}$ *in* $\mathbf{B}$*. There exist* $u_1, \ldots, u_r \in C$ *comaximal in* $\mathbf{B}/\mathfrak{M}\mathbf{B}$ *such that for each* $j$ *the algebra* $\mathbf{B}\left[\frac{1}{u_j}\right]$ *is isomorphic to a quotient of a standard étale algebra* $\mathbf{A}_{[h_j]}\left[\frac{1}{g_j}\right]$ *where the surjective morphism* $\mathbf{A}_{[h_j]}\left[\frac{1}{g_j}\right] \to \mathbf{B}\left[\frac{1}{u_j}\right]$ *gives modulo* $\mathfrak{M}$ *an isomorphism.*



**Simple zeroes, local case**

***Corollary* 16.** (usual classical version of Theorem 15: cf. Raynaud, Chapter V, Th. 5, p. 51)
*Let* $(\mathbf{A}, \mathfrak{M})$ *be a residually discrete local ring,* $\mathbf{B}$ *an* $\mathbf{A}$*-algebra,* $\mathfrak{p}$ *a prime ideal of* $\mathbf{B}$ *lying over* $\mathfrak{M}$*. Assume that* $\mathbf{B}$ *is "unramified in the neibourhood of* $\mathfrak{p}$*", i.e. there exists* $p \notin \mathfrak{p}$ *such that* $\mathbf{B}\left[\frac{1}{p}\right]$ *is unramified over* $\mathbf{A}$*. Then there exists* $u \notin \mathfrak{p}$ *such that* $\mathbf{B}\left[\frac{1}{u}\right]$ *is isomorphic to a quotient of a standard étale algebra* $\mathbf{A}_{[h]}\left[\frac{1}{g}\right]$ *where the surjective morphism* $\mathbf{A}_{[h]}\left[\frac{1}{g}\right] \to \mathbf{B}\left[\frac{1}{u}\right]$ *gives residually an isomorphism.*

*Remark.* In order to have a constructive proof of this corollary, the prime ideal $\mathfrak{p}$ is assumed to be given through its complement $S$, which has to be a "prime filter": $st \in S$ iff $s$ and $t$ are in $S$, and if $s + t \in S$ then $s$ or $t$ is in $S$, with an explicit "or". Thus the localization $\mathbf{A}_S$ is a local ring in the constructive meaning.

page 23

# 6. *Simple zeroes, Multidimensional Hensel Lemma*

$\mathbf{A}$ is a local ring with detachable maximal ideal $\mathfrak{M}$ and $\mathbf{k} = \mathbf{A}/\mathfrak{M}$ is the residual field. We shall look at a polynomial system

$$f_1(X_1, \ldots, X_n) = \cdots = f_n(X_1, \ldots, X_n) = 0 \tag{$*$}$$

which has a simple zero at $(0, \ldots, 0)$ residually: $f_i(0, \ldots, 0) \in \mathfrak{M}$ and also the Jacobian of this system $J(0, \ldots, 0)$ is in $\mathbf{A}^\times$. In this case we will say that we have a Hensel system. To this polynomial system we associate

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

The ideal $\mathfrak{M}_\mathbf{B}$ is maximal because it is the kernel of the morphism $\mathbf{B} \to \mathbf{k}$ sending $g(\underline{x})$ to $\overline{g}(\underline{0})$. This shows also that $\mathbf{B}/\mathfrak{M}_\mathbf{B} = \mathbf{A}/\mathfrak{M}$.

page 24

### Multidimensional Hensel Lemma

This implies that the natural morphism $\mathbf{A} \to \mathbf{B}$ is injective, so we can identify $\mathbf{A}$ with its image in $\mathbf{B}$ and we have $\mathbf{B} = \mathbf{A} \oplus \langle x_1, \ldots, x_n\rangle\,\mathbf{B}$. Nevertheless it is not at all evident that the morphism from $\mathbf{A}$ to $\mathbf{B}_{1+\mathfrak{M}\mathbf{B}}$ is injective.
It can be easily seen that the natural morphism $\varphi : \mathbf{A} \to \mathbf{B}_{1+\mathfrak{M}_\mathbf{B}}$ shares the following universal property: it is a local morphism (i.e., $\varphi(x) \in (\mathbf{B}_{1+\mathfrak{M}_\mathbf{B}})^\times$ implies $x \in \mathbf{A}^\times$) and if $\psi : \mathbf{A} \to \mathbf{C}$ is a local morphism such that $(y_1, \ldots, y_n)$ is a solution of $(*)$ with the $y_i$'s in the maximal ideal of the local ring $\mathbf{C}$ then there exists a unique local morphism $\theta : \mathbf{B} \to \mathbf{C}$ such that $\theta \circ \varphi = \psi$.
Since $\mathbf{B}_{1+\mathfrak{M}_\mathbf{B}}$ satisfies this universal property w.r.t. the system $(*)$ we introduce the notation

$$\mathbf{B}_{1+\mathfrak{M}_\mathbf{B}} = \mathbf{A}_{[\![f_1,\ldots,f_n]\!]}.$$

page 25

### Multidimensional Hensel Lemma

The Multidimensionnal Hensel Lemma (MHL fort short) is a kind of “primitive element theorem”.

**Theorem 17.** (Multidimensional Hensel Lemma)
*With the preceeding hypotheses and notations, the local ring* $\mathbf{A}_{[\![f_1,\ldots,f_n]\!]} = \mathbf{B}_{1+\mathfrak{M}_\mathbf{B}}$ *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* $y \in \mathfrak{M}_\mathbf{B}$ *and a monic polynomial* $f(X) \in \mathbf{A}[X]$ *with* $f(y) = 0$ *and* $f'(0) \in 1 + \mathfrak{M}$ *(thus* $f'(y) \in 1 + \mathfrak{M}_\mathbf{B}$*),*
*such that each* $x_i$ *belongs to* $\mathbf{A}[y, \frac{1}{1+y}]$ *(in other words* $\mathbf{B} \subseteq \mathbf{A}[y, \frac{1}{1+y}]$*), and the natural morphism* $\mathbf{A}_{[\![f]\!]} \to \mathbf{B}_{1+\mathfrak{M}_\mathbf{B}}$ *sending* $x$ *to* $y$ *is an isomorphism (*$x$ *is* $X$ *viewed in* $\mathbf{A}_{[\![f]\!]}$*).*
*In short* $\mathbf{A}_{[\![f_1,\ldots,f_n]\!]} = \mathbf{A}_{[\![f]\!]}$.

page 26

Here is an example where $\mathbf{A}$ 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 $\mathbf{B} = \mathbf{A}[x,y]$ 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 $s \in \mathbf{B}$ integral over $\mathbf{A}$ such that $sx, sy$ integral over $B$ and $s = 1$ mod. $\mathfrak{M}\mathbf{B}$.
Following the proof we take $t = 1 + ax + by$. We have that $t = 1$ mod. $\mathfrak{M}\mathbf{B}$ and $t, ty$ integral over $\mathbf{A}[x]$. We have even $ty = y + axy + by^2 = b - ax^2$ in $\mathbf{A}[x]$. The equation for $t$ is

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

We have then

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

and so

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

If we take $u = t - (a - 2b)x = 1 + 2bx + by$ we have $u = 1$ mod. $\mathfrak{M}\mathbf{B}$ and $ux$ in $\mathbf{A}$ and $u$ is integral over $\mathbf{A}$. Indeed $u$ is integral over $\mathbf{A}[1/u]$ since $x$ is in $\mathbf{A}[1/u]$ and $u$ is integral over $\mathbf{A}[x]$.
If we take $s = tu^2$ we have $s, sx, sy$ integral over $\mathbf{A}$.
Indeed, $ux$ is in $\mathbf{A}$ and since $t^2 - (1+ax)t - b + ax^2 = 0$ we have $tu$ and hence $s$ integral over $\mathbf{A}$. Since $ty = b - ax^2$ we have $sy = vu^2 - a(ux)^2$ integral over $\mathbf{A}$. Finally $sx = (tu)(ux)$ is integral over $\mathbf{A}$.
It can be checked that $s$ is a root of a monic polynomial $f$ of degree 4 of the form $T^3(T-1)$ residually.



*Thank you*

*Thanks to the organizers*