Application of ZMT

March 4, 2006

1 Henselian extensions

In all this paper A will be a local ring, with a detachable maximal ideal $\mathfrak{M}$. We let k be the residue field $A/\mathfrak{M}$. If we have such a local ring $A, \mathfrak{M}$ it is convenient to think of the elements of $\mathfrak{M}$ as "infinitesimal", whereas the elements of $A^\times$ are the ones that are observationally different from 0. (The introduction of [8] is helpful there.)

We shall look at a polynomial system

$$f_1(x_1, \ldots, x_n) = \ldots = f_n(x_1, \ldots, x_n) = 0 \tag{$*$}$$

which has a simple zero at $(0, \ldots, 0)$ residually: we have not only $f_i(0, \ldots, 0) = 0$ residually but also the Jacobian of this system $J(0, \ldots, 0)$ is in $A^\times$.

We are going to associate, in an explicit way, to such a system a unitary polynomial f of degree m which is of the form $X^{m-1}(X-1)$ residually. To this polynomial we can associate the extension A_f of A obtained by forcing $f(z) = 0$ and inverting all elements $g(z)$ such that $g(1) \in A^\times$. Intuitively we have added a root of f which is infinitely close to 1. The extension A_f is called a *simple Hensel extension* of A. One can show that A_f is a local ring and we have a local embedding of A into A_f, the maximal ideal $\mathfrak{M}_f$ being the set of elements $h(z)/g(z)$ such that $h(1) \in \mathfrak{M}$ [1]. (This is actually rather direct since f is unitary.) For instance we have $z - 1 \in \mathfrak{M}_f$ and this expresses that z is infinitely close to 1.

The polynomial f will be such that in A_f there is a solution $(x_1, \ldots, x_n)$ of the system $(*)$ where all $x_1, \ldots, x_n$ are in $\mathfrak{M}_f$. Thus we have found a local extension of A in which the system $(*)$ has a solution "infinitely close" to 0.

A unitary polynomial which is of degre m and of the form $X^{m-1}(X-1)$ residually is called a *special polynomial*. Notice that if f is a special polynomial we always have $f(1) = 0$ and $f'(1) = 1$ residually. Notice also that z is a unit of A_f. We call such an element a *special unit*.

We can summarise this discussion by the following result.

Theorem 1.1 *There exists a special polynomial f such that the system $(*)$ has an infinitesimal solution in A_f.*

In particular this means that it is consistent to add a root of the system $(*)$ and if we do that, we do it in a conservative way over A. Furthermore, it shows that the system $(*)$ has a solution in the Henselization of A, which is obtained from A by adding successively roots of special polynomials [1].

To build such a solution, the first step is to extend the system $(*)$ so that we get a new system which has the property that it implies that all x_i are in $\mathfrak{M}A[x_1, \ldots, x_n]$.

Lemma 1.2 *Assume $f_1, \ldots, f_n \in k[X_1, \ldots, X_n]$ are such that $f_1(0, \ldots, 0) = \ldots = f_n(0, \ldots, 0) = 0$ and have a Jacobian $J(0, \ldots, 0)$ in $k^\times$ and let $k[x_1, \ldots, x_n]$ be $k[X_1, \ldots, X_n]/{<}f_1, \ldots, f_n{>}$. Then there exists an idempotent element $e \in 1 + \Sigma x_i k[x_1, \ldots, x_n]$ such that $ex_1 = \ldots = ex_n = 0$.*

Proof. After a linear change of coordinates we can assume that we have $f_i = X_i - g_i$ where all monomials in g_i are of degree > 1. This means that, if x is the column vector $(x_1, \dots, x_n)$, we can write $x = Mx$ where M is a $n \times n$ matrix in coefficient in $\Sigma x_i k[x_1, \dots, x_n]$. If e is the determinant of $I_n - M$ we have $ex_1 = \dots = ex_n = 0$, and $e \in 1 + \Sigma x_i k[x_1, \dots, x_n]$. This implies $e^2 = e$. $\square$

Corollary 1.3 *With the notations of Lemma 1.2, $X_1, \dots, X_n, 1 - X \in <f_1, \dots, f_m, Xe - 1>$ in $k[X_1, \dots, X_n, X]$.*

Proof. Indeed this ideal contains $e^2 - e$ and $Xe - 1$ so it contains $e - 1$ and $X - 1$. Since it contains $eX_1, \dots, eX_n$ it contains also $X_1, \dots, X_n$. $\square$

If we lift this to A and $A[X_1, \dots, X_n]$ this means that, maybe after adding one indeterminate and one equation, one can assume that we have $\nu_1, \dots, \nu_n$ in $\mathfrak{M}A[X_1, \dots, X_n]$ such that $X_1 - \nu_1, \dots, X_n - \nu_n$ are in $<f_1, \dots, f_n>$.

We shall follow Peskine's proof of Zariski Main Theorem [7] for proving constructively the following formulation of this theorem.

Theorem 1.4 *We assume that $B = A[x_1, \dots, x_n]$ is an A-algebra such that $x_1, \dots, x_n \in \mathfrak{M}B$. There exists $s \in 1 + \mathfrak{M}B$ such that $s, sx_1, \dots, sx_n$ are integral over A.*

The statement is proved only for two elements x, y, but it holds, with the same argument as the one we give, for n elements as well. The argument we give for Theorem 1.4 follows closely Peskine's proof. One main point is the elimination of the use of a generic minimal prime.

Before giving the proof of Theorem 1.4, we explain how it can be used for Theorem 1.1. We apply it to the algebra $B = A[x_1, \dots, x_n]$ where $x_1, \dots, x_n$ are forced to be a solution of the system $(*)$, assuming that this system implies $x_1, \dots, x_n \in \mathfrak{M}B$. Notice that, a priori, it may be that $1 \in \mathfrak{M}B$ or that $1 = 0$ in B. It will be a consequence of Theorem 1.1 that this is not the case, and furthermore B is conservative over A: if $a \in A$ then $a = 0$ in B if and only if $a = 0$ in A.

By Theorem 1.4 we find $s = s(x_1, \dots, x_n)$ in $1 + \mathfrak{M}B$ and $s, sx_1, \dots, sx_n$ are integral over A. We let $D = A[s, sx_1, \dots, sx_n]$.

Lemma 1.5 *For each $u \in B$ there exists p such that $s^p u$ is in D.*

Proof. Indeed u can be written as a polynomial in $x_1, \dots, x_n$ and so $s^m u$ can be written as a polynomial in $s, sx_1, \dots, sx_n$ for m big enough. $\square$

Since $s, sx_1, \dots, sx_n$ are integral over A, D is a finite A-module. So it is a finite $A[s]$-module as well, and the generators are $m_0 = 1, m_1, \dots, m_l$ where each $m_1, \dots, m_l$ is a product of powers of sx_i. So each generator $m_1, \dots, m_l$ is in $\mathfrak{M}B$.

Lemma 1.6 *There exists p such that all $s^p m_1, \dots, s^p m_l$ are in $\mathfrak{M}D$.*

Proof. Indeed each m_i is in $\mathfrak{M}B$ and we can apply Lemma 1.5. $\square$

Corollary 1.7 *There exists a unitary polynomial $d(X) = X^{lp} + \dots$ which is X^{lp} residually such that $d(s)D \subseteq A[s]$.*

Proof. Indeed we write $s^p m_i = \Sigma \mu_{ij} m_j$ for $i = 1, \dots, l$ and $m_0 = 1$ where each μ_{ij} is in $\mathfrak{M}$. By taking the determinant $d(s)$ of this system we obtain the result. $\square$

This shows that each $x_1, \dots, x_n$ can be expressed as a rational function of s, and we write $h_i(s) = d(s)sx_i = q(s)x_i$ with $q(X) = Xd(X)$. We let N be a bound of the degree of $f_1, \dots, f_n$ and we let $F_i(z)$ be $q(z)^N f_i(h_1(z)/q(z), \dots, h_n(z)/q(z))$.

Corollary 1.8 *s is a root of the system $F_1(s) = \dots = F_n(s) = 0$.*

Notice that $s - 1 \in \mathfrak{M}B$. By using Lemma 1.5 we have N such that $s^N(s-1) \in \mathfrak{M}D$. By using Corollary 1.7, we get $d(s)s^N(s-1) \in \mathfrak{M}A[s]$. Thus we see that s is the root of a polynomial which is of the form $X^{p-1}(X-1)$ residually. We can get a little better and obtain that s is the root of a *special polynomial*.

Lemma 1.9 *Let p be minimal such that s is a root of a polynomial F of the form $X^{p-1}(X-1)$ residually. Then s is the root of a special polynomial of degree p.*

Proof. We have that $1, \dots, s^{p-1}$ generates $A[s]$ as a A-module by using Nakayama's lemma. Thus s is the root of a unitary polynomial of degree p. This polynomial G has to be $X^{p-1}(X-1)$ residually, otherwise s would be the root of the gcd of this polynomial F and G (we do the computation residually). Since this polynomial divides $X^{p-1}(X-1)$ residually it has to be of the form $X^{q-1}(X-1)$ residually with $q < p$. $\square$

We don't need to be able to compute the minimal value for p, and we cannot compute it in general. We follow the proof of Lemma 1.9 and proceed dynamically. We find in this way a special polynomial f of which s is a root, and we can do as if this polynomial is of minimal degree.

The claim is now that for this polynomial f the system $(*)$ has a root in A_f. For this, since we have $F_i(z) = q(z)^N f_i(h_1(z)/q(z), \dots, h_n(z)/q(z))$ and $q(1) = 1$ residually the only condition that we have to check is $F_1(z) = \dots = F_n(z) = 0$. By the minimality condition on f we can assume that $F_1(X), \dots, F_n(X)$ are multiple of $f(X)$ residually. (This is an example where we can reason dynamically: if after dividing $F_1, \dots, F_n$ by f we find some remaining polynomial which is not 0 residually we can replace f by a smaller special polynomial. After a finite number of such operations we are in the situation where $F_1(X), \dots, F_n(X)$ are all multiple of $f(X)$ residually.)

Thus we have that all $F_1(z), \dots, F_n(z)$ are infinitely small in A_f. We let I be the ideal $<F_1(z), \dots, F_n(z)>$ in A_f.

Lemma 1.10 *(Newton's lemma) If C is an A-algebra, I an ideal of C, and there is a solution $(u_1, \dots, u_n)$ of $(*)$ mod. I then there exists $i_1, \dots, i_n \in I$ such that $(u_1 + i_1, \dots, u_n + i_n)$ is a solution of $(*)$ mod. I^2.*

Lemma 1.11 *In the ring A_f we have $I = I^2$.*

Proof. Notice that $h_1(z)/q(z), \dots, h_n(z)/q(z)$ a solution of the system $(*)$ mod I. By Lemma 1.10 there exits a solution $y_1, \dots, y_n$ mod I^2 of the system $(*)$. It follows that $t = s(y_1, \dots, y_n) \in 1 + \mathfrak{M}A[y_1, \dots, y_n]$ is a root of the special polynomial f mod I^2, and that we have $q(t)y_i = h_i(t)$. (Indeed, all this follows uniquely formally as soon as we have somewhere a solution of the system $(*)$.) Also t is in A_f infinitely close to 1. Since t is infinitely close to 1 and $f(t) = 0$ mod I^2 it follows that we have $z = t$ mod I^2: we can write $f(t) = (t-z)f'(z) + (t-z)^2 u$ and since $t - z \in \mathfrak{M}_f$ and $f'(z)$ is invertible, $f(t) \in I^2$ implies $t - z \in I^2$. Thus $q(z)y_i = h_i(z)$ mod I^2 and we have $F_1(z), \dots, F_n(z) = 0$ mod I^2, as desired. $\square$

Corollary 1.12 *We have $I = 0$ and so $h_1(z)/q(z), \ldots, h_n(z)/q(z)$ is a solution of the system $(*)$ in A_f.*

Proof. Since $F_1(z), \ldots, F_n(z)$ are infinitely small in A_f, the inclusion $I \subseteq I^2$ implies (like in Nakayma's lemma) that $I = 0$. $\square$

2 Zariski Main Theorem

In the following we shall reserve the names $A, B, \mathfrak{M}$ as described in the statement of Theorem 1.4. The monoid $M = 1 + \mathfrak{M}B$ will play a crucial role.

Lemma 2.1 *If $R \subseteq S$ and $t \in S$ satisfies an equation $a_n t^n + \ldots + a_0 = 0$ with $a_0, \ldots, a_n \in R$ then $a_n t$ is integral over R.*

Proof. We have, by multiplying the equation by a_n^{n-1}

$$(a_n t)^n + a_{n-1}(a_n t)^{n-1} + \ldots + a_n^{n-1} a_0 = 0$$

which shows that $a_n t$ is integral over R. $\square$

This is only a special case of a more important result, which comes from [3].

Lemma 2.2 *If $R \subseteq S$ and $t \in S$ satisfies an equation $a_n t^n + \ldots + a_0 = 0$ with $a_0, \ldots, a_n \in R$ and we take $u_n = a_n, u_{n-1} = u_n t + a_{n-1}, \ldots, u_0 = u_1 t + a_0 = 0$ then $u_n, \ldots, u_0$ and $u_n t, \ldots, u_0 t$ are integral over R and $<u_0, \ldots, u_n> = <a_0, \ldots, a_n>$ as ideals of S.*

Proof. By Lemma 2.21 we have first $u_n t = a_n t$ integral over R. It follows that $u_{n-1} = t u_n + a_{n-1}$ is integral over R. We have then

$$u_{n-1} t^{n-1} + a_{n-2} t^{n-2} + \ldots + a_0 = 0$$

so that, by Lemma 2.21 again, $u_{n-1} t$ is integral over $R[u_n]$ and so over R. In this way, we get that $u_n, u_n t, u_{n-1}, u_{n-1} t, \ldots, u_0 = 0$ are all integral over R. $\square$

We deduce from this the following way of building integral elements that are in the monoid M.

Corollary 2.3 *If $A \subseteq C \subseteq B$ and $t \in B$ satisfies an equation $a_n t^n + \ldots + a_0 = 0$ with $a_0, \ldots, a_n \in C$ and at least one of them in M then there exists u in M such that u, ut are integral over C.*

Proof. By Lemma 2.2 we first find $u_n, \ldots, u_0 \in B$ such that $u_n, u_n t, \ldots, u_0, u_0 t$ are integral over C and by Lemma 2.2 at least one u_i is in M. $\square$

Corollary 2.3 can be formulated as follow: if t is the root of a polynomial in $C[T]$ which is not 0 mod $\mathfrak{M}B$ then there exists u in M such that u, ut are integral over C.

Lemma 2.4 *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.*

Proof. 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. $\square$

Lemma 2.6 is a variation on this lemma. With Corollary 2.3 this gives the second way of building integral elements.

Lemma 2.5 *If t is integral over $R[x]$ then there exists l such that for all $a \in R$ we have that $a^l t$ is integral over $R[ax]$.*

Proof. We have an equation for t of the form $t^n + p_1(x)t^{n-1} + \ldots + p_n(x) = 0$. Let l be the greatest exponent of x in this expression. By multiplying by a^l we get an equality of the form

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

and hence, by Lemma 2.1, $a^l t$ is integral over $R[ax]$. $\square$

Lemma 2.6 *If t is integral over $R[x]$ and $p(x) = a_k x^k + \ldots + a_0$ 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. By Lemma 2.5 we have l such that $a^l t$ is integral over $R[ax]$ for all a. 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 $m \geq l$ and P monic. We can then apply Lemma 2.4. $\square$

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

We assume now t integral over $R[x]$ of degree n and R integrally closed in $S = R[x,t]$. We define $J = (R[x] : S)$.

Lemma 2.8 *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 $q_{n-1}(x)t^{n-1} + \ldots + q_0(x)$. $\square$

Lemma 2.9 *If $u \in S$ and $a_0, \ldots, a_k \in R$ and $u(a_0 + \ldots + a_k x^k) \in J$ then there exists m such that $ua_k^m \in J$.*

Proof. We have by Lemma 2.8

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

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 $\sqrt{J}$ of J *in* S.

Corollary 2.10 *If $u \in S$ and $a_0, \ldots, a_k \in R$ and $u(a_0 + \ldots + a_k x^k) \in \sqrt{J}$ then $ua_0, \ldots, ua_k \in \sqrt{J}$.*

Proof. We have l such that $u^l(a_0 + \ldots + a_k x^k)^l \in J$. By Lemma 2.9 we have m such that $u^l(a_k^l)^m \in J$ and hence $ua_k \in \sqrt{J}$. It follows that $ua_k x^k \in \sqrt{J}$ and so $u(a_0 + \ldots + a_{k-1}x^{k-1}) \in \sqrt{J}$ and we get successively $ua_{k-1}, \ldots, ua_0 \in \sqrt{J}$. $\square$

Corollary 2.11 *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 $D = S/\sqrt{J}$ and $C = R/R \cap \sqrt{J}$ then $D = C[x,t]$ is a reduced ring with a subring C such that t is integral over $C[x]$ and x is transcendent over C in the strong sense that we have for all $u \in D$ and $a_0, \ldots, a_k \in C$, if $u(a_0 + \ldots + a_k x^k) = 0$ then $ua_0 = \ldots = ua_k = 0$.*

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

Lemma 2.12 *If S is integral over R then the integral closure of I in S is $\sqrt{IS}$.*

Proof. See [2] Lemma 5.14. □

Lemma 2.13 *If $X^k + a_1X^{k-1} + \ldots + a_k$ divides $X^n + b_1X^{n-1} + \ldots + b_n$ then $a_1, \ldots, a_k$ are integral over $b_1, \ldots, b_n$*

Proof. We can assume $X^k + a_1X^{k-1} + \ldots + a_k = (X - t_1)\ldots(X - t_k)$. 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 $t_1, \ldots, t_k$. □

From now on, we assume that D is a reduced C-algebra and that $x \in D$ is *strongly* transcendent over C in the sense that we have for all $u \in D$ and $a_0, \ldots, a_n \in C$, if $u(a_0x^n + \ldots + a_n) = 0$ then $ua_0 = \ldots = ua_n = 0$. This hypothesis is stable by localisation: x is still strongly transcendent over C in $D[1/u]$ for any $u \in D$. More generally, if U is a monoid of D then x is still strongly transcendent over C in D_U. We assume also that I is an ideal of C, that $P(T, X) = T^m + a_1(X)T^{m-1} + \ldots + a_m(X)$ and $Q(T, X) = X^nT^n + \mu_1(X)X^{n-1}T^{n-1} + \ldots + \mu_n(X)$ in $C[X, T]$ are such that $\mu_1(X), \ldots, \mu_n(X) \in IC[X]$, $m \leq n$ and that $t \in D$ is such that $P(t, x) = Q(t, x) = 0$. The goal is to show that, under these hypotheses, we have t integral over $IC[x]$[1]. By Lemma 2.12 this is equivalent to say that 0 belongs to the monoid $t^{\mathbb{N}} + IC[x, t]$, and by localising at this monoid U, i.e. replacing D by D_U, we are reduced to show that $1 = 0$ in D.

Lemma 2.14 *Assume $C_1 \subseteq D$, that x is transcendent over C_1 and that $G(T, x) = T^k + b_1(x)T^{k-1} + \ldots + b_k(x)$ divides $Q(T, x)$, with $b_1(x), \ldots, b_k(x) \in C_1[x]$ and $G(t, x) = 0$. Then D is a trivial ring.*

Proof. Since x is transcendent over C_1 we have that $G(T, X) = T^k + b_1(X)T^{k-1} + \ldots + b_k(X)$ divides $Q(T, X) = X^nT^n + \mu_1(X)X^{n-1}T^{n-1} + \ldots + \mu_n(X)$. By taking $T = X^N$ we see that $X^{Nk} + b_1(X)X^{N(k-1)} + \ldots + b_k(X)$ divides $X^nX^{Nn} + \mu_1(X)X^{n-1}X^{N(n-1)} + \ldots + \mu_n(X)$. If N is big enough we can apply Lemma 2.13 and conclude that all coefficients of $b_1(X), \ldots, b_k(X)$ are integral over I. Since $G(t, x) = t^k + b_1(x)t^{k-1} + \ldots + b_k(x) = 0$ it follows that t is integral over $IC[x]$, and so D is a trivial ring. □

Lemma 2.15 *If $u \in D$ and u, ux are integral over C then $u = 0$.*

Proof. We have $(ux)^l + c_1(ux)^{n-1} + \ldots + c_l = 0$ for some $c_1, \ldots, c_l$ in C. From $c_l = -(ux)^l - c_1(ux)^{n-1} - \ldots - c_{l-1}ux$ and the fact that u is integral over C and that D is reduced it follows that we have $c_l = 0$. We have then $ux((ux)^{l-1} + \ldots + c_{l-1}) = 0$ and similarly $uxc_{l-1} = 0$ and so $uc_{l-1} = 0$. In this way we deduce $uc_{l-2} = \ldots = u = 0$. □

Corollary 2.16 *If $C_1 \subseteq D$ and C_1 is integral over C then x is strongly transcendent over C_1.*

[1] At this point, Peskine's argument is essentially to introduce a minimal prime of D to reduce the proof to the case where D is an integral domain. We avoid the use of this minimal prime ideal by considering all subresultants instead of the gcd of the polynomials $P(T, x)$ and $Q(T, x)$.

Lemma 2.17 *If $C_1 \subseteq D$ and x is strongly transcendent over C_1 and $a \in C$ then x is strongly transcendent over $C_1[1/a]$ in $D[1/a]$.*

Lemma 2.18 *D is a trivial ring.*

Proof. We compute the subresultants of $P(T, x)$ and $Q(T, x)$ in $C[x][T]$ and we show that they are all 0, i.e. $P(T, x)$ has to divide $Q(T, x)$. The conclusion follows then from Lemma 2.14. We consider one such subresultant $s_0(x)T^k + c_1(x)T^{k-1} + \ldots + c_k(x)$ asssuming that all previous subresultants have been shown to be 0. We can assume $s_0(x)$ to be invertible, replacing D by $D[1/s_0]$. 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 $T^k + b_1(x)T^{k-1} + \ldots + b_k(x)$ divides $P(T, x)$ we have that $b_1(x), \ldots, b_k(x)$ are integral over $C[x]$ by Lemma 2.13. By Lemma 2.4, $b_1(x), \ldots, b_k(x)$ are in $C_1[1/a][x]$ with C_1 integral over C. By Corollary 2.16 and Lemmas 2.14 and 2.17, we have $1 = 0$ in $D[1/a]$ and hence $a = 0$ in D. $\square$

Corollary 2.19 *If $S = R[x, t]$ and R is integrally closed in S and t is integral over $R[x]$ and I ideal of R such that $tx \in \sqrt{IS}$ then $t \in \sqrt{IS}$ mod $\sqrt{J}$ where $J = (R[x] : S)$.*

Proof. This follows from Corollary 2.11 and Lemma 2.18. $\square$

Corollary 2.20 *If $A \subseteq C[x] \subseteq B$ and t in M and t is integral over $C[x]$ and $tx \in \sqrt{\mathfrak{M}C[x, t]}$ then there exists u in M such that u, ux are integral over C.*

Proof. Let R be the integral closure of C in $S = C[x, t]$. By Corollary 2.3, it is enough to find a polynomial in $R[T]$, with one coefficient in M, of which x is a root. By Corollary 2.19 we get $a \in J \cap M$. Since $a, at \in M \cap R[x]$ both are polynomial in $R[x]$ and both have their constant coefficient in M. Using $tx \in \mathfrak{M}C[x, t]$ we get a polynomial in $R[T]$, with one coefficient in M, of which x is a root. $\square$

Lemma 2.21 *If t, ty are integral over $A[x]$ and s, sx integral over A then there exists N such that $s^N t, s^N tx, s^N ty$ are integral over A.*

Proof. We write $t^k + a_1(x)t^{k-1} + \ldots + a_k(x) = 0$ and $t^l y^l + b_1(x)t^{l-1}y^{l-1} + \ldots + b_l = 0$. 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 A, and we take $N = d + 1$. $\square$

We now have all the elements for the proof of main Theorem.

Theorem 2.1 *We assume that $B = A[x, y]$ is an A-algebra such that $x, y \in \mathfrak{M}B$. There exists $s \in 1 + \mathfrak{M}B$ such that s, sx, sy are integral over A.*

Proof. We can write $y = \mu(y)$ with $\mu(y) \in \mathfrak{M}[x][y]$. The polynomial $T - \mu(T)$ in $A[x][T]$ is then a polynomial, which is 1 mod $\mathfrak{M}B$, of which y is a root. Hence by Corollary 2.3 there exists w in M such that w, wy integral over $A[x]$. We can even assume $wy \in A[x]$.

Since $x \in \mathfrak{M}B$ we have $xw^l \in \mathfrak{M}A[x, w, wy]$ for l big enough. If we take $t = w^l$ it follows from Lemma 2.12 that we have $xt \in \sqrt{\mathfrak{M}S}$ where $S = A[x, t]$. By Corollary 2.20 we find $u \in M$ such that u, ux are integral over A. We can then take $s = tu^N$ for N big enough using Lemma 2.21. $\square$

We show that the same argument works with $B = A[x_1, x_2, x_3]$. We have $\nu_i(X_1, X_2, X_3) \in \mathfrak{M}A[X_1, X_2, X_3]$ such that

$$x_1 = \nu_1(x_1, x_2, x_3),\ x_2 = \nu_2(x_1, x_2, x_3),\ x_3 = \nu_3(x_1, x_2, x_3)$$

Using Corollary 2.3 we compute first t in M such that t is integral over $A[x_1, x_2]$ and $tx_3 \in A[x_1, x_2]$. We have then for some l that $x_2 t^l$ is in $\mathfrak{M}A[x_1, x_2, t, tx_3]$ and hence is in $\sqrt{\mathfrak{M}A[x_1, x_2, t^l]}$. Using 2.19 we find u in M such that ut^l is in $C[x_2]$ where C is the integral closure of $A[x_1]$. Then using $x_2 \in \sqrt{\mathfrak{M}A[x_1, x_2, t^l]}$ again we find a polynomial in $C[T]$, which is 1 mod $\mathfrak{M}B$, of which x_2 is a root, and hence we can find v in M such that v, vx_2 are in C, i.e. are integral over $A[x_1]$. Taking $w = tv^N$ for v large enough, we get w in M such that w, wx_3, wx_2 are integral over $A[x_1]$. Since $x_1 = \nu_1(x_1, x_2, x_3)$ we can find p large enough such that $x_1 w^p$ is in $\mathfrak{M}A[x_1, w, wx_2, wx_3]$ and using Corollary 2.20 we find s in M such that s, sx_1 are integral over A. We can then finish by taking ws^M for M big enough.

3 Examples

3.1 One variable

If we have a system $x = a_0 + a_2x^2 + \ldots + a_nx^n$ with $a_0 \in \mathfrak{M}$. We first take $t = 1 - a_2x - \ldots - a_nx^{n-1}$ and we have $xt = a_0$. In this case it is easy to compute the equation for t since $t - 1 = -a_2x - \ldots - a_nx^{n-1}$ and hence $t^{n-1}(t-1) = -a_2a_0t^{n-2} - \ldots - a_na_0^{n-1}$. We find in this way the change of variables of [1].

3.2 Two variables

We analyse the 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

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

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 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

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

and so

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

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

If we take $s = tu^2$ we have s, sx, sy integral over A. Indeed, ux is in A and since $t^2 - (1 + ax)t - b + ax^2$ we have tu and hence s integral over A. Since $ty = b - ax^2$ we have $sy = vu^2 - a(ux)^2$ integral over A. Finally $sx = (tu)(ux)$ is integral over A.

For this example, it can be checked that u satisfies the equation $f(u) = 0$ with

$$f(u) = u^4 - u^3 + (a^2 - 4ab - b^2)u^2 + a(2b - a)u + a^2b(4b - a)$$

One can then check that if we take

$$x = \frac{a}{u}, \qquad y = \frac{bu^2 - a}{u(u^2 - a(2b - a))}$$

then one has identically $-b + y + ax^2 + axy + by^2 = 0$ and the equation $f(u) = 0$ implies $-a + x + bxy + 2bx^2 = 0$. Thus, the system $(*)$ has a solution in A_f which is a simple Hensel extension of A.

References

[1] M-E. Alonso, H. Lombardi and H. Perdry. Elementary Constructive Theory of Henselian Local Rings. Preprint 2005.

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

[CC] J. Cederquist and Th. Coquand. Entailment Relations and Distributive Lattices. *Proceeding of Logic Colloquium 1998.*

[3] E. Hallouin. Parcours initiatique à travers la théorie des valuations. technical report. Université de Poitiers, 1997.

[4] P. Johnstone. *Stone Spaces.* Cambridge studies in advanced mathematics 3, 1982.

[5] H. Lombardi and C. Quitté. *Algèbre Commutative. Modules projectifs de type fini.* to appear, 2006

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

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

[8] G. Wraith. Generic Galois theory of local rings. in *Applications of sheaves*, pp. 739–767, Lecture Notes in Math., 753, Springer, Berlin, 1979.