Some Lemmas around Peskine's Proof of Zariski Main Theorem

January 7, 2008

Introduction

We present a constructive reading of Peskine's proof of Zariski Main Theorem [4].

1 Main Lemma

Lemma 1.1 *Let k be a field, and P, Q two polynomials in $k[X,T]$. There exists G, P_1, Q_1 in $k[X,T]$ such that $P = GP_1,\ Q = GQ_1$ and G belongs to the ideal $<P,Q>$ in $k(X)[T]$.*

Proof. This follows from Theorem 4.7 of [3]. □

Let A be a ring and $\mathfrak{m}$ an ideal of A. If $\phi : A \to k$ is a map from A to a field k we still write $\phi : A[X,T] \to k[X,T]$ for the canonical extension of this map to the polynomial ring $A[X,T]$ (that is $\phi(\Sigma a_{ij}X^iT^j) = \Sigma\phi(a_{ij})X^iT^j$). We assume given two polynomials $P(X,T) = T^n + p_1(X)T^{n-1} + \ldots + p_n(X)$ and $Q(X,T) = X^mT^l + \mu(X,T)$ in $A[X,T]$ with $\mu(X,T)$ in $\mathfrak{m}A[X,T]$.

Lemma 1.2 *For any map $\phi : A \to k$ there exists a polynomial $S = T^p + \nu(X,T)$ in $A[X,T]$, with $\nu(X,T)$ in $\mathfrak{m}A[X,T]$ such that $\phi(S)$ belongs to the ideal $<\phi(P), \phi(Q)>$ in $k(X)[T]$.*

Proof. We apply Lemma 1.1 to $\phi(P)$ and $\phi(Q)$. We have $\phi(P) = GA,\ \phi(Q) = GQ_1$ with P_1, Q_1 in $k[X,T]$ and G belongs to the ideal $<\phi(P), \phi(Q)>$ in $k(X)[T]$. We can assume that G is of the form $T^k + q_1(X)T^{k-1} + \ldots + q_k(X)$. Let R be the integral closure of $\phi(A)$ in k. Using Kronecker's Theorem, we see that all coefficients of G, P_1, Q_1 are in R. Modulo $\sqrt{\phi(\mathfrak{m})R}$ we get that $\phi(Q)$ if X^mT^l and hence G is T^k modulo $\sqrt{\phi(\mathfrak{m})R}$. Hence all coefficients of $q_1, \ldots, q_k$ are in $\sqrt{\phi(\mathfrak{m})R}$. Hence [1], G divides a polynomial $\phi(S)$, with $S = T^p + \nu(X,T)$ in $A[X,T]$, and $\nu(X,T)$ in $\mathfrak{m}A[X,T]$. □

To each ring A we can associate its spectrum for the constructible topology, which has for basic open $D(a) \cap V(b_1, \ldots, b_n)$. We have a sheaf of rings which associates to $D(a) \cap V(b_1, \ldots, b_n)$ the reduced ring $(A/\sqrt{<b_1, \ldots, b_n>})[1/a]$. The stalk of this sheaf at the point $\mathfrak{p}$ is the residual field $k_{\mathfrak{p}}$. We can apply Lemma 1.2: we obtain a continuous family of polynomials $S_{\mathfrak{p}}(X,T) = T^{p_{\mathfrak{p}}} + \nu_{\mathfrak{p}}(X,T)$ in $k_{\mathfrak{p}}[X,T]$ and maps $\phi_{\mathfrak{p}} : A \to k_{\mathfrak{p}}$ such that $\phi_{\mathfrak{p}}(S_{\mathfrak{p}})$ belongs to the ideal $<\phi_{\mathfrak{p}}(P), \phi_{\mathfrak{p}}(Q)>$ in $k_{\mathfrak{p}}(X)[T]$.

More concretely, this corresponds to building a binary tree where nodes are reduced rings R and where each branching is determined by an element a of A: to the left we change R by $R[1/a]$ and to the right we change R to $R/\sqrt{<a>}$. The root of the tree is the reduced ring $A/\sqrt{<0>}$ associated to A. To each leaf of this tree is associated a ring $R_i = (A/\sqrt{<b_1, \ldots, b_l>})[1/a_1 \ldots a_k]$ which is obtained by inverting some elements $a_1, \ldots, a_k$ and annulating some elements $b_1, \ldots, b_l$.

To each leaf is also associated a polynomial $S_i = T^{p_i} + \nu_i(X,T)$ in $A[X,T]$, with $\nu_i(X,T)$ in $\mathfrak{m}A[X,T]$. Furthermore we can write $N_iS_i = L_iP + M_iQ$ in $R_i[X,T]$ where L_i, M_i are in $A[X,T]$, N_i is in $A[X]$ and at least one coefficient of N_i divides a power of $a_1 \dots a_k$.

Notice that for building this tree, A does not need to be discrete (i.e. to have a decidable equality). Here is a simple example: $P = T^2 - b^2$ and $Q = XT - a$. We have the identity

$$(XT + a)(XT - a) - X^2(T^2 - b^2) = X^2b^2 - a^2$$

So we have three cases. If $a \neq 0$ or if $a = 0$ and $b \neq 0$ the gcd is 1. If $a = b = 0$ then the gcd is T.

2 Some applications

Here is a first application of Lemma 1.2, which classically is proved by using minimal prime ideals.

Corollary 2.1 *Let A be a ring with an ideal $\mathfrak{m}$. Let $B = A[x,t]$ be a reduced ring, with t integral over $A[x]$ and xt is in $\sqrt{\mathfrak{m}A[x,t]}$. We assume that x is* strongly transcendant *over A: if $u(a_0 + \dots + a_nx^n) = 0$ with u in B and $a_0, \dots, a_n$ in A then we have $ua_0 = \dots = ua_n = 0$ in B. Then t belongs to $\sqrt{\mathfrak{m}A[x,t]}$.*

Proof. We have $P(X,T) = T^n + p_1(X)T^{n-1} + \dots + p_n(X)$ such that $P(x,t) = 0$ and $Q(X,T) = X^mT^l + \mu(X,T)$ in $A[X,T]$ with $\mu(X,T)$ in $\mathfrak{m}A[X,T]$ such that $Q(x,t) = 0$. Applying Lemma 1.2 we get a binary tree with polynomials $S_i(X,T) = T^{p_i} + \nu_i(X,T)$ with $\nu_i(X,T)$ in $\mathfrak{m}A[X,T]$ on each leaves. Let Π be the product of all elements $S_i(x,t)$. We claim that we have $\Pi = 0$ in B which shows that t is integral over the ideal $\mathfrak{m}A[x]$.

To simplify the presentation, we consider the case where the tree has three branches, one for $a \neq 0$, one for $a = 0, b \neq 0$ and one for $a = b = 0$. The argument is general however and consists, like in [2] in going through this tree systematically to the leftmost branch. We have S_1 for $a \neq 0$, S_2 for $a = 0, b \neq 0$ and S_3 for $a = b = 0$. We write $s_i = S_i(x,t)$. We know that x is strongly transcendant and hence that x is transcendant in $B[1/a]$. We have also an equality $S_1N_1 = L_1P + M_1Q$ with L_1, M_1 in $R[1/a][X,T]$ and N_1 in $R[1/a][X]$ with at least one coefficient invertible in $R[1/a]$. Hence we have $as_1 = 0$. Thus $a = 0$ in $B[1/s_1]$. This implies that $a = 0$ in $B[1/bs_1]$, and hence $bs_1s_2 = 0$ in B. This implies $b = 0$ in $B[1/s_1s_2]$ and hence $\Pi = s_1s_2s_3 = 0$ in B. □

The following Lemma is proved in a constructive way in [4].

Lemma 2.2 *Let $B = A[x,t]$ be such that t is integral over $A[x]$. Let R be the subring of B of elements that are integral over A and let α be the conductor $(R[x] : B)$. Then x is strongly transcendant in $B/\sqrt{\alpha}$.*

An application of Corollary 2.1 and Lemma 2.2 is then the following result.

Proposition 2.3 *Let A be a ring with an ideal $\mathfrak{m}$. If B is 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 $\sqrt{\mathfrak{m}B}$. If α is the conductor $(R[x] : B)$ then α meets $t^{\mathbb{N}} + \mathfrak{m}B$.*

Corollary 2.4 *Let A be a ring with an ideal $\mathfrak{m}$. If B is 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 $\sqrt{\mathfrak{m}B}$. There exists $a_0, \dots, a_n$ in B such that $a_0 + \dots + a_nx^n = 0$ and $<a_0, \dots, a_n>$ meets $t^{\mathbb{N}} + \mathfrak{m}B$.*

Proof. Let R be the integral closure of A in B. Using Corollary 2.1 and Lemma 2.2 we find s of the form $t^l + \nu$, with ν in $\mathfrak{m}B$ such that s is in $(R[x] : B)$. In particular s and st are in $R[x]$ and we can write $s = s_0 + s_1 x + \ldots$ and $at = r_0 + r_1 x + \ldots$ with s_i, r_j in R. Using that xt is integral over $\mathfrak{m}A[x]$ we get a relation of the form $x^n t^n = \mu(x,t)$ with $\mu(x,t) \in \mathfrak{m}A[x,t]$. If we multiply by a large enough power of s we get a polynomial relation

$$a_0 + a_1 x + \ldots + a_n x^n = 0$$

Furthermore $a_0 + a_1 X + \ldots$ is the product of $s_0 + s_1 X + \ldots$ and $r_0 + r_1 X + \ldots$ in $B[X]$ mod. $\mathfrak{m}B$. Using the fact that the product of primitive polynomials is primitive, we have that $<a_0, \ldots, a_n>$ meets $t^{\mathbb{N}} + \mathfrak{m}B$. $\square$

Corollary 2.5 *Let A be a ring with an ideal $\mathfrak{m}$. If B is 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 $\sqrt{\mathfrak{m}B}$. There exists $b_0, \ldots, b_n$ such that $<b_0, \ldots, b_n>$ meets $t^{\mathbb{N}} + \mathfrak{m}B$ and $b_0, \ldots, b_n, b_0 x, \ldots, b_n x$ are integral over A.*

We can now state our constructive version of Zariski Main Theorem.

Theorem 2.6 *Let A be a ring with an ideal $\mathfrak{m}$. If B integral extension of $A[x_1, \ldots, x_n]$, and let R be the integral closure of A in B. Assume that we have primitive polynomials $p_1, \ldots, p_n$ in $A[X]$ such that $p_i(x_i)$ is in $\sqrt{\mathfrak{m}B}$ then there exists $f_1, \ldots, f_k$ in R such that all elements $f_j x_i$ are in R and $1 = <f_1, \ldots, f_k>$ in B.*

Corollary 2.7 *Let A be a ring and B is a 0-dimensional extension of A. Let R be the integral closure of A in B. There exists $f_1, \ldots, f_k$ in R such that $1 = <f_1, \ldots, f_k>$ in B and $B_{f_i} = R_{f_i}$.*

References

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

[2] H. Lombardi, C. Quitté On Seminormality Theoretical Computer Science, to appear

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

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