Math 711: Lecture of November 19, 2004

Proposition. *Let B be a domain that is an algebra over a field $\mathcal{K}$ and let $\mathcal{L}$ denote the fraction field of B. We assume that B has characteristic $p > 0$, since in characteristic zero B is always separable over $\mathcal{K}$. The following conditions are equivalent:*

(1) *B is separable over $\mathcal{K}$.*

(2) *$\mathcal{L}$ is separable over $\mathcal{K}$.*

Moreover, if B is finitely generated over $\mathcal{K}$ the following conditions are also equivalent:

(3) *$\mathcal{K}^{1/p} \otimes_{\mathcal{K}} \mathcal{L}$ is reduced.*

(4) *$\mathcal{L}$ has a separating transcendence basis over $\mathcal{K}$.*

(5) *For some element $b \in B - \{0\}$, B_b is smooth over $\mathcal{K}$.*

(6) *If B is presented as $\mathcal{K}[Y_1, \ldots, Y_d]_G/(F_1, \ldots, F_h)$, where the quotient has dimension $d - h$, then some $h \times h$ minor of $\bigl(\dfrac{\partial F_j}{\partial Y_i}\bigr)$ has nonzero image in B.*

Proof. For any field extension $\mathcal{K}'$ of $\mathcal{K}$, $\mathcal{K}' \otimes_{\mathcal{K}} B \subseteq \mathcal{K}' \otimes_{\mathcal{K}} \mathcal{L}$, and the latter is a localization of the former, so that the two rings are reduced or not alike. Thus, (1) $\Leftrightarrow$ (2) is clear. Moreover, (2) $\Rightarrow$ (3) is immediate from the definition of separability.

The proof that (3) $\Rightarrow$ (4) is similar to the argument given earlier for the case where $\mathcal{K}$ is perfect. Choose a transcendence basis $\underline{u} = u_1, \ldots, u_s$ so as to minimize the degree of $\mathcal{L}$ over $\mathcal{L}_0 = \mathcal{K}(\underline{u})^{\mathrm{sep}}$, where $^{\mathrm{sep}}$ indicates separable closure in $\mathcal{L}$. If $v \in \mathcal{L}$ is not in $\mathcal{L}_0$, let $G(u_1, \ldots, u_d, V) \in \mathcal{K}[u_1, \ldots, u_d, V]$ be its minimal polynomial over $\mathcal{K}(u_1, \ldots, u_s)$, with denominators efficiently cleared. This polynomial is irreducible. If some exponent on one of the variables, say u_i, is not divisible by p, we can use the u_j for $j \neq i$ and v as a transcendence basis $\underline{u}'$. Then $\mathcal{K}(\underline{u}')^{\mathrm{sep}}$ contains u_i, because $G(\underline{u}, v)$ gives a polynomial that u_i satisfies that is separable over $\mathcal{K}(\underline{u}')$. This implies that $\mathcal{L}_1 = \mathcal{K}(\underline{u}')^{\mathrm{sep}} \supseteq \mathcal{L}_0$. But $v \in \mathcal{K}(\underline{u}')^{\mathrm{sep}}$, and so $[\mathcal{L} : \mathcal{L}_1] < [\mathcal{L} : \mathcal{L}_0]$. Thus, all exponents on all variables are divisible by p (this must be true for V, since G is not separable in V). Since G is irreducible, not all of its coefficients are pth powers, or it will be a pth power itself. We can therefore form $H(V) \in \mathcal{K}^{1/p} \otimes_{\mathcal{K}} \mathcal{K}[u_1, \ldots, u_s, V]$ such that $H^p = G$, and at least one coefficient of H is in $\mathcal{K}^{1/p} - \mathcal{K}$. It follows that $H(v)^p = G(v) = 0$, and to complete the proof it will suffice to check that $H(v)$ itself is nonzero. Note that $\mathcal{K}(\underline{u})(v) \cong \mathcal{K}(\underline{u})[V]/\bigl(G(V)\bigr)$, and so $\mathcal{K}^{1/p} \otimes_{\mathcal{K}} \mathcal{K}(\underline{u})(v) \cong \mathcal{K}^{1/p}(\underline{u})[V]/\bigl(G(V)\bigr)$, and this contains $H(v)$ and is contained in $\mathcal{K}^{1/p} \otimes_{\mathcal{K}} \mathcal{L}$. It therefore suffices to check that $H(V)$ is not a multiple of $G(V)$ in $\mathcal{K}^{1/p}(\underline{u})[V]$, which is obvious since $H(V)^p = G(V)$.

If there is a separating transcendence basis, after replacing B by a suitable localization at one element we may assume that the separating transcendence basis $\underline{u}$ is in B. We may then choose a primitive element v for the finite separable algebraic field extension $\mathcal{K}(\underline{u}) \subseteq \mathcal{L}$, and we may similarly assume that this element is in B. After inverting one more element, we may assume the extension is generated over a localization $\mathcal{K}[\underline{u}]_g$ by v, where v is a simple root of a monic polynomial $f(V)$ over $\mathcal{K}(\underline{u})$ whose coefficients are actually in $\mathcal{K}[\underline{u}]_g$. Inverting the value of f' makes this extension étale over a localization at one element of a polynomial ring, and, therefore, smooth.

But (5) and (6) are equivalent by the Jacobian criterion for smoothness: if a minor is nonzero we may invert it to achieve smoothness, while if the localization is smooth some $h \times h$ minor is invertible and, therefore, nonzero.

Finally, smooth algebras are obviously separable, since they remain regular, and so reduced, after any finite extension of the base field, so that (5) $\Rightarrow$ (2). $\square$

We now return to the problem of proving the Artin Approximation Theorem. Let $\delta(x, Y)$ be a nonvanishing minor of the Jacobian matrix, which we assume, by renumbering, comes from the first h rows. If the base V is a DVR we also assume for the moment that the image of $\delta(x, Y)$ in $\widehat{A}$ is not divisible by t. We will need to justify this assertion later.

Let $R = A^{\mathrm{h}}$ and $\mathfrak{A} = m^N$ in the Tougeron implicit function theorem. It follows that in order to complete the proof of the Artin Approximation Theorem it suffices to show that given a finitely generated T-subalgebra $S = T[s_1, \ldots, s_d]$ of $\widehat{A}$ and

$$F_1, \ldots, F_h \in T[Y_1, \ldots, Y_d]$$

generating $PT[Y_1, \ldots, Y_d]_P$, where P is the prime ideal of relations on the $s_1, \ldots, s_d$, then for every positive integer N there exists $y' = y'_1, \ldots, y'_d \in A^{\mathrm{h}}$ such that

$$(*) \qquad y' \equiv s \bmod m^N \widehat{A}$$

and

$$(**) \qquad F_j(y') \equiv 0 \bmod \delta^2(x, y') m^N.$$

The Tougeron Implicit Function Theorem enables us to pass from the solution of the equations mod $\delta^2(x, y')m^N$ to an “honest” solution. The next idea is this: we prefer to worry about a solution mod $\delta^2(x, y')$ and not about the factor m^N, which can be handled automatically by a trick.

The following Lemma permits this reduction:

Lemma. *Suppose that $V[x_1, \ldots, x_\nu]^{\mathrm{h}}_{(t,x)}$ is an approximation ring for $\nu < n$. Suppose that we have elements $g, F_1, \ldots, F_h$ and $s_1, \ldots, s_d \in \widehat{A}$ such that t does not divide $g(x, s)$ in $\widehat{A}$ while $g(x, s)$ divides $F_j(x, s)$ in $\widehat{A}$ for $1 \le j \le h$.*

Then for every positive integer N there exists $\underline{y}_N = y_{1N}, \ldots, y_{dN} \in (A^{\mathrm{h}})^d$ such that $F_j(x, \underline{y}_N)$ is divisible by $g(x, \underline{y}_N)$ for all j and $s \equiv \underline{y}_N \bmod m^N \widehat{A}$.

By applying this with $g = \delta(x, Y)^2$ for larger and larger values of N, we can get the conclusions $(*)$ and $(**)$ we need to complete the proof of the Theorem. Of course, we still need to prove the Lemma, and for that we shall need the Weierstrass preparation theorem.