Math 711: Lecture of November 15, 2004

By the result proved last time, we need only prove that rings of the form $V[\underline{x}]^{\mathrm{h}}_Q$ are approximation rings, where (V, tV) denotes either $(K, 0)$, where K is a field, or (V, tV) where V is an excellent DVR.

We need to show that given a solution of a finite system of polynomial equations over such a ring with coefficients in A^{h}, where $A = V[\underline{x}]_Q$, if there is a solution in $\widehat{A}$, there is a solution in A^{h}.

First, we want to get rid of coefficients in A^{h}: we want to use coefficients in A. The idea is to use systems over A with a congruence condition instead.

Lemma. *Let (A, m) be as above and suppose that for every system of polynomial equations $F_j(Y_1, \ldots, Y_d) = 0$, $1 \le j \le s$, with coefficients in A, if there is a solution $(\widehat{y}_1, \ldots, \widehat{y}_d)$ over $\widehat{A}$, then for every positive integer N there is a solution $(y'_1, \ldots, y'_d)$ over A^{h} such that $y'_j \equiv \widehat{y}_j$ mod $m^N\widehat{A}$, $1 \le j \le d$. Then A^{h} is an approximation ring.*

Proof. Suppose that we are given a system of equations $F_j(Y_1, \ldots, Y_d) = 0$ over A^{h} with a solution $(\widehat{y}_1, \ldots, \widehat{y}_d)$ over $\widehat{A}$. We must show that these equations have a solution in A^{h}. For each coefficient $c_{\mu,j}$ of F_j in (we have that $c_{\mu,j} \in A^{\mathrm{h}}$) we introduce a new variable $Z_{\mu,j}$. Let $G_j = G_j(Y, Z)$ be the polynomial obtained from F_j by replacing every coefficient $c_{\mu,j}$ by the corresponding variable. Thus, G_j has coefficients each of which is 1 or 0.

Every $c_{\mu,j}$ is algebraic over A: for every choice of μ and j, choose a nonzero polynomial equation $H_{\mu,j}(Z_{\mu,j}) = 0$ with coefficients in A that is satisfied by $c_{\mu,j}$. For all μ, j we can choose N so large that if c is any root of $H_{\mu,j}(Z_{\mu,j}) = 0$ in A^{h} with $c \neq c_{\mu,j}$, then $c - c_{\mu,j} \notin m^N A^{\mathrm{h}}$, and since there are only finitely many choices of μ, j we can choose a single value of N so large that this condition holds simultaneously for all μ, j.

Now consider the family of equations $G_j(Y, Z) = 0$ together with $H_{\mu,j}(Z_{\mu,j}) = 0$. These have the solution $Y = (\widehat{y}_1, \ldots, \widehat{y}_d)$, $Z_{\mu,j} = c_{\mu,j}$ in $\widehat{A}$. It follows from our hypothesis that these equations have a solution $(y'_1, \ldots, y'_d)$, $c'_{\mu,j}$ in A^{h} that is congruent to the first solution mod $m^N\widehat{A}$. For all μ, j , we have that $c'_{\mu,j}$ and $c_{\mu,j}$ are both roots of $H_{\mu,j}(Z_{\mu,j}) = 0$ in A^{h}, and that $c'_{\mu,j} - c_{\mu,j} \in m^N\widehat{A} \cap A^{\mathrm{h}} = m^N A^{\mathrm{h}}$. By our choice of N, we must have that $c'_{\mu,j} = c_{\mu,j}$ for all μ, j. But when these values are used for the $Z_{\mu,j}$, the polynomials $G_j(Y, Z)$ become the polynomials $F_j(Y)$ with which we started. Therefore $(y'_1, \ldots, y'_d)$ is a solution of the equations $F_j(Y) = 0$ in A^{h}, as required. $\square$

We next observe that once we know the coefficients are in $A = T_Q$, we may multiply by an element of $T - Q$ to clear denominators. Since $\widehat{A}$ is regular it is a domain, and the solutions of the equations in both A^{h} and in $\widehat{A}$ are unaffected. Hence:

Corollary. *Let (A, m) and $T = V[x_1, \ldots, x_n]$ be as above and suppose that for every system of polynomial equations $F_j(Y_1, \ldots, Y_d) = 0$, $1 \le j \le s$, with coefficients in T, if there is a solution $(\widehat{y}_1, \ldots, \widehat{y}_d)$ over $\widehat{A}$, then for every positive integer N there is a solution*

$(y'_1, \ldots, y'_d)$ *over* A^{h} *such that* $y'_j \equiv \widehat{y}_j$ *mod* $m^N\widehat{A}$, $1 \leq j \leq d$. *Then* A *is an approximation ring.* $\square$

We next observe that we can state the result somewhat more conceptually this way: given a finitely generated T-subalgebra S of $\widehat{A}$ and a power of the maximal ideal m^N, there is a T-algebra map $\phi : S \to A^{\mathrm{h}}$ such that for every element $u \in S$, $\phi(u) \equiv u$ mod $m^N\widehat{A}$. Here, S is generated by solutions $\widehat{y_j}$ of a system of equations $F_j(Y)$ over T, and the elements $\widehat{y_j}$ satisfy these equations. The images under the homomorphism also satisfy the same equations. Note that the condition that $\phi(u) \equiv u$ mod $m^N\widehat{A}$ for all $u \in S$ is equivalent to the same condition imposed on a set of generators of S over T: the set of elements of S that satisfy this condition is a T-subalgebra of S, and so will be all of S if it contains generators for S as a T-algebra. We henceforth shall usually write $s_1, \ldots, s_d$ for a set of generators of S over T instead of writing $\widehat{y}_1, \ldots, \widehat{y}_d$.

By phrasing the problem in terms of S we achieve certain freedoms: we can change the generators of S and this changes the equations we need to solve. (We can even replace S by a larger finitely generated T-subalgebra of $\widehat{A}$: a homomorphism from the larger subalgebra may be restricted to the original subalgebra. We will not need to do this now, but will later in the DVR case.) We can map $T[Y_1, \ldots, Y_d] \twoheadrightarrow S$ and consider the kernel, which is a prime ideal P of $T[Y_1, \ldots, Y_d]$. We can take the equations we need to solve to be any set of generators of P. By making use of a congruence condition as well, we can do a little bit more.

Let h denote the height of the ideal P. Then $T[T_1, \ldots, T_d]_P$ is a regular local ring of dimension h, and we can choose h generators $F_1, \ldots, F_h$ for $PT[Y_1, \ldots, Y_d]_P$ such that $F_1, \ldots, F_h \in T[Y_1, \ldots, Y_d]$. Then $P/(F_1, \ldots, F_h)$ becomes 0 when we localize at P, and so there is an element $G \in T - P$ such that $GP \subseteq (F_1, \ldots, F_d) \subseteq P$.

Since $G(s_1, \ldots, s_d) \neq 0$ in $\widehat{A}$, by increasing the value of N, if necessary, we may guarantee that $G(s_1, \ldots, s_d) \notin m^N\widehat{A}$. Then it suffices to approximate the solution of $F_j(Y) = 0$ mod m^N, that is, it suffices to find $y'_1, \ldots, y'_d \in A^{\mathrm{h}}$ such that $y'_i \equiv s_i$ mod $m^N\widehat{A}$, $1 \leq i \leq d$ and $F_j(y'_1, \ldots, y'_d) = 0$, $1 \leq j \leq h$. We claim that it now follows that $F(y'_1, \ldots, y'_d) = 0$ for all $F \in P$. The reason is that we know that $GF \in (F_1, \ldots, F_h)$, and so

$$G(y'_1, \ldots, y'_d)F(y'_1, \ldots, y'_d) = 0$$

in the domain $\widehat{A}$. But

$$G(y'_1, \ldots, y'_d) \equiv G(s_1, \ldots, s_d) \text{ mod } m^N\widehat{A},$$

and since $G(s_1, \ldots, s_d) \notin m^N\widehat{A}$, it follows that $G(y'_1, \ldots, y'_d) \notin m^n\widehat{A}$, and, in particular, $G(y'_1, \ldots, y'_d) \neq 0$. Therefore, $F(y'_1, \ldots, y'_d) = 0$.

We shall soon see that we can assume that some $h \times h$ minor of $(\dfrac{\partial F_j}{\partial Y_i})$ is not contained in P, and in the DVR case we shall show by enlarging S so that $\widehat{A}/S$ is torsion-free over V that we may even assume that the image of some minor in $\widehat{A}$ is not divisible by t.

We shall also need the following generalization of the implicit function theorem characterization of Henselian local rings:

Lemma (Tougeron's implicit function theorem). *Let (R, m) be a Henselian quasilocal ring and let $F_1, \ldots, F_h \in R[Y_1, \ldots, Y_d]$. Let $\mathfrak{A} \subseteq m$ be any ideal. Let*

$$\delta = \delta(Y) = \det\Big(\frac{\partial F_j}{\partial Y_i}\Big)$$

be an $h \times h$ minor of the Jacobian matrix obtained by choosing h of the variables (equivalently, h rows of the Jacobian matrix).

Suppose that we can find elements $y'_1, \ldots, y'_d \in R$ such that for $1 \le j \le h$,

$$F_j(y') \equiv 0 \bmod \delta(y')^2\mathfrak{A}.$$

Then there exist $y_1, \ldots, y_d \in R$ such that for $1 \le j \le h$,

$$F_j(y) = 0 \text{ and } y \equiv y' \bmod \delta(y')\mathfrak{A}.$$

This statement looks a bit technical, but notice that if $d = h$, $\mathfrak{A} = m$, and $\delta(y')$ is a unit, this is precisely the implicit function theorem characterization of Henselian rings.