Commutative Algebra Seminar: Lecture of April 22, 2003

Before we can do Step 2 we need to discuss Henselization and related notions. A quasi-local ring $(R,\, m,\, K)$ is called *Henselian* if for every monic polynomial F over $R[X]$, if f denotes the image of F in $K[X]$, and one has a factorization $f = gh$ into monic polynomials such that g and h have no common factor, then this factorization lifts to R, i.e., one has $F = GH$ with G and H monic over $R[X]$, and such that the images of G and H modulo m are g and h, respectively. Hensel's Lemma asserts that complete local rings are Henselian. One constructs the factorization recursively: one shows that a factorization modulo m^N lifts to a factorization mod m^{N+1}.

Homomorphic images of Henselian rings are Henselian, and local module-finite extensions of Henselian rings are Henselian.

By a theorem, every quasi-local ring has a *Henselization*: a local homomorphism to a quasi-local ring R^{h} (R^{h} turns out to be Noetherian when R is) which is Henselian, and such that every local homomorphism to a Henselian ring T factors uniquely $R \to R^{\mathrm{h}} \to T$. R^{h} is unique up to unique isomorphism as an R-algebra. We focus on the case where R is Noetherian.

R^{h} is faithfully flat over R, and the maximal ideal of R expands to that of R^{h}. Moreover, $R \to R^{\mathrm{h}}$ induces an isomorphism of completions, so that R^{h} may always be thought of as a subring of $\widehat{R}$. Of course, the universal property of the Henselization provides a unique R-algebra map $R^{\mathrm{h}} \to \widehat{R}$. The map $R \to R^{\mathrm{h}}$ induces an isomorphism of residue class fields. Moreover, the ring R^{h} is a directed union of *pointed étale extensions* of R, and these, by a theorem, turn out to be the local extension algebras of the form $S = (R[X]/(F))_Q$ where:

(1) $F = F(x)$ is a monic polynomial in x.
(2) Q is a maximal ideal of $R[x]$ generated by m and a single linear polynomial of the form $x - r$, where r is an element of R such that $F(r) \in m$.
(3) If λ is the residue of r in K, then $\overline{F}'(\lambda) \neq 0$, where F' is the derivative of F with respect to X, and the bar indicates that the coefficients are to be reduced modulo m (this is equivalent to the requirement that the image of F' in S be invertible).

Every pointed étale extension of R admits a unique local R-algebra homomorphism into R^{h}.

The Henselization of an excellent local ring is excellent. The result we need is this:

Theorem (Artin approximation). *Let $(R,\, m,\, K)$ be an excellent local ring. If a system of polynomial equations in finitely many variables over R has a solution in $\widehat{R}$, then it has a solution in R^{h}. Moreover, given an integer $N > 0$, the solution in R^{h} can be chosen so that it is congruent to the original solution modulo $m^N\widehat{R}$.*

We want to point out right away that the solution can actually be taken in a pointed étale extension of R: we do not need to use all of R^{h}. This solution can therefore be chosen in a ring obtained from R by first making a module-finite extension of R and then localizing at a maximal ideal (which will necessarily lie over m).

The statement about the congruence conditions in the last sentence of the theorem can be deduced from what is asserted in the second sentence: the congruence condition is easily expressed by using extra equations involving extra variables. E.g., if $r \in R$ is congruent to the value in $\widehat{R}$ of one of the variables X modulo m^N, one can impose the additional equation that the solution for the variable X be congruent to r module m^N by an equation that sets $X - r$ equal to a linear combination of generators for m^N with unknown coefficients.

The theorem was first proved by M. Artin in the case of a local ring essentially of finite type over a field or over an excellent DVR, and also in the case of an analytic local ring (i.e., for a quotient of the ring of convergent power series in n variables over the complex numbers — analytic local rings are Henselian). The more general result follows from a theorem of D. Popescu called General Néron Desingularization: for a considerable time there was some controversy about whether Popescu's argument, which certainly had gaps, was essentially correct. The conflict was resolved in an expository paper by R. Swan which gave all details of a complete and correct proof. Swan's version was based in turn on a paper by T. Ogoma which also gave an exposition of the proof of Popescu's theorem. We shall assume the general form of Artin approximation here.

Step (2). Next, we want to show that we may assume that R is complete. Therefore, we want to show that if u is in the tight closure of I but not the plus closure, this is preserved when we complete. This will follow if we can show that if u is in the plus closure of $I\widehat{R}$, where R is excellent local and normal, then u is already in the plus closure of I.

The idea of the argument is to encode the problem of giving a module-finite extension T of a ring R_1 with $R \subseteq R_1 \subseteq \widehat{R}$ such that $u \in IT$ into solving a finite system of polynomial equations in finitely many variables with coefficients in R (but whose solutions we think of as in R_1). Once we have such a system, from the fact that the equations have a solution in $\widehat{R}$, we can deduce that they have a solution in a pointed étale extension of R. We then need to do some further work to show that R itself has a module-finite extension T such that $u \in IT$.

Fix generators for the module-finite extension T of R_1: call them $\theta_1, \ldots, \theta_h$. We choose h from the module-finite extension domain of $\widehat{R}$ such that u is in the expansion of I. We may assume without loss of generality that θ_1 is taken to be 1. The structure of T an R_1-algebra is completely determined by giving:

(1) The relations on the θ_k over R_1: think of these as given by an $h \times s$ unknowns (W_{ij}). The values w_{ij} of these coefficients determine the structure of T as an R_1-module: we assume that $\sum_i w_{ij}\theta_i = 0$ for every j, so that the module is the cokernel of the matrix (w_{ij}).

(2) For each θ_i and θ_j, the coefficients needed to write $\theta_i\theta_j$ as an R_1-linear combination of $\theta_1, \ldots, \theta_h$: say $\theta_i\theta_j = \sum_{k=1}^{h} y_{ijk}\theta_k$. Think of the Y_{ijk} as h^3 additional unknowns whose values y_{ijk} determine the multiplication.

We need equations to be satisfied to get a commutative associative ring to which R_1 maps, in which θ_1 is the identity, and such that $u \in IT$. We also need equations that will guarantee that T is an overring of R_1.

Since we want θ_1 to be an identity in T, we impose the condition that

(a) $Y_{1jk} = 1$ if $j = k$ and 0 otherwise.

We may guarantee commutativity by the condition that

(b) $Y_{ijk} = Y_{jik}$ for all i, j.

Associativity is more complicated. We can use the values of the Y_{ijk} to work out $(\theta_\mu\theta_\nu)\theta_\rho$. We first use the equations given in (2) to write $\theta_\mu\theta_\nu$ as a linear combination of the θ_k. We then multiply by θ_ρ and use several applications of the equations in (2) to write this as a linear combination of the θ_k. We proceed similarly to expand $\theta_\mu(\theta_\nu\theta_\rho)$. We get two different expressions, each of which is a linear combination of the θ_k whose coefficients are polynomials in the Y's. The difference gives a relation on the θ_k. The vector of coefficients from such a difference must therefore be a linear combination of the relations on the θ_k specified in (1).

(c) For each choice of μ, ν, and ρ, write down equations that represent the difference vector of coefficients described above as a linear combination, using new unknowns for coefficients, of the column vectors given in (1).

Recall that $x_1, \ldots, x_d$ generate I. The fact that $u \in IT$ can be expressed as follows.

(d) Consider $u\theta_1$ minus a linear combination of the θ_k, where each of the coefficients in the subtrahend is a linear combination of the x's with new unknown coefficients. Write the vector of coefficients of the θ_k arising in this difference as an unknown linear combination of the relation vectors from (1) using new unknowns again.

One can express the condition that the map $R_1 \to T$ be injective (in the case where, as here, circumstances are forcing R_1 to be a domain) by requiring that there exist a map $T \to R_1$ whose value on θ_1 (the identity) is not 0. The map is determined by its values on the θ_k. Use new unknowns Z_k for those values. The Z_k must satisfy:

(e) The relations imposed on the θ_k in (1).

In the case we are considering, where the original solution of the equations will be in $\widehat{R}$ and the new solution in R^{h}, the linear map from T to $\widehat{R}$ having nonzero value on θ_1 will actually have a value congruent to $r \in R$ mod m^N for some $N \gg 0$ such that $r \notin m^N$.

(f) Include an equation that sets $Z_1 - r$ equal to an unknown linear combination of the generators of m^N.

A module-finite extension domain T of $\widehat{R}$ such that $u \in IT$ gives a solution of the equations specified in (a) – (f) in $\widehat{R}$. By Artin approximation, there is a solution in a pointed étale extension S of R. Then $S \subseteq \widehat{R}$. Since R is excellent and normal, $\widehat{R}$ is normal and, in particular, is a domain. Note that $S \subseteq \widehat{R}$ is therefore also a domain. The solution in S gives a ring T_0 module-finite over S. It is an extension ring because there is an S-linear map to S whose value on 1 is not 0. Moreover, $u \in IT_0$. It is not clear that T_0 is a domain. But we may kill a minimal prime disjoint from $S - \{0\}$ and so we get a module-finite extension domain T_1 of S such that $u \in IT_1$.

Now, T_1 is a domain module-finite over a localization at a maximal ideal of a module-finite extension domain of R. We can replace T_1 by its localization at a maximal ideal. The resulting ring can be obtained as the localization at a maximal ideal m_2 of a module-finite extension domain T_2 of R. There is no harm in replacing T_2 by a larger domain that is integral over it. For sufficiently large $q = p^e \gg 0$, the fraction field of $R^{1/q}[T_2]$ will be separable over the fraction field of $R^{1/q}$. This field extension may be enlarged to be Galois. Thus, we may assume that T_3 is the integral closure of $R^{1/q}$ in a finite Galois extension of its fraction field. We know that there is a maximal ideal m_3 of T_3 lying over m_2, and since $u \in I(T_2)_{m_2}$, we have that $u \in I(T_3)_{m_3}$. We claim that $u \in IT_3$. To prove this, it suffices to show that it is true after localization at every maximal ideal of T_3. We claim that the Galois group G of the extension of fraction fields between $R^{1/q}$ and T_3 acts transitively on the maximal ideals of T_3. To see this, let v be an element in m_3 not in any of the other maximal ideals. Then $\prod_{g \in G} g(v)$ is invariant under the action of G, and so is in the fraction field of $R^{1/q}$. It is also integral over $R^{1/q}$. But since R is normal, $R^{1/q}$ is normal, and so $\prod_{g \in G} g(v) \in R^{1/q}$. Evidently, it must be in the maximal ideal. Therefore, every maximal ideal of T_3 contains it. But that means that every maximal ideal m' contains one of the elements $g(v)$, and then we must have $m' = g(m_3)$. It follows that $u \in I(T_3)_{m'}$ for every maximal ideal of T_3, and so $u \in IT_3$. Thus, $u \in IT_3$, and so $u \in I^+$. $\square$

We are now in the complete local case. Our counter-example is still one of smallest possible Krull dimension, and the parameter ideal is generated by a full system of parameters. In the next step we shall show that there is a Gorenstein counter-example of the same Krull dimension. In doing so we shall lose normality, but we shall make no further use of normality in the argument.