Math 615: Lecture of March 30, 2007

The following Theorem, which constructs coefficient rings when the maximal ideal of the ring is nilpotent, is the heart of the proof of the existence of coefficient rings in complete mixed characteristic local rings. Before giving the proof, we introduce the following notation, which we will use in another argument later. Let x, y be indeterminates over $\mathbb{Z}$. Let q be a power of p, a prime. Then $(x+y)^q - x^q - y^q$ is divisible by p in $\mathbb{Z}[x, y]$, since the binomial coefficients that occur are all divisible by p, and we write $G_q(x, y) \in \mathbb{Z}[x, y]$ for the quotient, so that $(x+y)^q = x^q + y^q + pG_q(x, y)$.

Theorem. *Suppose that (R, m, K) is local where K has characteristic $p > 0$, and that $m^n = 0$. Choose a p-base Θ for K, and a lifting of the p-base to R: that is, for every $\theta \in \Theta$ choose an element $t_\theta \in R$ with residue θ modulo m. Let $T = \{t_\theta : \theta \in \Theta\}$. Then R has a unique coefficient ring V that contains T. In fact, suppose that we fix any sufficiently large power $q = p^N$ of p (in particular, $N \geq n-1$ suffices) and let S_N be the set of all expressions of the form $\sum_{\mu\in\mathcal{M}} r_\mu^q \mu$, where the $\mathcal{M}$ is a finite set of mutually distinct N-special monomials in the elements of T and every $r_\mu^q \in R^q = \{r^q : r \in R\}$. Then we may take*

$$V = S_N + pS_N + p^2S_N + \cdots + p^{n-1}S_N,$$

which will be the same as the smallest subring of R containing R^q and T.

Before giving the proof, we note that it is not true in general that R^q is closed under addition, and neither is S_N, but we will show that for large N, V is closed under addition and multiplication, and this will imply at once that it is the smallest subring of R containing R^q and T. Of course, R^q *is* closed under multiplication.

Proof of the Proposition. We first note if $r \equiv s \bmod m$ then $r^q \equiv s^q \bmod m^n$ if $N \geq n-1$, by the Lemma at then end of the Lecture Notes of March 26. Therefore R^q maps *bijectively* onto $K^q = \{\lambda^q : \lambda \in K\}$ when we take residue classes mod m. It follows from our analysis of the properties of p-bases that the residue class map $R \to K$ sends S_N *bijectively* onto K.

Suppose that W is a coefficient ring containing T. For each $r \in R$, if $w \equiv r \bmod m$, then $w^q = r^q$. Thus, $R^q \subseteq W$. Then $S_N \subseteq W$, and so $V \subseteq W$. Now consider any element $w \in W$. Since S_N contains a complete set of representatives of elements of K, every element of W has the form $\sigma_0 + u$ where $\sigma_0 \in S_N$ and $u \in m \cap W = pW$, and so $w = \sigma_0 + pw_1$. But we may also write w_1 in this way and substitute, to get an expression

$$w = \sigma_0 + p\sigma_1 + p^2 w_2,$$

where σ_0, $\sigma_1 \in S_N$ and $w_2 \in W$. Continuing in this way, we find, by a straightforward induction, that

$$W = S_N + pS_N + \cdots + p^j S_N + p^{j+1}W$$

for every $j \geq 0$. We may apply this with $j = n-1$ and note that $p^n = 0$ to conclude that $W = V$. Thus, if there is a coefficient ring, it must be V. However, at this point we do not even know that V is closed under addition.

We next claim that V is a ring. Let $\widetilde{V}$ be the closure of V under addition. Then we can see that $\widetilde{V}$ is a ring, since, by the distributive law, it suffices to show that the product of two elements $p^i r^q \mu$ and $p^j r'^q \mu'$ has the same form. The point is that $\mu\mu'$ can be rewritten in the form $\nu^q \mu''$ where μ'' has all exponents $\leq q-1$, and $p^{i+j}(rr'\nu)^q \mu''$ has the correct form. Thus, $\widetilde{V}$ is the smallest ring that contains R^q and T.

We next prove that V itself is closed under addition. We shall achieve this by proving by reverse induction on j that $p^j V = p^j \widetilde{V}$ for all j, $0 \leq j \leq n$. The case that we are really aiming for is, of course, where $j = 0$. The statement is obvious when $j = n$, since $p^n = 0$ and $p^n V = p^n \widetilde{V} = 0$. Now suppose that $p^{j+1} V = p^{j+1} \widetilde{V}$ for some fixed j. We shall show that $p^j V = p^j \widetilde{V}$, thereby completing the inductive step. Since $p^j \widetilde{V}$ is spanned over $p^{j+1}\widetilde{V} = p^{j+1} V$ by $p^j S_N$, it will suffice to show that given any two elements of $p^j S_N$, their sum differs from an element of $p^j S_N$ by an element of $p^{j+1}\widetilde{V} = p^{j+1} V$. Call the two elements

$$v = p^j \sum_{\mu \in \mathcal{M}} r_\mu^q \mu$$

and

$$v' = p^j \sum_{\mu \in \mathcal{M}} r'^q_\mu \mu,$$

where $r_\mu, r'_\mu \in R$ and $\mathcal{M}$ is a finite set of n-special monomials in elements of T large enough to contain all those monomials that occur with nonzero coefficient in the expressions for v and v'. Since S_N gives a complete set of representatives of K and r^q only depends on what r is modulo m, we may assume that all of the r_μ and r'_μ are elements of S_N. Let

$$v'' = p^j \sum_{\mu \in \mathcal{M}} (r_\mu + r'_\mu)^q \mu.$$

Then

$$v'' - v - v' = p^j \sum_{\mu \in \mathcal{M}} p G_q(r_\mu, r'_\mu)\mu = p^{j+1} \sum_{\mu \in \mathcal{M}} G_q(r_\mu, r'_\mu)\mu \in p^{j+1} V',$$

as required, since all the r_μ, $r'_\mu \in S_N$ and $\widetilde{V}$ is a ring. This completes the proof that $\widetilde{V} = V$, and so V is a subring of R.

We have now shown that V is a subring of R, and that it is the only possible coefficient ring. It is clear that $pV \subseteq m$, while an element of $V - pV$ has nonzero image in K: its constant term in S_N is nonzero, and S_N maps bijectively to K. Thus, $m \cap V = pV$, and we know that $V/pV \cong K$, since S_N maps onto K. It follows that pV is a maximal ideal of V generated by a nilpotent, and so pV is the only prime ideal of V. Any nonzero element

of the maximal ideal can be written as $p^t u$ with t as large as possible (we must have that $t < n$), and then u must be a unit. Thus, every nonzero element of V is either a unit, or a unit times a power of p. It follows that every nonzero proper ideal is generated by p^k for some positive integer k, where k is as small as possible such that p^k is in the ideal. It follows that V is a principal ideal ring. Thus, V is a Noetherian local ring, and, in fact, an Artin local ring. $\square$

We want to extend this result to complete local rings in which m is not nilpotent. We first need:

Lemma. *Let K be a field of characteristic $p > 0$ and let (V, pV, K), (W, pW, K) and (V_n, pV_n, K), $n \in \mathbb{N}$, be coefficient rings.*

(a) *If $p^t = 0$ while $p^{t-1} \neq 0$ in V, which is equivalent to the statement that p^t is the characteristic of V, then $\mathrm{Ann}_V p^j V = p^{t-j}V$, $0 \leq j \leq t$. Moreover, if $p^s = 0$ while $p^{s-1} \neq 0$ in W, and $W \twoheadrightarrow V$ is a surjection, then $V = W/p^t W$.*

(b) *Suppose that*

$$V_0 \twoheadleftarrow V_1 \twoheadleftarrow \cdots \twoheadleftarrow V_n \twoheadleftarrow \cdots$$

is an inverse limit system of coefficient rings and surjective maps, and that the characteristic of V_n is $p^{t(n)}$ where $t(n) \geq 1$. Then either $t(n)$ is eventually constant, in which case the maps $h_n : V_{n+1} \twoheadrightarrow V_n$ are eventually all isomorphisms, and the inverse limit is isomorphic with V_n for any sufficiently large n, or $t(n) \to \infty$ as $n \to \infty$, in which case the inverse limit is a complete local principal ideal domain V with maximal ideal pV and residue class field K. In particular, the inverse limit V is a coefficient ring.

Proof. (a) Every ideal of V (respectively, W) has the form $p^k V$ (respectively, p^W)for a unique integer k, $0 \leq k \leq t$ (respectively, $0 \leq k \leq s$). The first statement follows because $k+j \geq n$ iff $k \geq n-j$. The second statement follows because V must have the form $S/p^k S$ for some k, $0 \leq k \leq S$, and the characteristic of $S/p^k S$ is p^k, which must be equal to p^t.

(b) If $t(n)$ is eventually constant it is clear that all the maps are eventually isomorphisms. Therefore, we may assume that $t(n) \to \infty$ as $n \to \infty$. By passing to an infinite subsequence of the V_n we may assume without loss of generality that $t(n)$ is strictly increasing with n. We may think of an element of the inverse limit as a sequence of elements $v_n \in V_n$ such that v_n is the image of v_{n+1} for every n. It is easy to see that one of the v_n is a unit if and only if all of them are. Suppose on the other hand that none of the v_n is a unit. Then each v_n can be written as pw_n for $w_n \in V_n$. The problem is that while pw_{n+1} maps to pw_n, for all n, it is not necessarily true that w_{n+1} maps to w_n.

Let h_n be the map $V_{n+1} \to V_n$. For all n, let $w'_n = h_n(w_{n+1})$. We will show that for all n, $v_n = pw'_n$ and that $h_n(w'_{n+1}) = w'_n$ for all n. Note first that $h_n(pw_{n+1}) = pw_n = v_n$, and it is also pw'_n. This establishes the first statement. Since $p(w_{n+1} - w'_{n+1}) = 0$, it follows that $w_{n+1} - w'_{n+1} = p^{t(n+1)-1}\delta$, by part (a). Then

$$w'_n = h_n(w_{n+1}) = h_n(w'_{n+1}) + p^{t(n+1)-1}h_n(\delta) = h_n(w'_{n+1}),$$

as required, since $p^{t(n+1)-1}$ is divisible by $p^{t(n)}$, the characteristic of V_n.

It follows that the inverse limit has a unique maximal ideal generated by p. No nonzero element is divisible by arbitrarily high powers of p, since the element will have nonzero image in V_n for some n, and its image in this ring is not divisible by arbitrarily high powers of p. It follows that every nonzero element can be written as a power of p times a unit, and no power of p is 0, because the ring maps onto V_t for arbitrarily large values of t. It is forced to be a principal ideal domain in which every nonzero ideal is generated by a power of p. The fact that the ring arises as an inverse limit implies that it is complete. $\square$

We can now prove:

Theorem (I. S. Cohen). *Every complete local ring (R, m, K) has a coefficient ring. If the residue class field has characteristic $p > 0$, there is a unique coefficient ring containing a given lifting T to R of a p-base Θ for K.*

Proof. We may assume that K has characteristic $p > 0$: we already know that there is a coefficient field if the characteristic of K is 0.

Any coefficient ring for R containing T must map onto a coefficient ring for $R_n = R/m^n$ containing the image of T. Here, there is a unique coefficient ring V_n, which may be described, for any sufficiently large $q = p^N$, as the smallest subring containing all qth powers and the image of T . We may take q large enough that it may be used in the description of coefficient rings V_{n+1} for R_{n+1} and V_n for R_n, and it is then clear that $R_{n+1} \twoheadrightarrow R_n$ induces $V_{n+1} \twoheadrightarrow V_n$. If we construct $V = \varprojlim_n V_n$ and $\varprojlim_n R_n = R$ as sequences of elements $\{r_n\}_n$ such that r_{n+1} maps to r_n for all n, it is clear that

$$V = \varprojlim_n V_n \subseteq \varprojlim_n R_n = R.$$

By part (b) of the preceding Lemma, V is a coefficient ring, and it follows that V is a coefficient ring for R. $\square$