Math 615: Lecture of April 4, 2007

Let $p > 0$ be a prime integer. We now know that a coefficient ring of mixed characteristic p and characteristic p^n, where $n \geq 2$, is determined up to isomorphism by its residue class field. Let K be a given field of characteristic p. We also know that there is a complete mixed characteristic Noetherian discrete valuation ring (V, pV, K) with residue class field K. This implies that V/p^nV is a coefficient ring of characteristic p^n. Hence, as asserted earlier:

Theorem. *A mixed characteristic coefficient ring of characteristc p^n, where $p > 0$ is prime, has the form V/p^nV, where V is a complete Noetherian discrete valuation ring that is a coefficient field.* $\square$

This completes our proof of all of the structure theorems for complete local rings. We restate the following:

Theorem. *Every complete local ring is either a homomorphic image of $K[[x_1, \ldots, x_n]]$, a power series ring over a field K, or of $V[[x_1, \ldots, x_n]]$, a power series ring over a mixed characteristic coefficient ring (V, pV, K) that is a Noetherian discrete valuation ring.*

Both $K[[x_1, \ldots, x_n]]$ and $V[[x_1, \ldots, x_n]]$ are Cohern-Macaulay, as is every regular local ring, since a minimal system of generators for the maximal ideal is a regular sequence. But Cohen-Macaulay rings are universally catemary. Hence:

Corollary. *Every complete local ring is universally catenary.* $\square$

Complete regular local rings are formal power series rings in equal chacteristic, and also in mixed characteristic if unramified. The following is an important tool in working with formal power series rings.

Theorem (Weierstrass preparation theorem). *Let (A, m, K) be a complete local ring and let x be a formal indeterminate over A. Let $f = \sum_{n=0}^{\infty} a_n x^n \in A[[x]]$, where $a_h \in A - m$ is a unit and $a_n \in m$ for $n < h$. (Such an element f is said to be* regular *in x of order h.) Then the images of $1, x, \ldots, x^{h-1}$ are a free basis over A for the ring $A[[x]]/fA[[x]]$, and every element $g \in A[[x]]$ can be written uniquely in the form $qf + r$ where $q \in A[[x]]$, and $r \in A[x]$ is a polynomial of degree $\leq h - 1$.*

Proof. Let $M = A[[x]]/(f)$, which is a finitely generated $A[[x]]$-module, and so will be separated in the $\mathcal{M}$-adic topology, where $\mathcal{M} = (m, x)A[[x]]$. Hence, it is certainly separated in the m-adic topology. Then $M/mM \cong K[[x]]/(\overline{f})$, where $\overline{f}$ is the image of f under the map $A[[x]] \twoheadrightarrow K[[x]]$ induced by $A \twoheadrightarrow K$: it is the result of reducing coefficients of f mod

m. It follows that the lowest nonzero term of $\overline{f}$ has the form cx^h, where $c \in K$, and so $\overline{f} = x^h\gamma$ where γ is a unit in $K[[x]]$. Thus,

$$M/mM \cong K[[x]]/(\overline{f}) = K[[x]]/(x^h),$$

which is a K-vector space for which the images of 1, x, ... , x^{h-1} form a K-basis. By the Proposition on p. 2 of the Lecture Notes of March 23, the elements 1, x, ... , x^{h-1} span $A[[x]]/(f)$ as an A-module. This means precisely that every $g \in A[[x]]$ can be written $g = qf + r$ where $r \in A[x]$ has degree at most $h-1$.

Suppose that $g'f + r'$ is another such representation. Then $r' - r = (q - q')f$. Thus, it will suffice to show if $r = qf$ is a polynomial in x of degree at most $h-1$, then $q = 0$ (and $r = 0$ follows). Suppose otherwise. Since some coefficient of q is not 0, we can choose t such that q is not 0 when considered mod $m^tA[[x]]$. Choose such a t as small as possible, and let d be the least degree such that the coefficient of x^d is not in m^t. Pass to R/m^t. Then q has lowest degree term ax^d, and both a and all higher coefficients are in m^{t-1}, or we could have chosen a smaller value of t. When we multiply by f (still thinking mod m^t), note that all terms of f of degree smaller than h kill q, because their coefficients are in m. There is at most one nonzero term of degree $h + d$, and its coefficient is not zero, because the coefficient of x^h in f is a unit. Thus, qf has a nonzero term of degree $\geq h + d > h - 1$, a contradiction. This completes the proof of the existence and uniqueness of q and r. $\square$

Corollary. *Let $A[[x]]$ and f be as in the statement of the Weierstrass Preparation Theorem, with f regular of order h in x. Then f has a unique multiple fq which is a monic polynomial in $A[x]$ of degree h. The multiplier q is a unit, and qf has all non-leading coefficients in m. The polynomial qf called the* unique monic associate *of f.*

Proof. Apply the Weierstrass Preparation Theorem to $g = x^h$. Then $x^h = qf + r$, which says that $x^h - r = qf$. By the uniqueness part of the theorem, these are the only choices of q, r that satisfy the equation, and so the uniqueness statement follows. It remains only to see that q is a unit, and that r has coefficients in m. To this end, we may work mod $mA[[x]]$. We use $\overline{u}$ for the class of $u \in A[[x]]$ mod $mA[[x]]$, and think of $\overline{u}$ as an element of $K[[x]]$.

Then $x^h - \overline{r} = \overline{q}\overline{f}$. Since $\overline{f}$ is a unit γ times x^h, we must have $\overline{r} = 0$. It follows that $x^h = x^h\overline{q}\gamma$. We may cancel x^h, and so $\overline{q}$ is a unit of of $K[[x]]$. It follows that q is a unit of $A[[x]]$, as asserted. $\square$

Discussion. This result is often applied to the formal power series ring in n variables, $K[[x_1, \ldots, x_n]]$: one may take $A = K[[x_1, \ldots, x_{n-1}]]$ and $x = x_n$, for example, though, obviously, one might make any of the variable play the role of x. In this case, a power series f is regular in x_n if it involves a term of the form cx_n^h with $c \in K - \{0\}$, and if one takes h as small as possible, f is regular of order h in x_n. The regularity of f of order h in x_n is equivalent to the assertion that under the unique continuous $K[[x_n]]$-algebra map $K[[x_1, \ldots, x_n]] \to K[[x_n]]$ that kills $x_1, \ldots, x_{n-1}$, the image of f is a unit times x_n^h. A logical notation for the image of f is $f(0, \ldots, 0, x_n)$. The Weierstrass preparation theorem

asserts that for any g, we can write $f = qg + r$ uniquely, where $q \in K[[x_1, \ldots, x_n]]$, and $r \in K[[x_1, \ldots, x_{n-1}]][x_n]$. In this context, the unique monic associate of f is sometimes call the *distinguished pseudo-polynomial* associated with f. If $K = \mathbb{R}$ or $\mathbb{C}$ one can consider instead the ring of convergent (on a neighborhood of 0) power series. One can carry through the proof of the Weierstrass preparation theorem completely constructively, and show that when g and f are convergent, so are q and r. See, for example, [O. Zariski and P. Samuel, *Commutative Algebra*, Vol. II, D. Van Nostrand Co., Inc., Princeton, 1960], pp. 139–146.

Any nonzero element of the power series ring (convergent or formal) can be made regular in x_n by a change of variables. The same applies to finitely many elements $f_1, \ldots, f_s$, since it suffices to make the product $f_1 \cdots f_s$ regular in x_n, (if the image of $f_1 \cdots f_s$ in $K[[x_n]]$ is nonzero, so is the image of every factor). If the field is infinite one may make use of a K-automorphism that maps $x_1, \ldots, x_n$ to a different basis for $Kx_1 + \cdots + Kx_n$. One can think of f as $f_0 + f_1 + f_2 + \cdots$ where every f_j is a homogeneous polynomial of degree j in $x_1, \ldots, x_n$. Any given form occurring in $f_j \neq 0$ can be made into a monic polynomial by a suitable linear change of variables, by problem **3.** of Problem Set #3 for Math 614, Fall 2003 and its solution.

If K is finite one can still get the image of f under an automorphism to be regular in x_n by mapping $x_1, \ldots, x_n$ to $x_1 + x_n^{N_1}, \ldots, x_{n-1} + x_n^{N_{n-1}}, x_n$, respectively, as in the proof of the Noether normalization theorem, although the details are somewhat more difficult. Consider the monomials that occur in f (there is at least one, since f is not 0), and totally order the monomials so that $x_1^{j_1} \cdots x_n^{j_n} < x_1^{k_1} \cdots x_n^{k_n}$ means that for some i, $1 \leq i \leq n$, $j_1 = k_1$, $j_2 = k_2$, …, $j_{i-1} = k_{i-1}$, while $j_i < k_i$. Let $x_1^{d_1} \cdots x_n^{d_n}$ be the smallest monomial that occurs with nonzero coefficient in f with respect to this ordering, and let $d = \max\{d_1, \ldots, d_n\}$. Let $N_i = (nd)^{n-i}$, and let θ denote the continuous K-automorphism of $K[[x_1, \ldots, x_n]]$ that sends $x_i \mapsto x_i + {x_n}^{N_i}$ for $1 \leq i \leq n-1$, and $x_n \mapsto x_n$. We claim that $\theta(f)$ is regular in x_n. The point is that the value of $\theta(f)$ after killing $x_1, \ldots, x_{n-1}$ is

$$f(x_n^{N_1}, x_n^{N_2}, \ldots, x_n^{N_{n-1}}, x_n),$$

and the term $c'x_1^{e_1} \cdots x_n^{e_n}$ where $c' \in K - \{0\}$ maps to

$$c' x_n^{e_1 N_1 + e_2 N_2 + \cdots + e_{n-1} N_{n-1} + e_n}.$$

In particular, there is a term in the image of $\theta(f)$ coming from the $x_1^{d_1} \cdots x_n^{d_n}$ term in f, and that term is a nonzero scalar multiple of

$$x_n^{d_1 N_1 + d_2 N_2 + \cdots + d_{n-1} N_{n-1} + d_n}.$$

It suffices to show that no other term cancels it, and so it suffices to show that if for some i with $1 \leq i \leq n$, we have that $e_j = d_j$ for $j < i$ and $e_i > d_i$, then

$$e_1 N_1 + e_2 N_2 + \cdots + e_{n-1} N_{n-1} + e_n > d_1 N_1 + d_2 N_2 + \cdots + d_{n-1} N_{n-1} + d_n.$$

Subtracting the right hand side of the inequality above from the left hand side yields

$$(e_i - d_i) N_i + \sum_{j>i} (e_j - d_j) N_j,$$

since $d_j = e_j$ for $j < i$. It will be enough to show that this difference is positive. Since $e_i > d_i$, the leftmost term is at least N_i. Some of the remaining terms are nonnegative, and we omit these. The terms for those j such $e_j < d_j$ are negative, but what is being subtracted is bounded by $d_j N_j \leq dN_j$. Since at most $n-1$ terms are being subtracted, the sum of the quantities being subtracted is strictly bounded by $nd \max_{j>i}\{dN_j\}$. The largest of the N_j is N_{i+1}, which is $(dn)^{n-(i+1)}$. Thus, the total quantity being subtracted is strictly bounded by $(dn)(dn)^{n-i-1} = (dn)^{n-i} = N_i$. This completes the proof that

$$e_1N_1 + e_2N_2 + \cdots + e_{n-1}N_{n-1} + e_n > d_1N_1 + d_2N_2 + \cdots + d_{n-1}N_{n-1} + d_n,$$

and we see that $\theta(f)$ is regular in x_n, as required. $\square$

If the Weierstrass Preparation Theorem is proved directly for a formal or convergent power series ring R over a field K (the constructive proofs do not use *a priori* knowledge that the power series ring is Noetherian), the theorem can be used to prove that the ring R is Noetherian by induction on n. The cases where $n = 0$ or $n = 1$ are obvious: the ring is a field or a discrete valuation ring. Suppose the result is known for the power series ring A in $n-1$ variables, and let R be the power series ring in one variable x_n over A. Let I be an ideal of R. We must show that I is finitely generated over R. If $I = (0)$ this is clear. If $I \neq 0$ choose $f \in I$ with $f \neq 0$. Make a change of variables such that f is regular in x_n over A. Then $I/fR \subseteq R/fR$, which is a finitely generated module over A. By the induction hypothesis, A is Noetherian, and so R/fR is Noetherian over A, and hence I/fR is a Noetherian A-module, and is finitely generated as an A-module. Lift these generators to I. The resulting elements, together with f, give a finite set of generators for I.

Although we shall later give a quite different proof valid for all regular local rings, we want to show how the Weierstrass preparation theorem can be used to prove unique factorization in a formal power series ring.

Theorem. *Let K be a field and let (V, π, K) be a Noetherian discrete valuation ring. $R = K[[x_1, \ldots, x_n]]$ or $V[[x_1, \ldots, x_n]]$ be the formal power series ring in n variables over K or V. Then R is a unique factorization domain.*

Proof. We use induction on n. If $n = 0$ then R is a field or a discrete valuation ring. In the latter case, R is a principal ideal domain and, hence, a unique factorization domain.

Suppose that $n \geq 1$. It suffices to prove that if $f \in m$ is irreducible then f is prime. If π divides f, the f is a multiple of π by a unit, since f is irreducible. We know that π is prime, since $R/(\pi) \cong K[[x_1, \ldots, x_n]]$, a domain. Hence, we may assume that π does not divide f. Suppose that f divides gh, where it may be assumed without loss of generality that $g, h \in m$. Then we have an equation $fw = gh$, and since f is irreducible, we must have that $w \in m$ as well. If some power of π divides w, then π divides g or h. We may factor out π and obtain a similar equation in which a lower power of π divides w. Eventually, we obtain an equation in which π does not divide w: otherwise, w would be in every power of the maximal ideal. Then π does not divide g nor h as well. Hence, π does not divide fgh.

Therefore, by the Discussion on pp. 3 and 4, we can make a change of variables in the formal power series ring such that fgh is regular in x_n modulo π. Since an element of the ring that is a unit modulo π is a unit, we have that fgh is regular in x_n in R as well. Then f, g, and h are all regular in x_n, and we may multiply each by a unit so as to replace it by its unique monic associate: here we view R as $A[[x_n]]$ where $A = K[[x_1, \ldots, x_{n-1}]]$ or $V[[x_1, \ldots, x_{n-1}]]$. Thus, we may assume without loss of generality that f, g, and h are monic polynomials in $A[x_n]$ whose non-leading coefficients are in $Q = (x_1, \ldots, x_{n-1})A$. In the process of replacing f, g, h by their products units, w is replaced by its product with a certain unit as well, so that we still have $fw = gh$. However, *a priori*, w may be a power series in x_n rather than a polynomial.

It is easy, however, to see that $w \in A[x_n]$ as well. We can divide $gh \in A[x_n]$ by f, which is monic in x_n, to get a unique quotient and remainder, say $gh = qf + r$, where the degree of r is less than the degree d of f. The Weierstrass preparation theorem guarantees a unique such representation in $A[[x_n]]$, and in the larger ring we know that $r = 0$. Therefore, the equation $gh = qf$ holds in $A[x_n]$, and this means that $q = w$ is a monic polynomial in x_n as well.

By the induction hypothesis, A is a UFD, and so $A[x_n]$ is a UFD. We first note that f is still irreducible in $A[x_n]$ (this is an issue because it might factor as a polynomial with an invertible constant term in one factor: such a factorization does not contradict irreducibility in $A[[x_n]]$). But if f factors non-trivially $f = f_1 f_2$ in $A[x_n]$, the factors f_1, f_2 must be polynomials in x_n of lower degree which can be taken to be monic. Mod Q, f_1, f_2 give a factorization of x_n^d, and this must be into two powers of x_n of lower degree. Therefore, f_1 and f_2 both have all non-leading coefficients in Q, and, in particular their constant terms are in Q. This implies that neither f_1 nor f_2 is a unit of R, and this contradicts the irreducibility of f in R. Thus, f must be irreducible in $A[x_n]$ as well. But then, in $A[x_n]$ we have that $f \mid g$ or $f \mid h$, and the same obviously holds in the larger ring R, as required. $\square$