Math 615: Lecture of March 26, 2007

The results of the preceding Lecture imply that a complete local ring (R, m) that has a coefficient field K is a homomorphic image of a formal power series ring in n variables over K, where n is the least number of elements needed to generate m. Of course, by Nakayama's Lemma, $n = \dim_K(m/m^2)$. This integer is called the *embedding dimension* of R.

To understand why, consider the analogous situation with finitely generated reduced algebras S over an algebraically closed field K. The ring S corresponds to an affine algebraic set X, whose points are in bijective correspondence with the maximal ideals of S. Giving a surjection $K[X_1, \ldots, X_n] \twoheadrightarrow S$ as K-algebras is equivalent to giving an embedding $X \hookrightarrow \mathbb{A}^n_K$ as a closed algebraic set. The least n for which such an embedding is possible is the smallest dimension of an affine space in which X can be embedded, and it is natural to think of n as the embedding dimension of X, and hence, of S, in this context. The terminology "embedding dimension" for $\dim_K(m/m^2)$ is used even when the local ring (R, m, K) does not contain a field.

The general construction of coefficient fields in positive characteristic

We now discuss the construction of coefficient fields in local rings (R, m, K) of prime characteristic $p > 0$ (these automatically contain the field $\mathbb{Z}/p\mathbb{Z}$) when K need not be perfect. If $q = p^n$ we write
$$K^q = \{c^q : c \in K\},$$
the subfield of K consisting of all elements that are q th powers.

It will be convenient to call a polynomial in several variables *n-special*, where $n \geq 1$ is an integer, if every variable occurs with exponent at most $p^n - 1$ in every term. This terminology is not standard.

Let K be a field of characteristic $p > 0$. Finitely many elements $\theta_1, \ldots, \theta_n$ in K (they will turn out to be, necessarily, in $K - K^p$) are called *p-independent* if the following three equivalent conditions are satisfied:

(1) $[K^p[\theta_1, \ldots, \theta_n] : K^p] = p^n$.

(2) $K^p \subseteq K[\theta_1] \subseteq K^p[\theta_1, \theta_2] \subseteq \cdots \subseteq K^p[\theta_1, \theta_2, \ldots, \theta_n]$ is a strictly increasing tower of fields.

(3) The p^n monomials $\theta_1^{a_1} \cdots \theta_n^{a_n}$ such that $0 \leq a_j \leq p-1$ for all j with $1 \leq j \leq n$ are a K^p-vecctor space basis for K over K^p.

Note that since every θ_j satisfies $\theta_j^p \in K^p$, in the tower considered in part (2) at each stage there are only two possibilities: the degree of θ_{j+1} over $K^p[\theta_1, \ldots, \theta_j]$ is either 1, which means that

$$\theta_{j+1} \in K^p[\theta_1, \dots, \theta_j],$$

or p. Thus, $K[\theta_1, \dots, \theta_n] = p^n$ occurs only when the degree is p at every stage, and this is equivalent to the statement that the tower of fields is strictly increasing. Condition (3) clearly implies condition (1). The fact that (2) $\Rightarrow$ (3) follows by mathematical induction from the observation that

$$1, \theta_{j+1}, \theta_{j+1}^2, \dots, \theta_{j+1}^{p-1}$$

is a basis for $L_{j+1} = K^p[\theta_1, \dots, \theta_{j+1}]$ over $L_j = K[\theta_1, \dots, \theta_j]$ for every j, and the fact that if one has a basis $\mathcal{C}$ for L_{j+1} over L_j and a basis $\mathcal{B}$ for L_j over K^p then all products of an element from $\mathcal{C}$ with an element from $\mathcal{B}$ form a basis for L_{j+1} over K^p.

Every subset of a p-independent set is p-independent. An infinite subset of K is called *p-independent* if every finite subset is p-independent.

A maximal p-independent subset of K, which will necessarily be a subset of $K - K^p$, is called a *p-base* for K. Zorn's Lemma guarantees the existence of a p-base, since the union of a chain of p-independent sets is p-independent. If Θ is a p-base, then $K = K^p[\Theta]$, for if there were an element θ' of $K - K^p[\Theta]$, it could be used to enlarge the p-base. The empty set is a p-base for K if and only if K is perfect. if K is not perfect, a p-base for K is *never* unique: one can change an element of it by adding an element of K^p.

It is easy to see that Θ is a p-base for K if and only if every element of K is uniquely expressible as a polynomial in the elements of Θ with coefficients in K^p such that the exponent on every $\theta \in \Theta$ is at most $p-1$, i.e., the monomials in the elements of Θ of degree at most $p-1$ in each element are a basis for K over K^p. An equivalent statement is that every element of K is uniquely expressible as as 1-special polynomial in the elements of Θ with coefficients in K^p.

If $q = p^n$, then the elements of $\Theta^q = \{\theta^q : \theta \in \Theta\}$ are a p-base for K^q over K^{pq}: in fact we have a commutative diagram:

$$\begin{array}{ccc} K & \xrightarrow{F^q} & K^q \\ \uparrow & & \uparrow \\ K^p & \xrightarrow[F^{pq}]{} & K^{pq} \end{array}$$

where the vertical arrows are inclusions and the horizontal arrows are isomorphisms: here, $F^q(c) = c^q$. In particular, $\Theta^p = \{\theta^p : \theta \in \Theta\}$ is a p-base for K^p, and it follows by multiplying the two bases together that the monomials in the elements of Θ of degree at most $p^2 - 1$ are a basis for K over K^{p^2}. By a straightforward induction, the monomials in the elements of Θ of degree at most $p^n - 1$ in each element are a basis for K over K^{p^n} for every $n \in \mathbb{N}$. An equivalent statement is that every element of K can be written uniquely as an n-special polynomial in the elements of Θ with coefficients in K^{p^n}.

Theorem. *Let (R, m, K) be a complete local ring of positive prime characteristic p, and let Θ be a p-base for K. Let T be a subset of R that maps bijectively onto Θ, i.e., a lifting of the p-base to R. Then there is a unique coefficient field for R that contains T, namely, $K_0 = \bigcap_n R_n$, where $R_n = R^{p^n}[T]$. Thus, there is a bijection between liftings of the p-base Θ and the coefficient fields of R.*

Proof. Note that any coefficient field must contain some lifting of Θ. Observe also that K_0 is clearly a subring of R that contains T. It will suffice to show that K_0 is a coefficient field and that any coefficient field L containing T is contained in K_0. The latter is easy: the isomorphism $L \to K$ takes T to Θ, and so T is a p-base for L. Every element of L is therefore in $L^{p^n}[T] \subseteq R^{p^n}[T]$. Notice also that every element of $R^{p^n}[T]$ can be written as a polynomial in the elements of T of degree at most $p^n - 1$ in each element, i.e., as an n-special polynomial, with coefficients in R^{p^n}. The reason is that any $N \in \mathbb{N}$ can be written as $ap^n + b$ with $a, b \in \mathbb{N}$ and $b \le p^n - 1$. So t^N can be rewritten as $(t^a)^{p^n} t^b$, and, consequently, if t^N occurs in a term we can rewrite that term so that it only involves t^b by absorbing $(t^a)^{p^n}$ into the coefficient from R^{p^n}. Thus, every element of $R^{p^n}[T]$ is represented by an n-special polynomial. Note that n-special polynomials in elements of T with coefficients in R^{p^n} map mod m onto the n-special polynomials in elements of Θ with coefficients in K^{p^n}, which we know give all of K.

We next observe that

$$R^{p^n}[T] \cap m \subseteq m^{p^n}.$$

Write the element of $u \in R^{p^n}[T] \cap m$ as an n-special polynomial in elements of T with coefficients in R^{p^n}. Then its image in K, which is 0, is an n-special polynomial in the elements of Θ with coefficients in K^{p^n}, and so cannot vanish unless every coefficient is 0. This means that each coefficient of the n-special polynomial representing u must have been in $m \cap R^{p^n} \subseteq m^{p^n}$. Thus,

$$K_0 \cap m = \bigcap_n (R^{p^n}[T] \cap m) \subseteq \bigcap_n m^{p^n} = (0).$$

We can therefore conclude that K_0 injects into K. It will suffice to show that $K_0 \to K$ is surjective to complete the proof.

Let $\lambda \in K$ be given. Since $K = K^{p^n}[\Theta]$, for every n we can choose an element of $R^{p^n}[T]$ that maps to λ: call it r_n. Then $r_{n+1} \in R^{p^{n+1}}[T] \subseteq R^{p^n}[T]$, and so $r_n - r_{n+1} \in R^{p^n}[T] \cap m \subseteq m^{p^n}$ (the difference $r_n - r_{n+1}$ is in m because both r_n and r_{n+1} map to λ in K). This shows that $\{r_n\}_n$ is Cauchy, and has a limit r_λ. It is clear that $r_\lambda \equiv \lambda$ mod m, since that is true for every r_n. Moreover, r_λ is independent of the choices of the r_n: given another sequence r'_n with the same property, $r_n - r'_n \in R^{p^n}[T] \cap m \subseteq m^{p^n}$, and so $\{r_n\}_n$ and $\{r'_n\}_n$ have the same limit. This implies that the map $K \to R$ such that $\lambda \mapsto R_\lambda$ is a ring homomorphism: if we have two Cauchy sequences whose terms map to λ and λ' respectively mod K, and whose nth terms are both in $R^{p^n}[T]$ for all n, when we add (respectively, multiply) the Cauchy sequences term by term, we get a Cauchy sequence whose limit is $r_{\lambda+\lambda'}$ (respectively, $r_{\lambda\lambda'}$). Moreover, if $t \in T$ maps to $\theta \in \Theta$ then the Cauchy sequence with constant term t can be used to find r_θ, and so $r_\theta = t$.

It remains only to show that for every n, $r_\lambda \in R^{p^n}[T]$. To see this, write λ as an n-special polynomial in the elements of Θ with coefficients in K^{p^n}. Explicitly,

$$\lambda = \sum_{\mu \in \mathcal{F}} c_\mu^{p^n} \mu$$

where $\mathcal{F}$ is some finite set of n-special monomials in the elements of Θ, and every $c_\mu \in K$. If $\mu = \theta_1^{k_1} \cdots \theta_s^{k_s}$, let $\mu' = t_1^{k_1} \cdots t_s^{k_s}$, where t_j is the element of T that maps to θ_j. Then $r_\mu = \mu'$ and

$$r_\lambda = \sum_{\mu \in \mathcal{F}} r_{c_\mu}^{p^n} \mu' \in R^{p^n}[T]. \qquad \square$$

Remark. The proof is valid for every complete and m-adically separated quasilocal ring (R, m, K) such that R has prime characteristic $p > 0$. We made no use of the fact that R is Noetherian.

Remark. This result shows that if (R, m, K) is a complete local ring that is not a field and K is not perfect, then the choice of a coefficient field is *never* unique. Given a lifting of a p-base T, where $T \neq \emptyset$ because K is not perfect, we can always change it by adding nonzero elements of m to one or more of the elements in the p-base.