Math 711: Lecture of October 12, 2007

Capturing the contracted expansion from an integral extension

Using the result of the first problem in Problem Set #1, we can now prove that tight closure has one of the good properties, namely property (3) on p. 15 of the Lecture Notes from September 5, described in the introduction to the subject in the first lecture.

Recall that if M is a module over a domain D, the *torsion-free rank* of M is

$$\dim_{\mathcal{K}}(\mathcal{K} \otimes_D M).$$

We first note a preliminary result that comes up frequently:

Lemma. *Let D be a domain with fraction field $\mathcal{K}$, and let M be a finitely generated torsion-free module over D. Then M can be embedded in a finitely generated free D-module D^h, where h is the torsion-free rank of M over D. In particular, given any nonzero element $u \in M$, there is a D-linear map $\theta : M \to D$ such that $\theta(u) \neq 0$.*

Proof. We can choose h elements $b_1, \ldots, b_h$ of M that are linearly independent over $\mathcal{K}$ and, hence, over D. This gives an inclusion map

$$Db_1 + \cdots + Db_h = D^h \hookrightarrow M.$$

Let $u_1, \ldots, u_n$ generate M. Then each u_n is a linear combination of $b_1, \ldots, b_h$ over $\mathcal{K}$, and we may multiply by a common denominator $c_i \in D - \{0\}$ to see that $c_i u_i \in D^h \subseteq M$ for $1 \leq i \leq n$. Let $c = c_1 \cdots c_n$. Then $cu_i \in D^h$ for all i, and so $cM \subseteq D^h$. But $M \cong cM$ via the map $u \mapsto cu$, and so we have that $f : M \hookrightarrow D^h$, as required.

If $u \neq 0$, then $f(u) = (d_1, \ldots, d_h)$ has some coordinate not 0, say d_j. Let π_j denote the jth coordinate projection $D^h \to D$. Then we may take $\theta = \pi \circ f$. $\square$

Theorem. *Let R be a Noetherian ring of prime characteristic $p > 0$. Suppose that $R \subseteq S$ is an integral extension, and that I is an ideal of R. Then $IS \cap R \subseteq I^*$.*

Proof. Let $r \in IS \cap R$. It suffices to show that the image of r is in I^* working modulo every minimal prime $\mathfrak{p}$ of R in turn. Let $\mathfrak{q}$ be a prime ideal of S lying over $\mathfrak{p}$: we can choose such a prime $\mathfrak{q}$ by the Lying Over Theorem. Then we have $R/\mathfrak{p} \hookrightarrow S/\mathfrak{q}$, and the image of r in $R/\mathfrak{p}$ is in $I(S/\mathfrak{q})$. We have therefore reduced to the case where R and S are domains.

Since $r \in IS$, if $f_1, \ldots, f_n$ generate I we can write

$$r = s_1 f_1 + \cdots + s_n f_n.$$

1

Hence, we may replace S by $R[f_1, \ldots, f_n] \subseteq SW$, and so assume that S is module-finite over R. By the preceding Lemma, S is solid as an R-algebra, and the result now follows from Problem 1 of Problem Set #1. $\square$

Test elements for reduced algebras essentially of finite type over excellent semilocal rings

Although we have test elements for F-finite rings, we do not yet have a satisfactory theory for excellent local rings. In fact, as indicated in the title of this section, we can do much better. In this section, we want to sketch the method that will enable us to prove the following result:

Theorem. *Let R be a Noetherian ring of prime characteristic $p > 0$. Suppose that R is reduced and essentially of finite type over an excellent semilocal ring B. Then there are elements $c \in R^\circ$ such that R_c is regular, and every such element c has a power that is a completely stable big test element.*

We shall, in fact, prove better results in which the hypotheses on R_c are weakened, but we want to use the Theorem stated to motivate the constructions we need.

The idea of the argument is as follows. We first replace the semilocal ring B by its completion $\widehat{B}$ with respect to its Jacobson radical. Then $R_1 = \widehat{B} \otimes_B R$ is essentially of finite type over $\widehat{B}$, is still reduced, and the map $R \to R_1$ is flat with geometrically regular fibers. It follows that $(R_1)_c$ is still regular. Thus, we have reduced to the case where B is a complete semilocal ring. Such a ring is a finite product of complete local rings, and so is the B-algebra R. The problem can be treated for each factor separately. Therefore, we can assume that B is a complete local ring. Then B is module-finite over a complete regular local ring A, and we henceforth want to think about the case where R is essentially of finite type over a regular local ring (A, m, K). We can choose a coefficient field $K \subseteq A$ such that the composite map $K \hookrightarrow A \twoheadrightarrow A/m$ is an isomorphism. We know from the structure theory of complete local rings that A has the form $K[[x_1, \ldots, x_n]]$, where $x_1, \ldots, x_n$ are formal power series indeterminates over K.

We know that R has the form $W^{-1}R_0$ where R_0 is finitely generated as an A-algebra. It is not hard to see that if $(W^{-1}R_0)_c$ is regular, then there exists $w \in W$ such that $\big((R_0)_w\big)_c$ is regular. If we show that c^N is a completely stable big test element for $(R_0)_w$, this is automatically true for every further localization as well, and so we have it for $W^{-1}R_0 = R$. This enables us to reduce to the case where R is finitely generated over $A = K[[x_1, \ldots, x_n]]$. The key to proving the Theorem above is then the following result.

Theorem. *Let K be a field of characteristic $p > 0$, let (A, m, K) denote the regular local ring $K[[x_1, \ldots, x_n]]$, and let R be a reduced finitely generated A-algebra. Suppose that R_c is regular. Then A has an extension A^Γ such that*

(1) $A \to A^\Gamma$ *is faithfully flat and local.*

(2) A^Γ *is purely inseparable over* A.

(3) *The maximal ideal of* A^Γ *is* mA^Γ.

(4) A^Γ *is F-finite.*

(5) $A^\Gamma \otimes_A R$ *is reduced.*

(6) $(A^\Gamma \otimes_A R)_c$ *is regular.*

It will take quite an effort to prove this. However, once we have this Theorem, the rest of the argument for the Theorem on p. 2 is easy. The point is that $R^\Gamma = A^\Gamma \otimes_A R$ is faithfully flat over R and is F-finite and reduced by (4) and (5) above, Moreover, we still have that $(R^\Gamma)_c$ is regular, by part (6). It follows that c^N is a completely stable big test element for R^Γ by the Theorem at the bottom of p. 4 of the Lecture Notes from October 1, and then we have the corresponding result for R.

This motivates the task of proving the existence of extensions $A \to A^\Gamma$ with properties stated above. The construction depends heavily on the behavior of p-bases for fields of prime characteristic $p > 0$.

Properties of p-bases

We begin by recalling the notion of a p-*base* for a field K of characteristic $p > 0$. As usual, if $q = p^e$ we write

$$K^q = \{c^q : c \in K\},$$

the subfield of K consisting of all elements that are qth powers. It will be convenient to call a polynomial in several variables e-*special*, where $e \geq 1$ is an integer, if every variable occurs with exponent at most $p^e - 1$ in every term. This terminology is *not* standard.

Let K be a field of characteristic $p > 0$. Finitely many elements $\lambda_1, \ldots, \lambda_n$ 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) $[K^p[\lambda_1, \ldots, \lambda_n] : K^p] = p^n$.

(2) $K^p \subseteq K[\lambda_1] \subseteq K^p[\lambda_1, \lambda_2] \subseteq \cdots \subseteq K^p[\lambda_1, \lambda_2, \ldots, \lambda_n]$ is a strictly increasing tower of fields.

(3) The p^n monomials $\lambda_1^{a_1} \cdots \lambda_n^{a_n}$ 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 λ_j satisfies $\lambda_j^p \in K^p$, in the tower considered in part (2) at each stage there are only two possibilities: the degree of λ_{j+1} over $K^p[\lambda_1, \ldots, \lambda_j]$ is either 1, which means that

$$\theta_{j+1} \in K^p[\lambda_1, \ldots, \lambda_j],$$

or p. Thus, $K[\lambda_1, \ldots, \lambda_n] = p^n$ 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

$$1, \lambda_{j+1}, \lambda_{j+1}^2, \ldots, \lambda_{j+1}^{p-1}$$

is a basis for $L_{j+1} = K^p[\lambda_1, \ldots, \lambda_{j+1}]$ over $L_j = K[\lambda_1, \ldots, \lambda_j]$ 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 Λ is a x-base, then $K = K^p[\Lambda]$, 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.

From the condition above, it is easy to see that Λ is a p-base for K if and only if every element of K is uniquely expressible as a polynomial in the elements of Λ with coefficients in K^p such that the exponent on every $\lambda \in \Lambda$ is at most $p - 1$: this is equivalent to the assertion that the monomials in the elements of Λ of degree at most $p - 1$ in each element are a basis for K over K^p. Another equivalent statement is that every element of K is uniquely expressible as as 1-special polynomial in the elements of Λ with coefficients in K^p.

If $q = p^e$, then the elements of $\Lambda^q = \{\lambda^q : \lambda \in \Lambda\}$ 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, $\Lambda^p = \{\lambda^p : \lambda \in \Lambda\}$ is a p-base for K^p, and it follows by multiplying the two bases together that the monomials in the elements of Λ 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 Λ of degree at most $p^e - 1$ in each element are a basis for K over K^{p^e} for every $e \geq 1$. An equivalent statement is that every element of K can be written uniquely as an e-special polynomial in the elements of Λ with coefficients in K^{p^e}.

By taking pth roots, we also have that $K^{1/p} = K[\lambda^{1/p} : \lambda \in \Lambda]$. It is also true that for any h distinct elements $\lambda_1, \ldots, \lambda_h$ of the p-base and for all q, $[K^q[\lambda_1, \ldots, \lambda_h] : K^q] = q^h$ and that $K^{1/q} = K[\lambda^{1/q} : \lambda \in \Lambda]$. It follows that the monomials of the form

$$(*) \quad \lambda_{i_1}^{\alpha_1} \cdots \lambda_{i_h}^{\alpha_h}$$

where every α is a rational number in $[0, 1)$ that can be written with denominator dividing q is a basis for $K^{1/q}$ over K.

Hence, with $K^\infty = \bigcap_q K^{1/q}$, we have

Proposition. *With K a field of prime characteristic $p > 0$ and Λ a p-base as above, the monomials of the form displayed in* $(*)$ *with $\lambda_1, \ldots, \lambda_h \in \Lambda$ and with the denominators of the $\alpha_i \in [0, 1)$ allowed to be arbitrary powers of p form a basis for K^∞ over K.* $\square$

The gamma construction for complete regular local rings

Let K be a fixed field of characteristic $p > 0$ and let Λ be a fixed p-base for K. Let $A = K[[x_1, \ldots, x_n]]$ be a formal power series ring over K. We shall always use Γ to indicate a subset of Λ that is *cofinite*, by which we mean that $\Lambda - \Gamma$ is a finite set. For every such Γ we define a ring A^Γ as follows.

Let K_e (or K_e^Γ if we need to be more precise) denote the field $K[\lambda^{1/q} : \lambda \in \Gamma]$, where $q = p^e$ as usual. Then $K \subseteq K_e \subseteq K^{1/q}$, and the qth power of every element of K_e is in K. We define
$$A^\Gamma = \bigcup_e K_e[[x_1, \ldots, x_n]].$$

We refer to A^Γ as being obtained from A by the *gamma construction*.

Our next objective is to prove the following:

Theorem. *Consider the local ring (A, m, K) obtained from a field K of characteristic $p > 0$ by adjoining n formal power series indeterminiates $x_1, \ldots, x_n$. That is, $A = K[[x_1, \ldots, x_n]]$ and $m = (x_1, \ldots, x_n)A$. Fix a p-base Λ for K, let Γ be a cofinite subset of Λ, and let A^Γ be defined as above. Then $A \hookrightarrow A^\Gamma$ is a flat local homomorphism, and the ring A^Γ is regular local ring of Krull dimension n. Its maximal ideal is mA^Γ and its residue class field is $K^\Gamma = \bigcup_e K_e^\Gamma$. Moreover, A^Γ is purely inseparable over A, and A^Γ is F-finite.*

It will take some work to prove all of this.