Math 711: Lecture of September 21, 2007

F-finite rings

Let R be a Noetherian ring of prime characteristic $p > 0$. R is called *F-finite* if the Frobenius endomorphism $F : R \to R$ makes R into a module-finite R-algebra. This is equivalent to the assertion that R is module-finite over the subring $F(R) = \{r^p : r \in R\}$, which may also be denoted R^p. When R is reduced, this is equivalent to the condition that $R^{1/p}$ is module-finite over R, since in the reduced case the inclusion $R \subseteq R^{1/p}$ is isomorphic to the homomorphism $F : R \to R$.

Proposition. *Let R be a Noetherian ring of prime characteristic $p > 0$.*

(a) *R is F-finite if and only if R_{red} is F-finite.*

(b) *R is F-finite if and only and only if $F^e : R \to R$ is module-finite for all e if and only if $F^e : R \to R$ is module-finite for some $e \geq 1$.*

(c) *If R is F-finite, so is every homomorphic image of R.*

(d) *If R is F-finite so is every localization of R.*

(e) *If R is F-finite, so is every algebra finitely generated over R.*

(f) *If R is F-finite, so is the formal power series ring $R[[x_1, \ldots, x_n]]$.*

(g) *If (R, m, K) is a complete local ring, R is F-finite if and only if the field K is F-finite.*

(h) *If R is F-finite, so is every ring essentially of finite type over R.*

(i) *If K is a field that is finitely generated as a field over a perfect field, then every ring essentially of finite type over K is F-finite.*

Proof. Parts (c) and (d) both follow from the fact that if B is a finite set of generators for R as $F(R)$-module, the image of B in S will generate S over $F(S)$ if $S = R/J$ and also if $S = W^{-1}R$. In the second case, it should be noted that $F(W^{-1}R)$ may be identified with $W^{-1}F(R)$ because localizing at w and a w^p have the same effect.

For part (a), note that if R is F-finite, so is R_{red} by part (c), since $R_{\mathrm{red}} = R/J$, where J is the ideal of all nilpotent elements. Now suppose that I is any ideal of R such that R/I is F-finite. Let the images of $u_1, \ldots, u_n$ span R/I over the image of $(R/I)^p$, and let $v_1, \ldots, v_h$ generate I over R. Let $A = R^p u_1 + \cdots + R^p u_n$. Then $R = A + Rv_1 + \cdots + Rv_h$. If we substitute the same formula for each copy of R occuring in an Rv_j term on the right, we find thtat

$$R = A + \sum_{i,j} R^p u_i v_j + \sum_{j,j'} R v'_j v_j.$$

It follows that the $n+nh$ elements u_i and u_iv_j span R/I^2 over the image of $(R/I^2)^p$. Thus, (R/I^2) is F-finite. By a straightforward induction, R/I^{2^k} is F-finite for all k. Hence if $I = J$ is the ideal of nilpotents, we see that R itself is F-finite.

For part (b), note that if $F : R \to R$ is F-finite, so is the e-fold composition. On the other hand, if $F^e : R \to R$ is finite, so is $F^e : S \to S$, where $S = R_{\mathrm{red}}$. Then we have $S \subseteq S^{1/p} \subseteq S^{1/q}$, and since $S^{1/q}$ is a Noetherian S-module, so is $S^{1/p}$. Thus, S is F-finite, and so is R by part (a).

To prove (e), it suffices to consider the case of a polynomial ring in a finite number of variables over R, and, by induction it suffices to consider the case where $S = R[x]$. Likewise, for part (f) we need only show that $R[[x]]$ is F-finite. Let $u_1, \ldots, u_n$ span R over R^p. Then, in both cases, the elements u_ix^j, $1 \le i \le n$, $1 \le j \le p-1$, span S over $S^p = R^p[x^p]$ (respectively, $R^p[[x^p]]$).

For (g), note that $K = R/m$, so that if (R, m, K) is F-finite, so is K. If R is complete it is a homomorphic image of a formal power series ring $K[[x_1, \ldots, x_n]]$, where K is the residue class field of R. By part (f), if K is F-finite, so is R.

Part (h) is immediate from parts (e) and (d). For part (i) first note that K itself is essentially of finite type over a perfect field, and a perfect field is obviously F-finite. The final statement is then immediate from part (h). $\square$

A proof of the following result of Ernst Kunz would take us far afield. We refer the reader to [E. Kunz, *On Noetherian rings of characteristic* p, Amer. J. Math. **98** (1976) 999–1013].

Theorem (Kunz). *Every F-finite ring is excellent.*

We are aiming to prove the following result about F-finite rings:

Theorem (existence of test elements). *Let R be a reduced F-finite ring, and let $c \in R^\circ$ be such that R_c is regular. Then c has a power c^N that is a completely stable big test element.*

This is terrifically useful. Elements $c \in R^\circ$ such that R_c is regular always exist. In any excellent ring,

$$\{P \in \mathrm{Spec}\,(R) : R_P \text{ is regular}\}$$

is open. Since the complement is closed, there is an ideal I such that

$$\mathcal{V}(I) = \{P \in \mathrm{Spec}\,(R) : R_P \text{ is not regular}\}.$$

We refer to this set of primes as the *singular locus* of $\mathrm{Spec}\,(R)$ or of R. Note that if R is reduced, we cannot have $I \subseteq \mathfrak{p}$ for any minimal prime $\mathfrak{p}$ of R, because that would mean the $R_\mathfrak{p}$ is not regular, and $R_\mathfrak{p}$ is a field. Hence, I is not contained in the union of the minimal primes of R, which means that I meets R°. If $c \in I \cap R^\circ$, then R_c is regular: primes that do not contain c cannot contain I. Hence, in a reduced F-finite (or any reduced excellent) ring, there is always an element $r \in R^\circ$ such that R_c is regular, and this means that Theorem above can be applied. Hence:

Corollary. *Every reduced F-finite ring has a completely stable big test element.*

It will take some time before we can prove the Theorem on existence of test elements. Our approach requires studying the notion of a *strongly F-regular* ring. We give the definition below. However, we first want to comment on the notion of an *F-split* ring.

Definition: F-split rings. Let R be a ring of prime characteristic $p > 0$. We shall say that R is *F-split* if, under the map $F : R \to R$, the left hand copy of R is a direct summand of the right hand copy of R.

If R is F-split, $F : R \to R$ must be injective. This is equivalent to the condition that R be reduced. An equivalent condition is therefore that R be reduced and that R be a direct summand of $R^{1/p}$ as an R-module, i.e., there exists an R-linear map $\theta : R^{1/p} \to 1$ such that $\theta(1) = 1$.

Proposition. *Let R be a reduced ring of prime characteristic $p > 0$. The following conditions are equivalent:*

(1) *R is F-split.*

(2) *$R \to R^{1/q}$ splits as a map of R-modules for all q.*

(3) *$R \to R^{1/q}$ splits as a map of R-modules for at least one value of $q > 1$.*

Proof. (1) $\Rightarrow$ (2). Let $\theta : R^{1/p} \to R$ be a splitting. Then for all $q = p^e > 1$, if $q' = p^{e-1}$, we may define a splitting $\theta_e : R^{1/q} \to R^{1/q'}$ by

$$\theta_e(r^{1/q}) = \big(\theta(r^{1/p})\big)^{1/q'}.$$

Thus, the diagram:

$$\begin{tikzcd} R^{1/q} \arrow[r, "\theta_e"] & R^{1/q'} \\ R^{1/p} \arrow[u, "\cong"] \arrow[r, "\theta"] & R \arrow[u, "\cong"] \end{tikzcd}$$

commutes, where the vertical arrows are the isomorphisms $r^{1/p} \mapsto r^{1/q}$ and $r \mapsto r^{1/q'}$, respectively. Of course, $\theta_1 = \theta$. Then θ_e is $R^{1/q'}$-linear and, in particular, R-linear. Hence, the composite map

$$\theta_1 \circ \theta_2 \circ \cdots \circ \theta_e : R^{1/q} \to R$$

gives the required splitting.

(2) $\Rightarrow$ (3) is clear. Finally, assume (3). Then $R \subseteq R^{1/p} \subseteq R^{1/q}$, so that a splitting $R^{1/q} \to R$ may simply be restricted to $R^{1/p}$, and (1) follows. $\square$

Strongly F-regular rings

We have defined a ring to be weakly F-regular if every ideal is tightly closed, and to be F-regular if all of its localizations have this property as well. We next want to introduce the notion of a *strongly F-regular ring* R: for the moment, we make this definition only when R is F-finite.

The definition is rather technical, but this condition turns out to be easier to work with than the other notions. It implies that every submodule of every module is tightly closed, it passes to localizations automatically, and it leads to a proof of the Theorem on existence of test elements stated on p. 2.

Of course, the value of this notion rests on whether there are examples of strongly F-regular rings. We shall soon see that every regular F-finite ring is strongly F-regular. Let $1 \leq t \leq r \leq s$ be integers. If K is an algebraically closed field (or an F-finite field), and X is an $r \times s$ matrix of indeterminates over K, then the ring obtained from the polynomial ring $K[X]$ in the entries of X by killing the ideal $I_t(X)$ generated by the $t \times t$ minors of X is strongly F-regular, and so is the ring generated over K by the $r \times r$ minors of X (this is the homogeneous coordinate ring of a Grassman variety). The normal rings generated by finitely many monomials in indeterminates are also strongly F-regular. Thus, there are many important examples.

In fact, in the F-finite case, every ring that is known to be weakly F-regular is known to be strongly F-regular.

Conjecture. *Every weakly F-regular F-finite ring is strongly F-regular.*

This is a very important open question. It is known to be true in many cases: we shall discuss what is known at a later point.

Definition: strong F-regularity. Let R be a Noetherian ring of prime characteristic $p > 0$, and suppose that R is reduced and F-finite. We define R to be *strongly F-regular* if for every $c \in R^\circ$ there exists q_c such that the map $R \to R^{1/q_c}$ that sends $1 \mapsto c^{1/q_c}$ splits over R. That is, for all $c \in R^\circ$ there exist q_c and an R-linear map $\theta : R^{1/q_c} \to R$ such that $\theta(c^{1/q_c}) = 1$.

The element q_c will usually depend on c. For example, one will typically need to make a larger choice for c^p than for c.

Remark. The following elementary fact is very useful. Let $h : R \to S$ be a ring homomorphism and let M be any S-module. Let u be any element of M. Suppose that the unique R-linear map $R \to M$ such that $1 \mapsto u$ (and $r \mapsto ru$) splits over R. Then R is a direct summand of S, i.e., there is an R-module splitting for $h : R \to S$. In fact, if $\theta : M \to R$ is R-linear and $\theta(u) = 1$, we get the required splitting by defining $\phi(s) = \theta(su)$ for all $s \in S$. Note also that the fact that $R \to M$ splits is equivalent to the assertion that $R \to Ru$

such that $1 \mapsto u$ is an isomorphism of R-modules, together with the assertion that Ru is a direct summand of M as an R-module.

We may apply this remark to the case where $S = R^{1/q_c}$ in the above definition. Thus:

Proposition. *A strongly F-regular ring R is F-split.*

We also note:

Proposition. *Suppose that R is a reduced Noetherian ring of prime characteristic $p > 0$, that $c \in R^\circ$, and that $R \to R^{1/q_c}$ sending $1 \mapsto c^{1/q_c}$ splits over R. Then for all $q \geq q_c$, the map $R \to R^{1/q}$ sending $1 \mapsto c^{1/q}$ splits over R.*

Proof. It suffices to show that if we have a splitting for a certain q, we also get a splitting for the next higher value of q, which is qp. Suppose that $\theta : R^{1/q} \to R$ is R-linear and $\theta(c^{1/q}) = 1$. We define $\theta' : R^{1/pq} \to R^{1/p}$ by the rule

$$\theta'(r^{1/pq}) = \big(\theta(r^{1/q})\big)^{1/p}.$$

That is, the diagram

$$\begin{array}{ccc} R^{1/pq} & \xrightarrow{\theta'} & R^{1/p} \\ \cong\uparrow & & \cong\uparrow \\ R^{1/q} & \xrightarrow{\theta} & R \end{array}$$

commutes. Then θ' is $R^{1/p}$-linear and $\theta'(c^{1/pq}) = 1 \in R^{1/p}$. By the Remark beginning on the bottom of p. 4, $R \to R^{1/q}$ splits, and so R is F-split, i.e., we have an R-linear map $\beta : R^{1/p} \to R$ such that $\beta(1) = 1$. Then $\beta \circ \theta'$ is the required splitting. $\square$

The following fact is now remarkably easy to prove.

Theorem. *Let R be a strongly F-regular ring. Then for every inclusion of $N \subseteq M$ of modules (these are not required to be finitely generated), N is tightly closed in M.*

Proof. We may map a free module G onto M and replace N by its inverse image $H \subseteq G$. Thus, it suffices to show that $H = H^*_G$ when G is free. Suppose that $u \in H^*_G$. We want to prove that $u \in H$. Since $u \in H^*_G$, for all $q \gg 0$, $cu^q \in H^{[q]}$. Choose q_c such that $R \to R^{1/q_c}$ with $1 \mapsto c^{1/q_c}$ splits. Then fix $q \geq q_c$ such that $cu^q \in H^{[q]}$. Then the map $R \to R^{1/q}$ sending $1 \to c^{1/q}$ also splits, and we can choose $\theta : R^{1/q} \to R$ such that $\theta(c^{1/q}) = 1$.

The fact that $cu^q \in H^{[q]}$ gives an equation

$$cu^q = \sum_{i=1}^{n} r_i h_i^q$$

with the $r_i \in R$ and the $h_i \in H$. We work in $R^{1/q} \otimes_R G$ and take qth roots to obtain

$$(*) \quad c^{1/q}u = \sum_{i=1}^{n} r_i^{1/q} h_i.$$

We have adopted the notation $r^{1/q}g$ for $r^{1/q} \otimes g$. By tensoring with G, from the R-linear map $\theta : R^{1/q} \to R$ we get an R-linear map $\theta' : R^{1/q} \otimes G \to G$ such that $\theta'(r^{1/q}g) = \theta(r^{1/q})g$ for all $g \in G$. We may now apply θ' to $(*)$ to obtain

$$u = 1 \cdot u = \theta(c^{1/q})u = \sum_{i=1}^{n} \theta(r_i^{1/q}) h_i.$$

Since every $\theta(r_i^{1/q}) \in R$, the right hand side is in H, i.e., $u \in H$. $\square$

Corollary. *A strongly F-regular ring is weakly F-regular and, in particular, normal.* $\square$