SOME FINITENESS PROPERTIES OF LYUBEZNIK'S F-MODULES

by Melvin Hochster

1. INTRODUCTION

Throughout this paper all rings are commutative, associative with multiplicative identity. Ring homomorphisms are assumed to preserve the multiplicative identity and modules are assumed unital.

Beginning with the work of Peskine and Szpiro [PS], and continuing in [HaSp], [Sh], [HuSh], and [Ly], the Frobenius endomorphism has been a critical tool in exploring the properties of local cohomology modules over Noetherian rings of characteristic p. This led to the penetrating study of $\mathcal{F}$-finite $\mathcal{F}$-modules by G. Lybeznik in [Ly], and it is the properties of Lybeznik's $\mathcal{F}$-modules that are the focus of this paper. We note that the results developed here are applied to the study of local cohomology in [EH].

We shall be considering, almost exclusively, Noetherian regular rings R of prime characteristic $p > 0$, and, henceforth, unless otherwise specified, we assume that given rings are Noetherian regular of prime characteristic $p > 0$, although we usually repeat this hypothesis in statements of theorems. Over any Noetherian ring R of positive prime characteristic $p > 0$ we shall let $\mathcal{F}$ or $\mathcal{F}_R$ denote the Frobenius functor from R-modules to R-modules, and $\mathcal{F}^e$ or $\mathcal{F}_R^e$ its eth iteration: we discuss these notions further in the next paragraph.

Here, if S is any R-algebra, say with structural homomorphism $h\colon R \to S$, we get a functor B_S from R-modules to S-modules, base change to S, by applying $S \otimes_R \_$, which preserves finite generation, preserves freeness, projectiveness, and flatness of modules, and

The author was supported in part by National Science Foundation Grant DMS–0400633.

June 21, 2007.

takes the R-module which is the cokernel of the matrix (r_{ij}) to the R-module which is the cokernel of the matrix $(h(r_{ij}))$. The functor $\mathcal{F}_R^e$ arises when $S = R$ but is viewed as an R-algebra via the e th power F^e of the Frobenius endomorphism $F : R \to R$, where $F(r) = r^p$ and $F^e(r) = r^{p^e}$. In general, with base change functors there is a map $M \to S \otimes_R M$ that sends u to $1 \otimes u$. In the case of $\mathcal{F}_R^e$ we denote the image of $u \in M$ under this map by u^{p^e}. Note that $\mathcal{F}^e$ takes the cokernel of the matrix (a_{ij}) to the cokernel of the matrix $(a_{ij}^{p^e})$.

When R is regular of prime characteristic $p > 0$, the functors $\mathcal{F}^e$ are all exact, i.e., $F^e : R \to R$ makes R into a flat (in fact, faithfully flat) R-algebra.

By an $\mathcal{F}$-module $\mathcal{M}$ over such a regular ring R of prime characteristic $p > 0$ we mean, following Lyubeznik [Ly], an R-module $\mathcal{M}$ together with an R-module isomorphism $\theta : M \cong \mathcal{F}(\mathcal{M})$: θ is called the *structural homomorphism* of M, and we often write θ_M for it, particularly when we are discussing structural homomoprhisms for several $\mathcal{F}_R$-modules.

If M is any R-module and $\beta : M \to F(M)$, one may obtain an $\mathcal{F}$-module from β by defining

$$\mathcal{M} = \varinjlim{}_e \big(M \xrightarrow{\beta} \mathcal{F}(M) \xrightarrow{\mathcal{F}(\beta)} \mathcal{F}^2(M) \xrightarrow{\mathcal{F}^2(\beta)} \mathcal{F}^3(M) \xrightarrow{\mathcal{F}^3(\beta)} \cdots\big).$$

Since $\otimes$ commutes with direct limits, we have that

$$\mathcal{F}(\mathcal{M}) \cong \varinjlim{}_e \big(\mathcal{F}(M) \xrightarrow{F(\beta)} \mathcal{F}^2(M) \xrightarrow{\mathcal{F}^2(\beta)} \mathcal{F}^3(M) \xrightarrow{\mathcal{F}^3(\beta)} \mathcal{F}^4(M) \xrightarrow{\mathcal{F}^4(\beta)} \cdots\big).$$

and since this is the same as the original direct limit system with the first term omitted, we have an isomorphism of $\mathcal{M} \cong \mathcal{F}(\mathcal{M})$ as R-modules. We shall refer to $\mathcal{M}$ as the $\mathcal{F}$-module *$\mathcal{F}$-generated* by β. If β is an injective map then the exactness of $\mathcal{F}$ implies that all the maps in the direct limit system are injective, so that M injects into $\mathcal{M}$. In this case we refer to β as a *root morphism* for $\mathcal{M}$, and M as a *root* for $\mathcal{M}$. If $\mathcal{M}$ is an $\mathcal{F}$-module possessing a root morphism $\beta : M \to \mathcal{F}(M)$ with M finitely generated over R, we say that $\mathcal{M}$ is *$\mathcal{F}$-finite*.

By a morphism (or $\mathcal{F}$-morphism or $\mathcal{F}_R$-morphism) of $\mathcal{F}$-modules $\mathcal{M} \to \mathcal{N}$ we mean an R-linear map $h : \mathcal{M} \to \mathcal{N}$ such that the diagram

$$\begin{array}{ccc} \mathcal{M} & \xrightarrow{h} & \mathcal{N} \\ {\scriptstyle \theta_{\mathcal{M}}}\downarrow & & \downarrow{\scriptstyle \theta_{\mathcal{N}}} \\ \mathcal{F}(\mathcal{M}) & \xrightarrow[\mathcal{F}(h)]{} & \mathcal{F}(\mathcal{N}) \end{array}$$

commutes. Then $\mathcal{F}_R$-modules form an abelian category, and the forgetful functor to R-modules preserves kernels, cokernels, images, and direct sums and products. We may think of an $\mathcal{F}_R$-submodule of an $\mathcal{F}_R$-module $\mathcal{M}$ with structural homomorphism θ as an R-submodule $\mathcal{N}$ of $\mathcal{M}$ such that the restriction of θ maps $\mathcal{N}$ isomorphically onto $\mathcal{F}(\mathcal{N}) \subseteq \mathcal{F}(\mathcal{M})$. We shall write $\mathrm{Hom}_{\mathcal{F}_R}(\mathcal{M}, \mathcal{N})$ for the abelian group of $\mathcal{F}_R$-morphisms from $\mathcal{M}$ to $\mathcal{N}$: the subscript R may be omitted.

Lyubeznik shows in [Ly] that an $\mathcal{F}$-finite $\mathcal{F}$-module $\mathcal{M}$ has ACC for its $\mathcal{F}$-submodules, and that if R is finitely generated over a regular local ring, then $\mathcal{M}$ has DCC as well, and so has finite length.

Our main result is as follows:

Theorem. *Let R be a Noetherian regular ring of prime characteristic $p > 0$ and let $\mathcal{M}$ and $\mathcal{N}$ be $\mathcal{F}_R$-finite $\mathcal{F}_R$-modules.*

(a) $\mathrm{Hom}_{\mathcal{F}_R}(\mathcal{M}, \mathcal{N})$ *is a finite dimensional $\mathbb{Z}/p\mathbb{Z}$-vector space, and, hence, is a finite set.*

(b) $\mathrm{Hom}_{\mathcal{F}_R}(\mathcal{M}, \mathcal{M})$ *is a finite ring, and hence each element is algebraic over $\mathbb{Z}/p\mathbb{Z}$. If $\mathcal{M}$ is simple as an $\mathcal{F}_R$-module, then* $\mathrm{Hom}_{\mathcal{F}_R}(\mathcal{M}, \mathcal{M})$ *is a commutative field.*

(c) *If $\mathcal{M}$ has DCC, which is automatic if R is finitely generated as an algebra over a regular local ring, then the set of $\mathcal{F}_R$-submodules of $\mathcal{M}$ is finite.*

This theorem is proved in §5, after an analysis of the case where the ring is a separably closed field in §4. See Theorem (5.1) and Corollary (5.2).

We shall also show in §3 that the category of $\mathcal{F}_R$-modules has enough injectives.

The next section summarizes some results that we shall need from [Ly].

2. SOME RESULTS OF LYUBEZNIK ON $\mathcal{F}$-MODULES

We collect here for convenient reference some results from [Ly] that we shall need to refer to later. The proofs are all given by appropriate references to [Ly].

(2.1) Proposition. *Every $\mathcal{F}_R$-finite $\mathcal{F}_R$-module has a root morphism $\beta : M \in \mathcal{F}_R(M)$, where M is finitely generated. Moreover, if $\mathcal{N} \subseteq \mathcal{M}$ is an $\mathcal{F}_R$-submodule of $\mathcal{M}$, then the restriction β_0 of β to $N = \mathcal{N} \cap M$ maps N into $\mathcal{F}_R(N)$, and is a root morphism for $\mathcal{N}$. In fact, there is a bijection between the $\mathcal{F}_R$-submodules of $\mathcal{M}$ and the R-submodules N of M such that $N = M \cap \mathcal{F}_R(N)$ ($\mathcal{F}_R(N) \subseteq \mathcal{F}_R(\mathcal{M})$, which may be identified with $\mathcal{M}$ using θ^{-1}, and then we take the intersection with $M \subseteq \mathcal{M}$).*

Proof. Cf. [Ly], Prop. (2.5), Cor. (2.6), and (1.10f). □

(2.2) Theorem. *Let R be a regular Noetherian ring of positive prime characteristic $p > 0$ and let I be an ideal of R that such that R/I is again regular. Then there is a category equivalence between the category of $\mathcal{F}_{R/I}$-modules and the full subcategory of $\mathcal{F}_R$-modules consisting of those modules in which every elements is killed by a power of I.*

Proof. Cf. [Ly], Prop. (3.1). □

(2.3) Theorem. *The $\mathcal{F}_R$-submodules of an $\mathcal{F}_R$-finite $\mathcal{F}_R$-module $\mathcal{M}$ satisfy the ascending chain condition. Moreover, if R is a regular ring finitely generated as an algebra over a regular local ring and $\mathcal{M}$ is $\mathcal{F}_R$-finite as an $\mathcal{F}_R$-module, then its $\mathcal{F}_R$-submodules satisfy the descending chain condition as well, which means that $\mathcal{M}$ has finite length, i.e., it has a finite filtration by $\mathcal{F}_R$-submodules such that all the factors are simple as $\mathcal{F}_R$-modules.*

Proof. Cf. [Ly], Theorem (3.2). □

(2.4) Theorem. *If $R \to S$ is a homomorphism of regular Noetherian rings of prime characteristic $p > 0$ and if $\mathcal{M}$ is an $\mathcal{F}_R$-module, then $S \otimes_R M$ is an $\mathcal{F}_S$-module in an obvious way (if $\theta : \mathcal{M} \cong \mathcal{F}_R(M)$, then $\mathbf{1}_S \otimes_R \theta : S \otimes_R \mathcal{M} \cong S \otimes_R \mathcal{F}_R(\mathcal{M})$, and the latter may be identified with $\mathcal{F}_S(S \otimes_R \mathcal{M})$): in particular, this holds when $S = W^{-1}R$ is a localization of R. Moreover, if $\mathcal{M}$ is $\mathcal{F}_R$-finite, then $S \otimes_R \mathcal{M}$ is $\mathcal{F}_S$-finite.*

Proof. Cf. [Ly], Def.-Prop. (1.3) and Prop. (2.9a). □

(2.5) Theorem. *If $\mathcal{M}$ is an $\mathcal{F}_R$-module and $W \subseteq R$ is a multiplicative system, then $W^{-1}\mathcal{M}$ is an $\mathcal{F}_R$-module. If W is generated by one element f and M is $\mathcal{F}_R$-finite then $\mathcal{M}_f$ is $\mathcal{F}_R$-finite. Moreover, every $\mathcal{F}_{R_f}$-finite $\mathcal{F}_{R_f}$-module is $\mathcal{F}_R$-finite when viewed as an $\mathcal{F}_R$-module via restriction of scalars.*

Proof. Cf. [Ly], Def.-Prop. (1.3b) and Prop. (2.9b) □

(2.6) Theorem. *The $\mathcal{F}_R$-finite $\mathcal{F}_R$-modules form a full abelian subcategory of the category of $\mathcal{F}_R$-submodules which is closed under formation of submodules, quotient modules, and extensions. Every $\mathcal{F}_R$-finite $\mathcal{F}_R$-module has ACC in the category of $\mathcal{F}_R$-modules.*

Proof. Cf. [Ly], Prop. (2.7) and Theorem (2.8). □

(2.7) Theorem. *If $\mathcal{M}$ is $\mathcal{F}_R$-finite and I is an ideal of R then $H^j_I(\mathcal{M})$ has the structure of an $\mathcal{F}_R$-finite $\mathcal{F}_R$-module for all j.*

Proof. Cf. [Ly], Example (1.2b), Prop. (1.8), and Prop. (2.10). □

(2.8) Remark. If I is generated up to radicals by $(f_1, \ldots, f_n)$ then the modules $H^I_I(M)$ may be calculated as the cohomology of the complex:

$$0 \to M \to \bigoplus_j M_{f_j} \to \cdots \to \bigoplus_{1 \le j_1 < \cdots < j_t \le n} M_{f_{j_1} \cdots f_{j_t}} \cdots \to M_{f_1 \cdots f_n} \to 0$$

obtained by tensoring together, over R, the n complexes $0 \to M \to M_{f_j} \to 0$. Theorem (2.7) can then be proved using Theorems (2.5) and (2.6) above, if one knows that the induced $\mathcal{F}_R$-module structure on the cohomology of this complex is the correct one: this issue is addressed in Prop. (1.8) of [Ly].

(2.9) Theorem. *If $\mathcal{M}$ is $\mathcal{F}_R$-finite then* $\operatorname{Ass} \mathcal{M}$ *is finite, and all the Bass numbers of $\mathcal{M}$ are finite. If $\mathcal{M}$ is a simple $\mathcal{F}_R$-module then it has a unique associated prime.*

Proof. Cf. [Ly], Theorems (2.11) and (2.12). □

(2.10) Theorem. *If $\mathcal{M}$ is an $\mathcal{F}_R$-module then* $\operatorname{id}_R \mathcal{M} \le \operatorname{dim} \operatorname{Supp} \mathcal{M}$. *In particular, if* $\operatorname{dim} \operatorname{Supp} \mathcal{M} = 0$, *then $\mathcal{M}$ is injective.*

Proof. Cf. [Ly], Theorem (1.4). □

3. EXISTENCE OF ENOUGH INJECTIVES

(3.1) Theorem. *The category of $\mathcal{F}_R$-modules over a Noetherian regular ring R of prime characteristic $p > 0$ has enough injectives, i.e., every $\mathcal{F}_R$-module can be embedded in an injective $\mathcal{F}_R$-module.*

We postpone the proof until we have established several lemmas.

(3.2) Lemma. *Every finite subset of the $\mathcal{F}_R$-module $\mathcal{M}$ is contained in a countably generated $\mathcal{F}_R$-submodule of $\mathcal{M}$.*

Proof. Let θ be the structural isomorphism of $\mathcal{M}$ with $\mathcal{F}(\mathcal{M})$. Call the finite set of elements S_1. We construct a non-decreasing sequence of finite sets S_i recursively as follows. For

each element u of S_i we can write $\theta(u)$ as a finite R-linear combination of elements v_j^p of $\mathcal{F}(\mathcal{M})$, and we enlarge S_i to a finite set S_{i+1} that contains all the v_j and also every $\theta^{-1}(u^p)$. Let N_i be the R-span of the set S_i. By the construction, $\mathcal{F}(N_i) \subseteq \theta(N_{i+1})$ and $\theta(N_i) \subseteq \mathcal{F}(N_{i+1})$. It follows that if $\mathcal{N}$ is the union of the N_i, then $\mathcal{F}(\mathcal{N}) \subseteq \theta(\mathcal{N})$ and $\theta(\mathcal{N}) \subseteq \mathcal{F}(\mathcal{N})$. Thus, $\mathcal{F}(\mathcal{N}) = \theta(\mathcal{N})$, and θ restricts to an isomorphism of $\mathcal{N}$ with $\mathcal{F}(\mathcal{N})$, as required. □

(3.3) Corollary. *Every countably generated submodule of the $\mathcal{F}_R$-module $\mathcal{M}$ is contained in a countably generated $\mathcal{F}_R$-submodule of $\mathcal{M}$.*

Proof. Take a sequence of generators for the submodule and let $\mathcal{N}_i$ be a countably generated $\mathcal{F}$-submodule containing the first i generators for each i. Then the sum of the $\mathcal{N}_i$ is the required subdmodule. □

Note that over a Noetherian ring R, every submodule A of a countably generated R-module B is countably generated (B is a countable union of finitely generated R-modules, the intersection of A with each of these is finitely generated, and A is the union of these interesections).

(3.4) Lemma. *There is a set W of pairs $(\mathcal{A}, \mathcal{B})$ where $\mathcal{A} \subseteq \mathcal{B}$ are countably generated $\mathcal{F}$-modules over R such that every inclusion of a countably generated $\mathcal{F}$-module over R in a countably generated $\mathcal{F}$-module is isomorphic with one of the inclusions $\mathcal{A} \subseteq \mathcal{B}$.*

Proof. Choose a set D whose cardinality is the same as the free R-module on a countably infinite set of generators. Then every countably generated R-module has the same cardinality as some subset of D. The set G of all $\mathcal{F}$-modules whose underlying set is a subset of D contains a representative of the isomorphism class of every countably generated $\mathcal{F}$-module over R. The set of all pairs $(\mathcal{A}, \mathcal{B})$ where $\mathcal{B}$ is in G and $\mathcal{A}$ is an $\mathcal{F}$-submodule of $\mathcal{B}$ satisfies the condition. □

(3.5) Lemma. *Given an $\mathcal{F}_R$-module $\mathcal{M}$, there is an embedding $\mathcal{M} \to \mathcal{M}'$ of $\mathcal{F}_R$-modules such that if A is any countably generated $\mathcal{F}_R$-submodule of $\mathcal{M}$ and $\mathcal{A} \to \mathcal{B}$ is an injective map of countably generated $\mathcal{F}_R$-modules, the composite map $\mathcal{A} \to \mathcal{M} \to \mathcal{M}'$ extends to a map $\mathcal{B} \to \mathcal{M}'$.*

Proof. Let W be as in Lemma (3.4). Consider the set of triples $\tau = (A_\tau, B_\tau, f_\tau)$ such that $(A_\tau, B_\tau) \in W$ and f_τ is an injection of A_τ into M. Then we may form the direct

sum $\mathcal{M}'' = M \oplus \bigoplus_\tau B_\tau$ and within it kill all elements of the form $f_\tau(a) \oplus a$ where $a \in A_\tau \subseteq B_\tau$. Call the quotient $\mathcal{M}'$. One can easily check that $\mathcal{M}'$ is an $\mathcal{F}_R$-module, not just an R-module, and that $\mathcal{M}$ injects into it, as does every B_τ, with its submodule A_τ identified with $f(A_\tau) \subseteq M$. It is then clear that $\mathcal{M}'$ has the required property. □

Proof of Theorem (3.1). Given an $\mathcal{F}_R$-module $\mathcal{N}$ we use transfinite induction to construct a direct limit system of $\mathcal{F}_R$-modules and injective maps thereof indexed by the first uncountable ordinal. The first module in the system is $\mathcal{N}$. At limit ordinals we take a direct limit. At the ordinal λ we construct $N_{\lambda+1}$ so that if $M = N_\lambda$ then $N_{\lambda+1}$ has the property of $\mathcal{M}'$ described in Lemma (3.5) above. The direct limit $\mathcal{E}$ of this system will be an injective $\mathcal{F}$-module containing the given module $\mathcal{N}$.

To see that $\mathcal{E}$ is injective we proceed as follows. Consider a map from an $\mathcal{F}_R$-submodule $\mathcal{H}$ of an $\mathcal{F}_R$-module $\mathcal{L}$ to $\mathcal{E}$. We may work modulo the kernel and assume the map is injective. We want to show that it extends to $\mathcal{L}$. By Zorn's lemma we may extend it maximally, and so assume that it cannot be extended further at all. Then if $\mathcal{L}/\mathcal{H}$ is not zero we may choose a countably generated $\mathcal{F}_R$-submodule $\mathcal{B}$ of $\mathcal{L}$ containing an element not in $\mathcal{H}$. We get a contradiction by extending the map from $\mathcal{H}$ to $\mathcal{H} + \mathcal{B}$, and to do so it suffices to extend the map from $\mathcal{A} = \mathcal{H} \cap \mathcal{B}$ to $\mathcal{B}$. (Recall that over a Noetherian ring R, every submodule of a countably generated module is countably generated.) Consider a sequence of generators of $\mathcal{A}$. By the construction of $\mathcal{E}$ the images of these lie in a sequence of modules in the direct limit system used to construct $\mathcal{E}$, and hence in a single specific module $\mathcal{N}_\lambda$ from the system. But then the map extends to $\mathcal{N}_{\lambda+1} \subseteq \mathcal{E}$, as required. □

4. SEPARABLY CLOSED FIELDS

(4.1) Lemma. *Let A be an invertible $n \times n$ matrix over a ring R of prime characteristic $p > 0$, let $x_1, \ldots, x_n$ be indeterminates over R, let X be the $n \times 1$ column vector having the x_i as its entries, let $F(X)$ denote the $n \times 1$ column vector having the elements x_i^p as its entries, and let I be the ideal of R generated by the entries of $AX - F(X)$. Let $S = R[x_1, \ldots, x_n]/I$. Then S is module-finite and free over R of rank p^n, and S is étale over R.*

If $R = K$ is a separably closed field, the matrix equation $AX = F(X)$ has precisely p^n solutions for X in K^n, and all solutions in L^n, where L is an algebraic closure of K, actually lie in K^n. These solutions form a vector space of dimension n over $\mathbb{Z}/p\mathbb{Z}$.

Proof. The fact that S is module-finite and free of rank p^n over R follows from Lemma (2.1a) on p. 51 of [HH]. That S is étale over R follows because the Jacobian matrix of the given presentation for S over R will be precisely the invertible matrix A: the partial derivative of x_i^p with respect to any of the variables is 0.

Now suppose that $R = K$ is a separably closed field. Then the étale extension given by S must be a product of copies of separable extensions of K, each of which must be K, and the number of factors in this product must be p^n. Thus, S is precisely the product of p^n copies of K. Let π_t be the projection map on the t th copy. Then the images of the x_i under $\pi_t : S \to K$ give a solution of the equations $AX = F(X)$. Also, any solution of the equations in an algebraic closure L of K gives rise to a maximal ideal of S, and so must be identical to one of the solutions given by the π_i. It follows that all solutions of the equations in L actually lie in K, and so there are p^n solutions in L and in K. The sum of two solutions is clearly a solution, from which it follows that the solutions form a vector space over $\mathbb{Z}/p\mathbb{Z}$. Since there are a total of p^n solutions, the dimension of this vector space must be n. $\square$

For part (b) in the result below, note the closely related Lemma (1.14) in [HaSp], and references in that paper.

(4.2) Theorem. *Let K be a field of characteristic $p > 0$. Let $\mathcal{M}$ and $\mathcal{N}$ be $\mathcal{F}_K$-finite $\mathcal{F}_K$-modules.*

(a) *$\mathcal{M}$ must be a finite-dimensional K-vector space.*

(b) *Let K be separably closed. If $\mathcal{M} = V$ has dimension n over K and structural morphism θ, then the set of vectors $u \in V$ is such that $\theta(u) = u^p$ is a $\mathbb{Z}/p\mathbb{Z}$-vector subspace of V of dimension n, and this subspace spans V over K.*

(c) *If K is separably closed, then every $\mathcal{F}_K$-finite $\mathcal{F}_K$-module is isomorphic with a finite direct sum of copies of K with the standard $\mathcal{F}_K$-module structure (where θ sends the identity element in K to the identity element in $\mathcal{F}_K(K) = K$).*

(d) *If K is given the standard $\mathcal{F}_K$-module structure then for any $\mathcal{F}_K$-module $\mathcal{M}$ with structural homomorphism θ, $\mathrm{Hom}_{\mathcal{F}_K}(K, \mathcal{M}) \cong \{u \in \mathcal{M} : \theta(u) = u^p\}$.*

(e) *If K is separably closed then $\mathrm{Ext}^1_{\mathcal{F}_K}(\mathcal{M}, \mathcal{N}) = 0$, where the Ext is computed in the ablelian category of $\mathcal{F}_K$-modules.*

(f) *$\mathrm{Hom}_{\mathcal{F}_K}(\mathcal{M}, \mathcal{N})$ is a vector space over $\mathbb{Z}/p\mathbb{Z}$ whose dimension is at most the product of the dimensions of $\mathcal{M}$ and $\mathcal{N}$ over K, with equality if K is separably closed.*

Proof. (a) A root of an $\mathcal{F}_K$-finite $\mathcal{F}_K$-module must be a finite-dimensional vector space V over K, and a monomorphsim $\beta : V \to \mathcal{F}(V)$ must be an isomorphism, since $\mathcal{F}(V)$ has the same dimension as a K-vector space that V does. This means that V itself is already the $\mathcal{F}$-module generated by the root morphism β, and β is actually the structural morphism.

To prove part (b) suppose that V is an $\mathcal{F}_K$-finite $\mathcal{F}_K$-module, where K is separably closed. Choose a basis $v_1, \ldots, v_n$ for V and consider the basis $v_1^p, \ldots, v_n^p$ for $F(V)$. The isomorphism $\theta : V \to \mathcal{F}(V)$ has an $n \times n$ matrix A with respect to this pair of bases. We now apply Lemma (4.1). Corresponding to each of the p^n solutions $(c_1, \ldots, c_n)$ of the system $AX = F(X)$ in K^n there is an element $u = \sum_{t=1}^n c_t v_t \in V$. The fact that the elements c_t give a solution of the equations says precisely that $\theta(u) = u^p$, so that, conversely, any element $u \in V$ such that $\theta(u) = u^p$ corresponds to a solution of the equations. It follows that the set T of such u is a $\mathbb{Z}/p\mathbb{Z}$-subsapce of V of dimension n. Let W be the K-subspace of V spanned by T. Then θ maps T onto $F(T)$ clearly, so that $T \subseteq V$ is an $\mathcal{F}_K$-submodule of V. But then, unless $\dim_K T = n$, it cannot contain p^n vectors u such that $\theta(u) = u^p$, a contradiction unless $T = V$.

Part (c) is now immediate: given any $\mathcal{F}_K$-finite $\mathcal{F}_K$-module V over the separably closed field K of dimension n over K, we can choose a basis for T (with notation as in the preceding paragraph) over $\mathbb{Z}/p\mathbb{Z}$, say $u_1, \ldots, u_n$, and then the u_i must be a basis for V, since T spans V and both dimensions are n. Each u_i is such that $\theta(u_i) = u_i^p$. But this shows that V is the direct sum as an $\mathcal{F}_K$-module of the n $\mathcal{F}_K$-submodules Ku_i, each of which is one-dimensional over K, and each of which is isomorphic as an $\mathcal{F}_K$-module to K with the trivial $\mathcal{F}_K$-module structure.

Any element of

$$\phi \in \mathrm{Hom}_{\mathcal{F}_K}(K, \mathcal{M})$$

is determined by the image of 1, and the isomorphism stated in part (d) arises by sending ϕ to $\phi(1) \in \mathcal{M}$: the condition that $\theta(u) = u^p$ is precisely what is needed for the map ϕ that sends 1 to u to be an $\mathcal{F}_K$-morphism.

To prove part (e), we observe that since we may use the Yoneda characterization of Ext it suffices to show that if one has a short exact sequence of $\mathcal{F}_K$-finite $\mathcal{F}_K$- modules $0 \to \mathcal{N} \to \mathcal{Q} \to \mathcal{M} \to 0$ then it is split. Call the K-vector space dimensions of these modules m, $m + n$, and n. Then one has an exact sequence

$$0 \to \mathrm{Hom}_{\mathcal{F}_K}(K, \mathcal{N}) \to \mathrm{Hom}_{\mathcal{F}_K}(K, \mathcal{Q}) \to \mathrm{Hom}_{\mathcal{F}_K}(K, \mathcal{M})$$

and by parts (b) and (d) these are $\mathbb{Z}/p\mathbb{Z}$-vector spaces of dimensions n, $n + m$ and m, respetively, from which it follows that the rightmost map is onto and the displayed sequence

is a short exact sequence of vector spaces over $\mathbb{Z}/p\mathbb{Z}$. Thus, we may choose a $\mathbb{Z}/p\mathbb{Z}$-basis $u_1, \ldots, u_n, v_1, \ldots, v_m$ for $\mathrm{Hom}_{\mathcal{F}_K}(K, \mathcal{Q})$ such that $u_1, \ldots, u_n$ is the image of a $\mathbb{Z}/p\mathbb{Z}$-basis for $\mathrm{Hom}_{\mathcal{F}_K}(K, \mathcal{N})$ and the image of $v_1, \ldots, v_m$ in $\mathrm{Hom}_{\mathcal{F}_K}(K, \mathcal{M})$ is a $\mathbb{Z}/p\mathbb{Z}$-basis. As in the proof of part (c), we have that the K-span of the u_i is an $\mathcal{F}_K$-submodule of $\mathcal{Q}$ and is the image of $\mathcal{N}$, while the the K-span $\mathcal{M}'$ of the v_j is an $\mathcal{F}_K$-submodule of $\mathcal{Q}$ that is mapped isomorphically onto $\mathcal{M}$: moreover, $\mathcal{Q}$ is the direct sum of the image of $\mathcal{N}$ and $\mathcal{M}'$ as an $\mathcal{F}_K$-module. Thus, the short exact sequence is split, and we have established part (e).

Part (f) follows because the Hom over K may be embeded in the Hom one obtains after applying $L \otimes_K \_$ for a separable closure L of K, and in the separably closed case we may assume that $\mathcal{M}$ is a finite direct sum of copies of K with the standard $\mathcal{F}_K$-module structure and the result reduces to the case where $\mathcal{F}_K$ is one of these copies of K. But then it is immediate from parts (b) and (d). $\square$

5. FINITENESS OF $\mathrm{Hom}_{\mathcal{F}_R}(\mathcal{M},\mathcal{N})$ WHEN $\mathcal{M}$, $\mathcal{N}$ ARE $\mathcal{F}$-FINITE

(5.1) Theorem. *Let R be a Noetherian regular ring of prime characteristic $p > 0$. Let $\mathcal{M}$ and $\mathcal{N}$ be $\mathcal{F}_R$-finite $\mathcal{F}_R$-modules. Then $\mathrm{Hom}_{\mathcal{F}_R}(\mathcal{M},\mathcal{N})$ is a finite-dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$ and, hence, is a finite set.*

Proof. By Noetherian induction on $\mathcal{N}$, we may assume the result when $\mathcal{N}$ is replaced by a proper quotient in the category of $\mathcal{F}$-modules. Choose P maximal among the associated primes of $\mathcal{N}$, and let $N_0 = H^0_P(N)$. By the long exact sequence for $\mathrm{Hom}_{\mathcal{F}_R}$ and the fact that the result holds (by the Noetherian induction hypothesis) for $N/H^0_P(N)$, we may reduce to the case where N has a unique associated prime P. Then there a map from $\mathrm{Hom}_{\mathcal{F}_R}(\mathcal{M},\mathcal{N}) \to \mathrm{Hom}_{\mathcal{F}_{R_P}}(\mathcal{M}_P,\mathcal{N}_P)$ that takes f to f_P, and it is injective (if f takes on a nonzero value then so does f_P, since $\mathcal{N}$ injects into $\mathcal{N}_P$). Thus, we may assume that R is local. But then the $\mathcal{F}_R$-modules have finite length, and so have finite filtrations with simple factors, and repeated use of the long exact sequence enables us to reduce to the case where the modules are both simple. Any map between them is then either 0 or an endomorphism. Thus, we may assume that the two modules are isomorphic simple modules. They have the same unique associated prime, and we may localize again, if necessary, and assume that the ring is local and that both simple modules are supported only at the maximal ideal. The category of $\mathcal{F}_R$-modules supported only at the maximal ideal m is equivalent to the category of $\mathcal{F}_R$-modules over R/m in such a way that $\mathcal{F}$-finiteness is preserved. We have now reduced to the case of a field, which was done in §4. $\square$

(5.2) Corollary. *Let R be a Noetherian regular ring of prime characteristic $p > 0$. Let $\mathcal{M}$ be an $\mathcal{F}$-finite $\mathcal{F}$-module over R.*

(a) *Every endomorphism of $\mathcal{M}$ is algebraic over $\mathbb{Z}/pZ$.*

(b) *If $\mathcal{M}$ has DCC as an $\mathcal{F}$-module (which is automatic if R is an affine algebra over a regular local ring), then $\mathcal{M}$ has only finitely many $\mathcal{F}$-submodules.*

(c) *If $\mathcal{M}$ is simple, its endomorphisms as an $\mathcal{F}$-module form a finite field.*

Proof. (a) The endomorphisms of any $\mathcal{F}$-finite module are algebraic over $\mathbb{Z}/p\mathbb{Z}$, since the entire ring of such endomorphisms is a finite-dimensional algebra over $\mathbb{Z}/p\mathbb{Z}$. This may be viewed as an analogue of a fact that holds for D-modules over $K[[x_1, \ldots, x_n]]$ when K is a field of characteristic zero.

(b) Let $\mathcal{M}$ be such a module which is a counterexample. Since its $\mathcal{F}$-submodules have ACC, we may replace it, if necessary, by an $\mathcal{F}$-module quotient which is a counterexample, but all of whose proper quotients have only finitely many submodules. Thus, we are using Noetherian induction. This quotient still has DCC, and, hence, finite length. Let $\mathcal{N}_i$ be the finite set of simple modules occurring in a finite filtration of M by such. Then any simple submodule of $\mathcal{M}$ is isomorphic to one of the $\mathcal{N}_i$. Since each $\mathrm{Hom}_{\mathcal{F}}(\mathcal{N}_i, \mathcal{M})$ is finite, there are only finitely many submodules of M isomorphic to a given $\mathcal{N}_i$, and hence $\mathcal{M}$ has only finitely many submodules that are simple. Every nonzero submodule contains at least one of these, and since there are only finitely many submodules in the quotient by any one of these, by the Noetherian induction hypothesis, we are done.

(c) The endomorphisms form a division ring, because any nonzero endomorphism is automatically an automorphism. But it is well known that a finite division ring must be a field. □

Bibliography

[EH] F. Enescu and M. Hochster, *The Frobenius structure of local cohomology*, preprint.

[HaSp] R. Hartshorne and R. Speiser, *Local cohomological dimension in characteristic p*, Annals of Math. **105** (1977), 45–79.

[HH] M. Hochster and C. Huneke, *Infinite integral extensions and big Cohen-Macaulay algebras*, Annals of Math. **135** (1992), 53–89.

[HuSh] C. Huneke and R. Sharp, *Bass numbers of local cohomology modules*, Trans. Amer. Math. Soc. **339**, 765–779.

[Ly] G. Lyubeznik, *F-moudules: applications to local cohomology and D-modules in characteristic $p > 0$*, J. reine angew. Math. **491** (1997), 65-130.

[PS] C. Peskine and L. Szpiro, *Dimension projective finie et cohomologie locale*, Inst. Hautes tudes Sci. Publ. Math. No. **42** (1973), 47–119.

[Sh] R. Sharp, *The Frobenius homomorphism and local cohomology in regular local rings of positive characteristic*, J. Pure Appl. Algebra **71** (1991), 313–317.

Department of Mathematics
University of Michigan
Ann Arbor, MI 48109–1043 USA
E-mail:
hochster@umich.edu