715: Lecture of October 21, 2002

We continue with the list of basic facts about Hilbert-Kunz functions begun last time.

(4) There are positive real constants c_1 and c_2 such that for all e, $c_1 q^d \leq \mathrm{HK}_{M,I}(e) \leq c_2 q^d$, where $d = \dim M$. The point is that if I is generated by r elements, then $I^{qr} \subseteq I^{[q]} \subseteq I^q$, and $\ell(M/I^n M)$ is given by a polynomial of degree d in n for $n \gg 0$, from which the stated result follows (this follows from the theory of Hilbert functions as presented, for example, in the book of Atiyah-McDonald or in my 614 lecture notes).

Note that when R is complete and K is algebraically closed, R is F-finite. If M is an R-module we use ${}^e M$ to denote M viewed as an R-module by restriction of scalars, where the map $R \to R$ used is F^e. Thus, if $m \in^e M$, we have that $r \cdot m = r^{p^e} m$. In the F-finite case, ${}^e M$ is again a finitely generated R-module. Note also that restriction of scalars is an exact functor. Furthermore, $({}^{e_0}M)/(I^{[q]}({}^{e_0}M)) \cong {}^{e_0}(M/I^{[qp^{e_0}]}M)$. When K is perfect, a finite length module N over R has the same length as ${}^e N$. It follows that:

(5) Over a complete local ring with perfect residue field, $HK_{{}^{e_0}M,I}(e) = HK_{M,I}(e+e_0)$. I

Therefore, if Monsky's theorem holds for ${}^{e_0}M$ for some e_0, it holds for M.
(6) Suppose that M contains a submodule N of smaller dimension. Let $M' = M/N$. Then $|\mathrm{HK}_{M,I}(e) - \mathrm{HK}_{M',I}(e)| = \mathrm{O}(q^{d-1})$.

The reason is that the exact sequence $0 \to N \to M \to M' \to 0$ yields an exact sequence $\cdots \to N/I^{[q]}N \to M/I^{[q]}M \to M'/I^{[q]}M' \to 0$ for all q, which implies that

$$\ell(M'/I^{[q]}M') \leq \ell(M/I^{[q]}M) \leq \ell(M'/I^{[q]}M') + \ell(N/I^{[q]}N) = \ell(M'/I^{[q]}M') + \mathrm{O}(q^{d-1})$$

by (4) above, from which the result follows.

Note that if M has two submodules N_1, N_2 of smaller dimension then their sum N_1+N_2, which is a homomorphic image of $N_1 \oplus N_2$, also has smaller dimension. It follows that a maximal submodule N of smaller dimension is actually a maximum submodule of smaller dimension, and that M/N will then have pure dimension equal to the dimension of M.

Proof of Monsky's theorem. We have already reduced to the case where R is complete with perfect residue field. If M has a submodule N of smaller dimension, we can kill a maximum such submodule without affecting whether the result holds. Thus, we may assume that all associated primes P of M are such that $\dim R/P = d = \dim M$. In particular, there are no embedded primes. Any element which has a power in $\mathrm{Ann}M$ kills ${}^{e_0}M$ for sufficiently large e_0. By applying this fact to each of finitely many generators for the radical of $\mathrm{Ann}M$, we can choose e_0 so large that the annihilator of ${}^{e_0}M$ is precisely the radical of $\mathrm{Ann}M$. Therefore, by (5), we may assume that $\mathrm{Ann}M$ is a radical ideal. By (1) we may replace R by $R/\mathrm{Ann}_R M$. Thus, we may assume that R is reduced, that all minimal P are such that

$\dim R/P = \dim M = d$, and that the minimal primes of R are the same as the associated primes of M.

Let W be the multiplicative system of nonzerodivisors in R, which are also nonzerodivisors on M. Then $W^{-1}R$ is a product of fields, and $W^{-1}M$ is a product of modules over these fields, each of which is a finite-dimensional vector space. Thus, $W^{-1}M$ is a direct sum of copies of modules $W^{-1}(R/P)$ (this is the fraction field of R/P for varying minimal primes P of R). Let $u_1, \ldots, u_h$ be the generators of the copies of the various R/P. Consider the images of a finite set of generators for M in $W^{-1}(\sum_i Ru_i)$. Then there will be a single element $w \in W$ such that the image of M is contained in $\sum R(w^{-1})u_i$. Thus, M embeds in a direct sum M' of prime cyclic modules R/P in such a way that the cokernel is killed by an element of W, say by $v \in W$. Then $M' \cong vM' \subseteq M$ and $vM \subseteq vM'$. This leads to short exact sequences $0 \to M \to M' \to N \to 0$ and $0 \to M' \to MtoN' \to 0$, where $\dim N$ and $\dim N'$ are both $\leq d-1$. Applying $R/I^{[q]} \otimes_R \_$, we get an exact sequence $\cdots \to M/I^{[q]}M \to M'/I^{[q]}M' \to N/I^{[q]}N \to 0$, which shows that $\ell(M'/I^{[q]}M') \leq \ell(M/I^{[q]}M) + \ell(N/I^{[q]}N)$, which shows $\ell(M'/I^{[q]}M') - \ell(M/I^{[q]}M)$ is bounded by Cq^{d-1} for some $C > 0$. The second short exact sequence shows that $\ell(M/I^{[q]}M) - \ell(M'/I^{[q]}M')$ is bounded by $C'q^{d-1}$ for some $C' > 0$. This shows that theorem holds for M if and only if it holds for M'. Thus, we have reduce to considering a direct sum of prime cyclic modules. This obviously comes down to the case of a single prime cyclic module, which is proved in the second lemma below. $\square$

Lemma. *Let R be a complete local domain of dimension d with perfect residue class field. Then the torsion free rank of ${}^eR \cong R^{1/q}$ as an R-module is q^d.*