Hilbert Functions

We recall that an $\mathbb{N}$-graded ring R is Noetherian iff R_0 is Noetherian and R is finitely generated over R_0. (The sufficiency of the condition is clear. Now suppose that R is Noetherian. Since R_0 is a homomorphic image of R, obtained by killing the ideal J spanned by all forms of positive degree, it is clear that R_0 is Noetherian. Let $S \subseteq R$ be the R_0-subalgebra of R generated by a finite set of homogeneous generators $G_1, \ldots, G_h$ of J (if R is Noetherian, J is finitely generated). Then $S = R$: otherwise, there is a form F in $R - R_0$ of least degree not in S: since it is in J, it can be expressed as a linear combination of those G_i of degree at most $d = \deg(F)$ with homogeneous coefficients of strictly smaller degree than d, and then the coefficients are in S, which implies $F \in S$.

This means that we may write R as the homomorphic image of $R_0[x_1, \ldots, x_n]$ for some n, where the polynomial ring is graded so that x_i has degree $d_i > 0$. In this situation R_t is the R_0-free module on the monomials $x_1^{a_1} \cdots x_n^{a_n}$ such that $\sum_{i=1}^n a_i d_i = t$. Since all the a_i are at most t, there are only finitely many such monomials, so that every R_t is a finitely generated R_0-module. Thus, since a Noetherian $\mathbb{N}$-graded ring R is a homomorphic of such a graded polynomial ring, all homogeneous components R_t of such a ring R are finitely generated R_0-modules. Moreover, given a finitely generated graded module M over R with homogeneous generators $u_1, \ldots, u_s$ of degrees $d_1, \ldots, d_s$,

$$M_n = \sum_{j=1}^{s} R_{n-d_j} u_j,$$

and since every R_{n-d_j} is a finitely generated R_0-module, every M_n is a finitely generated R_0-module.

The polynomial ring $R_0[x_1, \ldots, x_n]$ also has an $\mathbb{N}^n$-grading: if we let $h = (h_1, \ldots, h_n) \in \mathbb{N}^h$, then

$$[R]_h = R_0 x_1^{a_1} \cdots x_n^{a_n}$$

where $a_i d_i = h_i$, $1 \leq i \leq n$, or 0 if for some i, d_i does not divide h_i. The usual $\mathbb{N}$-grading on a polynomial ring is obtained when all the d_i are specified to be 1.

An $\mathbb{N}$-graded Noetherian A-algebra R is called *standard* if $A = R_0$ and it is generated over R_0 by R_1, in which case it is a homomorphic image of some $A[x_1, \ldots, x_n]$ with the usual grading. The kernel of the surjection $A[x_1, \ldots, x_n] \twoheadrightarrow R$ is a homogeneous ideal.

The *associated graded ring* of R with respect to I, denoted $\mathrm{gr}_I R$, is the $\mathbb{N}$-graded ring such that

$$[\mathrm{gr}_I(R)]_n = I^n / I^{n+1},$$

with multiplication defined by the rule $[i_h][i_k] = [i_h i_k]$, where $i_h \in I^h$, $i_k \in I^k$, and $[i_h]$, $[i_k]$, and $[i_h i_k]$ represent elements of I^h/I^{h+1}, I^k/I^{k+1}, and I^{h+k}/I^{h+k+1}, respectively. It is easy to see that if one alters i_h by adding an element of I^{h+1}, the class of $i_h i_k$ mod I^{h+k+1}

does not change since $i_h i_k$ is altered by adding an element of I^{h+k+1}. The same remark applies if one changes i_k by adding an element of I_{k+1}. It follows that multiplication on these classes is well-defined, and it extends to the whole ring by forcing the distributive law. This ring is generated over R/I by the classes $[i] \in I/I^2$, $i \in I$, and if $i_1, \ldots, i_s$ generate I then $[i_1], \ldots, [i_s]$, thought of in I/I^2, generate $\operatorname{gr}_I R$ over R/I. Thus, $\operatorname{gr}_I R$ is a standard graded R/I-algebra, finitely generated as an R/I-algebra whenever I is finitely generated as an ideal of R. In particular, if R is a Noetherian ring, $\operatorname{gr}_I R$ is a standard Noetherian (R/I)-algebra for every ideal I.

The associated graded ring can also be obtained from the *second Rees ring*, which is defined as $R[It,\, 1/t] \subseteq R[t,\, 1/t]$. More explicitly,

$$R[It,\, 1/t] = \cdots + R\frac{1}{t^2} + R\frac{1}{t} + R + It + I^2t^2 + \cdots .$$

This ring is a $\mathbb{Z}$-graded R-algebra. Let $v = 1/t$. Notice that v is not a unit in $S = R[It, 1/t]$ (unless $I = R$). In fact S/vS is $\mathbb{Z}$-graded: the negative graded components vanish, and the n th nonnegative graded component is $I^n t^n / I^{n+1} t^n \cong I^n/I^{n+1}$, since $I^{n+1}t^{n+1}v = I^{n+1}t^n$. Thus, S/vS may also be thought of as $\mathbb{N}$-graded, and, in fact, $R[It,\, v]/(v) \cong \operatorname{gr}_I R$.

Suppose that R contains a field of K. One may think of $R[It,\, v]$ as giving rise to a family of rings parametrized by K, obtained by killing $v - \lambda$ as λ varies in K. For values of $\lambda \neq 0$, the quotient ring is R, while for $\lambda = 0$, the quotient is $\operatorname{gr}_I R$.

If $\{M_n\}_n$ is an I-stable filtration of an R-module M, then there is an *associated graded module* $\bigoplus_n M_n/M_{n+1}$, which is easily checked to be a $\operatorname{gr}_I R$-module with multiplication determined by the rule $[i_h][m_k] = [i_h m_k]$ for $i_h \in I^h R$ and $m_k \in M_k$, where $[i_h]$, $[m_k]$, and $[i_h m_k]$ are interpreted in I^h/I^{h+1}, M_k/M_{k+1}, and M_{h+k}/M_{h+k+1}, respectively. If $M_{n+c} = I^n M_c$ for $n \in \mathbb{N}$, then this associated graded module is generated by its graded components with indices $\leq c$, namely M/M_1, M_1/M_2, $\ldots$, M_c/M_{c+1}. Thus, if R and M are Noetherian it is a finitely generated $\mathbb{N}$-graded $\operatorname{gr}_I(R)$-module, and is Noetherian. If the filtration is the I-adic filtration, one writes $\operatorname{gr}_I M$ for the associated graded module.

When we refer to a *graded ring* without specifying H, it is understood that $H = \mathbb{N}$. However, when we refer to a graded module M over a graded ring R, our convention is that M is $\mathbb{Z}$-graded. If M is finitely generated, it will have finitely many homogeneous generators: if the least degree among these is $a \in \mathbb{Z}$, then all homogeneous elements of M have degree $\geq a$, so that the n th graded component M_n of M will be nonzero for only finitely many negative values of n. When M is $\mathbb{Z}$-graded it is convenient to have a notation for the same module with its grading shifted. We write $M(t)$ for M graded so that $M(t)_n = M_{t+n}$. For example, $R(t)$ is a free R-module with a homogeneous free generator in degree $-t$: note that $R(t)_{-t} = R_0$ and so contains $1 \in R$.

Let M be a finitely generated graded module over a graded algebra R over $R_0 = A$ where A is an Artin local ring. We define the *Hilbert function* $\operatorname{Hilb}_M(n)$ of M by the rule $\operatorname{Hilb}_M(n) = \ell_A(M_n)$ for all $n \in \mathbb{Z}$, and we define the *Poincaré series* $P_M(t)$ of M by the formula $P_M(t) = \sum_{n=-\infty}^{\infty} \operatorname{Hilb}_M(n) t^n \in \mathbb{Z}[[t]]$. Note that $\ell(M_n)$ is finite for all $n \in \mathbb{Z}$, because each M_n is finitely generated as an A-module, by the discussion of the

first paragraph. If A has a coefficient field, lengths over A are the same as vector space dimensions over its coefficient field. Technically, it is necessary to specify A in describing length. For example, $\ell_{\mathbb{C}}(\mathbb{C}) = 1$, while $\ell_{\mathbb{R}}(\mathbb{C}) = 2$. However, it is usually clear from context over which ring lengths are being taken, and then the ring is omitted from the notation.

Note that $Z[t] \subseteq Z[[t]]$, and that elements of the set of polynomials W with constant ± 1 are invertible. We view $W^{-1}Z[t] \subseteq Z[[t]]$, and so it makes sense to say that a power series in $\mathbb{Z}[[t]]$ is in $W^{-1}\mathbb{Z}[t]$.

Example. Suppose that $R = K[x_1, \ldots, x_d]$ the standard graded polynomial ring. Here, $A = K$ and length over K is the same as vector space dimension. The length of the vector space R_n is the same as the number of monomials $x_1^{k_1} \cdots x_d^{k_d}$ of degree n in the variables $x_1, \ldots, x_d$, since these form a K-vector space basis for R_n. This is the same as the number of d-tuples of nonnegative integers whose sum is n. We can count these as follows: form a string of k_1 dots, then a slash, then a string of k_2 dots, then another slash, and so forth, finishing with a string of k_d dots. For example, $x_1^3 x_2^2 x_4^5$ would correspond to

$$\cdots / \cdot\cdot // \cdot\cdot\cdot\cdot .$$

The result is a string of dots and slashes in which the total number of dots is $k_1 + \cdots + k_d = n$ and the number of slashes is $d - 1$. There is a bijection between such strings and the monomials that we want to count. The string has total length $k + d - 1$, and is determined by the choice of the $d - 1$ spots where the slashes go. Therefore, the number of monomials is $\binom{n+d-1}{d-1}$. The Hilbert function of the polynomial ring is given by the rule $\mathrm{Hilb}_R(n) = 0$ if $n < 0$ and

$$\mathrm{Hilb}_R(n) = \binom{n+d-1}{d-1}$$

if $n \geq 0$. Note that, in this case, the Hilbert function agrees with a polynomial in n of degree $d - 1 = \dim(R) - 1$ for all $n \gg 0$. This gives one formula for the Poincaré series, namely

$$\sum_{n=0}^{\infty} \binom{n+d-1}{d-1} t^n.$$

We give a different way of obtaining the Poincaré series. Consider the formal power series in $Z[[x_1, \ldots, x_d]]$ which is the sum of all monomials in the x_i:

$$1 + x_1 + \cdots + x_d + x_1^2 + x_1 x_2 + \cdots + x_d^2 + \cdots$$

This makes sense because there are only finitely many monomials of any given degree. It is easy to check that this power series is the product of the series

$$1 + x_j + x_j^2 + \cdots + x_j^n + \cdots$$

as j varies from 1 to d: in distributing terms of the product in all possible ways, one gets every monomial in the x_j exactly once. This leads to the formula

$$1 + x_1 + \cdots + x_d + x_1^2 + x_1 x_2 + \cdots + x_d^2 + \cdots = \prod_{j=1}^{d} \frac{1}{1 - x_j}.$$

There is a unique continuous homomorphism $\mathbb{Z}[[x_1, \ldots, x_d]] \to \mathbb{Z}[[t]]$ that sends $x_j \to t$ for all j. Each monomial of degree n in the x_j maps to t^n. It follows that the formal power series

$$1 + x_1 + \cdots + x_d + x_1^2 + x_1x_2 + \cdots + x_d^2 + \cdots$$

maps to $P_R(t)$, but evidently it also maps to $1/(1-t)^d$. This calculation of the Poincaré series yields the identity:

$$\frac{1}{(1-t)^d} = \sum_{n=0}^{\infty} \binom{n+d-1}{d-1} t^n.$$

Theorem. *Let R be a finitely generated graded A-algebra with $R_0 = A$, an Artin ring, and suppose that the generators $f_1, \ldots, f_d$ have positive degrees $k_1, \ldots, k_d$, respectively. Let M be a finitely generated $\mathbb{N}$-graded R-module. Then $P_M(t)$ can be written as the ratio of polynomials in $\mathbb{Z}[t]$ with denominator*

$$(1 - t^{k_1}) \cdots (1 - t^{k_d}).$$

If M is finitely generated and $\mathbb{Z}$-graded, one has the same result, but the numerator is a Laurent polynomial in $\mathbb{Z}[t, t^{-1}]$.

Proof. If the set of generators is empty, M is a finitely generated A-module and has only finitely many nonzero components. The Poincaré series is clearly a polynomial (respectively, a Laurent polynomial) in t. We use induction on d. We have an exact sequence of graded modules:

$$0 \to \operatorname{Ann}_M f_d \to M \xrightarrow{f_d} M \to M/f_dM \to 0.$$

In each degree, the alternating sum of the lengths is 0. This proves that

$$P_M(t) - t^{d_k} P_M(t) = P_{M/f_dM}(t) - P_{\operatorname{Ann}_M f_d}(t).$$

Since multiplication by f_d is 0 on both modules on the right, each may be thought of as a finitely generated $\mathbb{N}$- (respectively, $\mathbb{Z}$-) graded module over $A[f_1, \ldots, f_{d-1}]$, which shows, using the induction hypothesis, that $(1 - t^{k_d})P_M(t)$ can be written as a polynomial (respectively, Laurent polynomial) in t divided by

$$(1 - t^{k_1}) \cdots (1 - t^{k_{d-1}}).$$

Dividing both sides by $1 - t^{k_d}$ yields the required result. □

Remark. Base change over a field K to a field L does not change the Krull dimension of a finitely generated K-algebra, nor of a finitely generated module over such an algebra. A finitely generated K-algebra R is a module-finite extension of a polynomial ring $K[x_1, \ldots, x_d] \hookrightarrow R$, where $d = \dim(R)$. Then $L[x_1, \ldots, x_d] \cong L \otimes_K K[x_1, \ldots, x_d] \hookrightarrow L \otimes_K R$, ($L$ is free and therefore flat over K), and if $r_1, \ldots, r_s$ span R over $K[x_1, \ldots, x_d]$, then $1 \otimes r_1, \ldots, 1 \otimes r_s$ span $L \otimes R$ over $L[x_1, \ldots, x_d]$.

Evidently, for graded K-algebras R with $R_0 = K$ and graded K-modules M,

$$L \otimes R = \bigoplus_n L \otimes_K R_n$$

and

$$L \otimes_K M = \bigoplus_n L \otimes_K M_n$$

are graded, and their Hilbert functions do not change.

Proposition. *If R is finitely generated and graded over $R_0 = A$, Artin local, and $f \in R$ is homogeneous of degree $k > 0$, then if f is a not a zerodivisor on M, a finitely generated graded R-module, then $P_M(t) = \frac{1}{1-t^k} P_{M/fM}$.*

Proof. This is immediate from the exact sequence

$$0 \to M(-k) \xrightarrow{f} M \to M/fM \to 0$$

of graded modules and degree preserving maps: one has

$$P_M(t) - t^k P_M(t) = P_{M/fM}(t).$$

□

By induction on the number of indeterminates, this gives at once:

Proposition. *Let A be Artin local and $x_1, \ldots, x_d$ indeterminates over A whose respective degrees are $k_1, \ldots, k_d$. Let $R = A[[x_1, \ldots, x_d]]$. Then*

$$P_R(t) = \frac{\ell(A)}{\prod_{i=1}^d (1 - t^{k_i})}.$$

□

We note the following facts about integer valued functions on $\mathbb{Z}$ that are eventually polynomial. It will be convenient to assume that functions are defined for all integers even though we are only interested in their values for large integers. We write $f \sim g$ to mean that $f(n) = g(n)$ for all $n \gg 0$.

If f is a function on $\mathbb{Z}$ we define $\Delta(f)$ by the rule

$$\Delta(f)(n) = f(n) - f(n-1)$$

for all n. We define $\Sigma(f)$ by the rule $\Sigma(f)(n) = 0$ if $n < 0$ and

$$\Sigma(f)(n) = \sum_{j=0}^{n} f(j)$$

if $n \geq 0$. Suppose that $d \in \mathbb{N}$. We shall assume that $\binom{n}{d}$, is 0 if n is negative or if $d > n$. It is a polynomial in n of degree d if $n \geq 0$, namely

$$\frac{1}{d!} n(n-1)\cdots(n-d+1).$$

It is obvious that if $f \sim g$ then $\Delta(f) \sim \Delta(g)$, that $\Sigma(f) - \Sigma(g)$ is eventually constant, that $\Delta\Sigma(f) \sim f$, and that $\Sigma\Delta(f) - f$ is equivalent to a constant function. When $f \sim g$ is a nonzero polynomial we refer to the *degree* and *leading coefficient* of f, meaning the degree and leading coefficient of g.

Lemma. *A function f from $\mathbb{Z}$ to $\mathbb{Z}$ that agrees with a polynomial in n for all sufficiently large n is equivalent to a $\mathbb{Z}$-linear combination of the functions $\binom{n}{d}$, and any such $\mathbb{Z}$-linear function has this property. Hence, a polynomial g that agrees with f has, at worst, coefficients in $\mathbb{Q}$, and the leading coefficient has the form $e/d!$, where $e \in \mathbb{Z}$ and $d = \deg(g)$.*

If $f : \mathbb{Z} \to \mathbb{Z}$ then $\Delta(f)$ agrees with a polynomial of degree $d-1$, $d \geq 1$, if and only if f agrees with a polynomial of degree d, and the leading coefficient of $\Delta(f)$ is d times the leading coefficient of f. $\Delta(f) \sim 0$ iff $f \sim c$, where c is a constant integer. For $d \geq 0$, $\Sigma(f)$ $\sim$ a polynomial of degree $d+1$ iff $f \sim$ a polynomial of degree d (nonzero if $d = 0$), and the leading coefficient of $\Sigma(f)$ is the leading coefficient of f divided by $d+1$.

Proof. Every polynomial in n is uniquely a linear combination of the functions $\binom{n}{d}$, since there is exactly one of the latter for every degree $d = 0, 1, 2, \ldots$. Note that $\Delta\binom{n}{d} = \binom{n}{d} - \binom{n-1}{d} = \binom{n}{d-1}$ for all $n \gg 0$, from which the statement about that $\Delta(f)$ is polynomial when f is follows, as well as the statement relating the leading coefficients. Also, if f is eventually polynomial of degree d, then we may apply the Δ operator d times to obtain a nonzero constant function $\Delta^d f$, whose leading coefficient is $d!a$, where a is the leading coefficient of the polynomial that agrees with f, and this is an integer for large n, whence it is an integer. It follows that the leading coefficient of f has the form $e/d!$ for some $e \in \mathbb{Z} - \{0\}$. We may therefore subtract $e\binom{n}{d}$ from f to obtain a $\mathbb{Z}$-valued function that is polynomial of smaller degree than f for large n. We may continue in this way. Thus, the polynomial that agrees with f is a $\mathbb{Z}$-linear combination of the polynomials that agree with the $\binom{n}{d}$. Note also that $\Sigma\binom{n}{d} = \binom{0}{d} + \cdots + \binom{n}{d} = \binom{d}{d} + \cdots + \binom{n}{d}$ for $n \geq d$ and 0 otherwise. The value of the sum shown, when $n \geq d$, is $\binom{n+1}{d+1}$, by a straightforward induction on n. Finally, f is equivalent to a polynomial when Δf is, since $\Sigma\Delta(f) - f$ is equivalent to a constant. $\square$

Theorem. *Let R be a standard graded A-algebra, where (A, μ, K) is Artin local, and let M be a finitely generated graded R-module. Then the Hilbert function $\mathrm{Hilb}_M(n)$ of the finitely generated graded module M is eventually a polynomial in n of degree $\dim(M) - 1$ with a positive leading coefficient, except when M has dimension 0, in which case the Hilbert function is eventually identically 0.*

Proof. The Poincaré series can be written in the form $t^k Q(1-t)/(1-t)^d$ for some $k \leq 0$: we can write a polynomial in t as a polynomial in $1-t$ instead. This is a sum of finitely many terms of the form $mt^k/(1-t)^s$. We have already seen that the coefficient on t^n in $1/(1-t)^s$ is eventually given by a polynomial in n of degree $s-1$, and multiplying by t^k has the effect of substituting $n-k$ for n in the Hilbert function. A linear combination of polynomials is still a polynomial. It remains to prove the assertion about dimensions.

Since A is Artin, we know that $\mu^s = 0$ for some positive integer s. Then M has a filtration

$$M \supseteq \mu M \supseteq \mu^2 M \supseteq \cdots \supseteq \mu^{s-1} M \supseteq \mu^S M = 0,$$

and each of the $\mu^j M$ is a graded submodule. It follows that the Hilbert function of M is the sum of the Hilbert functions of the modules $\mu^j M/\mu^{j+1} M$. Since the dimension of M is the supremum of the dimensions of the factors, it suffices to prove the result for each

$\mu^j M/\mu^{j+1}M$, which is a module over the standard graded K-algebra $R/\mu R$. We have therefore reduced to the case where $A = K$ is a field.

We may apply $L \otimes_K \_$ for some infinite field L, and so we may assume without loss of generality that K is infinite. We use induction on $d = \dim(M)$. Let m be the homogeneous maximal ideal of R, which is generated by 1-forms. If M is 0-dimensional, this is the only associated prime of M, and M has a finite filtration with factors $\cong K$ and is killed by a power of m. Thus, M is a finite-dimensional K-vector space, and M_n is 0 for all $n \gg 0$. Now assume that M has positive dimension. Let

$$N = \bigcup_t \operatorname{Ann}_M m^t.$$

The modules $\operatorname{Ann}_M m^t$ form an ascending chain, so this is the same as $\operatorname{Ann}_M m^t$ for any $t \gg 0$ and is a graded submodule of M of finite length. The Hilbert function of M is the sum of the Hilbert functions of M/N and N, and the latter is eventually 0. Therefore we may study M/N instead of N. In M/N no nonzero element is killed by a power of m (or else its representative in M is multiplied into N by a power of m — but then it would be killed by a power of m, and so it would be in N). Replace M by M/N. Then no element of $M - \{0\}$ is killed by m, and so $m \notin \operatorname{Ass} M$. This means that the associated primes of M cannot cover R_1, which generates m, for then one of them would contain R_1. Thus, we can choose a degree one element f in R_1 that is not a zerodivisor on M. Then $\dim(M/fM) = \dim(M) - 1$, and so $P(n) = \operatorname{Hilb}_{M/fM}(m)$ is eventually a polynomial in n of degree $d-2$ if $d \geq 2$; if $d = 1$, it is constantly 0 for $n \gg 0$. Let $Q(n) = \operatorname{Hilb}_M(n)$. Since $Q(n) - Q(n-1) = P(n)$, Q is a polynomial of degree $d-1$, (if $d = 1$, we can conclude that Q is constant). Since $Q(n)$ is positive for $n \gg 0$, the leading coefficient is positive for all $d \geq 1$. $\square$

Remark. The trick of enlarging the field avoids the need to prove a lemma on homogeneous prime avoidance.

Let (R, m, K) be a local ring, and let M be a finitely generated R-module with m-stable filtration $\mathcal{M} = \{M_n\}_n$. We write $\operatorname{gr}_{\mathcal{M}}(M)$ for the associated graded module $\bigoplus_{n=0}^{\infty} M_n/M_{n+1}$, which is a finitely generated $\operatorname{gr}_I R$-module, and we write $\operatorname{gr}_I M$ in case $\mathcal{M}$ is the I-adic filtration. In this situation we define $H_R(n) = \ell(R/m^{n+1})$, and call this the *Hilbert function of* R, and we write $H_{\mathcal{M}}(n) = \ell(M/M_{n+1})$, the *Hilbert function* of M with respect to the m-stable filtration $\mathcal{M}$. In case $\mathcal{M}$ is the m-adic filtration on M, we write $H_M(n)$ for $\ell(M/m^{n+1}M)$.

Our next objective is the following result:

Theorem (existence of Hilbert polynomials. *Let (R, m, K) be local and let M be a nonzero R-module of Krull dimension d. Then for any m-stable filtration $\mathcal{M}$ of M, $H_{\mathcal{M}}(n)$ is eventually a polynomial in n of degree d.*

First note that $\operatorname{gr}_{\mathcal{M}} M = \bigoplus_n M_n/M_{n+1}$, then for all n, $H_{\mathcal{M}}(n) = \ell(M/M_{n+1}) = \sum_{i=0}^{n} \ell(M_i/M_{i+1})$ since M/M_{n+1} has a filtration with the M_i/M_{i+1} as factors, $0 \leq i \leq n$. This says that $\Sigma \operatorname{Hilb}_{\operatorname{gr}\mathcal{M}} = H_{\mathcal{M}}$. This shows that $H_{\mathcal{M}}(n)$ is eventually polynomial in n

of degree $\dim\big(\mathrm{gr}_{\mathcal{M}}(M)\big)$. Once we complete the proof of the theorem above, it will follow that $\dim\big(\mathrm{gr}_{\mathcal{M}}(M)\big) = \dim(M)$, and, in particular, $\dim\big(\mathrm{gr}_m(R)\big) = \dim(R)$ for any local ring R. Before proving the theorem we need the following observation.

Proposition. *Let (R, m, K) be local, and let $0 \to N \to M \to \overline{M} \to 0$ be an exact sequence of finitely generated R-modules. Let $\mathcal{M}$ be an M-stable filtration on M, let $\overline{\mathcal{M}}$ be the induced filtration on $\overline{M}$ whose n th term in the image of M_n, and let $\mathcal{N}$ be the inherited filtration on N, whose n th term is $M_n \cap N$. Then the sequence*

$$0 \to \mathrm{gr}_{\mathcal{N}}(N) \to \mathrm{gr}_{\mathcal{M}}(M) \to \mathrm{gr}_{\overline{\mathcal{M}}}(\overline{M}) \to 0$$

is an exact sequence of graded modules with degree-preserving maps, and so

$$H_{\mathcal{M}}(n) = H_{\mathcal{N}}(n) + H_{\overline{\mathcal{M}}}(n)$$

for all n.

Proof. For every n, the sequence

$$(*_n) \qquad 0 \to N_n \to M_n \to (M/N)_n \to 0$$

is exact by construction: $(M/N)_n$ is the image of M_n by definition, and the kernel of $M_n \to (M/N)_n$ is the same as the kernel of $M_n \to M/N$, which is $N \cap M_n = N_n$ by definition. The exactness of $(*_n)$ and $(*_{n+1})$ implies the exactness of the sequence of quotients

$$0 \to \frac{N_n}{N_{n+1}} \to \frac{M_n}{M_{n+1}} \to \frac{(M/N)_n}{(M/N)_{n+1}} \to 0$$

for all n. $\square$

In order to prove the Theorem, we may again consider $N = \bigcup_t \mathrm{Ann}_N m^t$, which will be the same as $\mathrm{Ann}_M m^t$ for any $t \gg 0$. Any m-stable filtration on N is eventually 0, and so $H_{\mathcal{N}}(n) = \ell(N)$ for all sufficiently large n. If M is 0-dimensional we are done. If not, by the Proposition it suffices to consider M/N instead of M.

We have reduced the problem of proving that the degree of the Hilbert function of $M \neq 0$ is the Krull dimension of M to the case where $m \notin \mathrm{Ass}(M)$. Here M is a finitely generated module over the local ring (R, m, K).

Before proceeding further, we generalize the notion of Hilbert functions to a larger context. Let M be a finitely generated module over the local ring (R, m, K) and let $\mathfrak{A}$ be any ideal of R that is primary to m modulo the annihilator I of M. That is, $\mathfrak{A} + I$ is m-primary, or, equivalently, $\mathfrak{A}(R/I)$ is primary to $m/I \subseteq R/I$. Note that $\dim(M) = \dim(R/I)$, by definition. Then for any $\mathfrak{A}$-stable filtration $\mathcal{M} = \{M_n\}_n$, we define $H_{\mathcal{M}}(n) = \ell(M/M_{n+1})$. We may always use the $\mathfrak{A}$-adic filtration, in which case we write $H_{\mathfrak{A},M}(n) = \ell(M/\mathfrak{A}^n M)$. The calculation of the values of this function is unaffected if we replace R by R/I: all of the modules involved are killed by I, and multiplying any of these modules by $\mathfrak{A}$ is the same as multiplying it by the expansion of $\mathfrak{A}$ to R/I. Thus, without loss of generality, we may readily assume that M is faithful and that $\mathfrak{A}$ is m-primary, by passing to R/I as indicated.

The following result will complete the proof of the Theorem on the existence of the Hilbert polynomials.

Theorem. *Let M be a finitely generated nonzero module over a local ring (R, m, K). For any $\mathfrak{A}$-stable filtration $\mathcal{M}$ on M, $H_{\mathcal{M}}(n)$ is eventually a polynomial that agrees with $\Sigma\,\mathrm{Hilb}_{\mathrm{gr}_{\mathcal{M}}}(M)$. The degree and leading coefficient of this polynomial are independent of the choice of the $\mathfrak{A}$-stable filtration $\mathcal{M}$. The degree is the same as $\dim(M)$, and also the same as $\dim\big(\mathrm{gr}_{\mathcal{M}}(M)\big)$.*

Proof. We kill $\mathrm{Ann}_R M$, and so assume that M is faithful over R, that $\mathfrak{A}$ is m-primary, and that $\dim(M) = \dim(R)$. Since $\mathrm{gr}_{\mathcal{M}}(M)$ is a finitely generated module over $\mathrm{gr}_{\mathfrak{A}}R$, which is a standard graded algebra over the Artin local ring $R/\mathfrak{A}$, we have that $\mathrm{Hilb}_{\mathrm{gr}_{\mathcal{M}}(M)}(n)$ is a polynomial of degree $\dim\big(\mathrm{gr}_{\mathcal{M}}(M)\big) - 1$. Since

$$\ell(M_{n+1}) = \ell(M/M_1) + \ell(M_1/M_2) + \cdots + \ell(M_n/M_{n+1}),$$

it follows that $H_{\mathcal{M}}(n)$ is polynomial of degree $\dim\big(\mathrm{gr}_{\mathcal{M}}(M)\big)$.

We know compare the leading term of the polynomial coming from $\mathcal{M} = \{M_n\}_n$ with the polynomial given by the $\mathfrak{A}$-adic filtration. Since $\mathfrak{A}M_n \subseteq M_{n+1}$ for all n, $\mathfrak{A}^n M \subseteq M_n$ for all n, and $\ell(M/M_n) \leq \ell(M/\mathfrak{A}^n M)$. Let c be such that $M_{n+c} = \mathfrak{A}^n M_c$ for all $n \geq c$. Then $M_{n+c} \subseteq \mathfrak{A}^n m$, and so $\ell(M/M_{n+c}) \geq \ell(M/\mathfrak{A}^n M)$ for all n. Thus,

$$H_{\mathcal{M}}(n+c) \geq H_{\mathfrak{A},M}(n) \geq H_{\mathcal{M}}(n)$$

for all n, and so $H_{\mathfrak{A},M}$ is trapped between two polynomials with the same degree and leading coefficient. Therefore all three have the same degree and leading coefficient. This shows that the leading term of the polynomial in independent of the choice of $\mathcal{M}$.

We next show that the degree is independent of the choice of $\mathfrak{A}$. We can choose c such that $m^b \subseteq \mathfrak{A} \subseteq m$, and then $m^{nb} \subseteq \mathfrak{A}^n \subseteq m^n$ for all n, and so

$$\ell(M/m^{nb}) \geq \ell(M/\mathfrak{A}^n M) \geq \ell(M/m^n M)$$

which shows that $H_{\mathfrak{A},M}$ is eventually a polynomial trapped between $H_M(n)$ and $H_M(bn)$. The latter two are eventually polynomials of the same degree, and so $H_{\mathcal{M}}(n)$ must be as well, since we know that it is eventually polynomial.

It remains to see that the degree is $d = \dim(M) = \dim(R)$. To see that the degree is $\leq \dim(R)$, we choose $\mathfrak{A}$ to be generated by a system of parameters $x_1, \ldots, x_d \in m$. Then $\mathrm{gr}_{\mathfrak{A}}(R)$ is generated over $R/\mathfrak{A}$ by the classes of the elements x_i in $\mathfrak{A}/\mathfrak{A}^2$. Since the algebra is generated by d elements of degree 1, the denominator of the Poincaré series for $\mathrm{gr}_{\mathcal{M}}M$ is $(1-t)^d$, at worst, and this shows that the degree of the Hilbert polynomial of the associated graded module is at most $d-1$, which yields the upper bound d for the degree of $H_{\mathcal{M}}(n)$.

The last step is to show that the degree is at least d. We use induction on $\dim(M)$: the case where $d = 0$ is trivial. Since the degree is independent of both the m-primary ideal $\mathfrak{A}$ chosen and the specific $\mathfrak{A}$-stable filtration used, it suffices to consider the m-adic filtration. Moreover, we have already shown that one need only consider the case when no element of M is killed by m (for we may kill $\bigcup_t \mathrm{Ann}_M m^t$). Thus, we may assume that $m \notin \mathrm{Ass}(M)$,

and by prime avoidance we may choose $f \in m$ such that f is not a zerodivisor on M. Consider the short exact sequence

$$0 \to M \xrightarrow{f} M \to M/fM \to 0.$$

Place the m-adic filtration on the central copy of M, the inherited m-adic filtration on the left hand copy of M (using that it is isomorphic with fM to think of it as a submodule of M: specifically, $M_n = m^n M :_M f$), and the image of the m-adic filtration of M on M/fM: this is the same as the m-adic filtration on M/fM. By the Proposition from last time, we find that $H_M(n) - H_{\mathcal{M}}(n) = H_{M/fM}(n)$. By what was proved above, the two polynomials on the left have the same leading term: when we subtract, we get a polynomial of lower degree. By the induction hypothesis, the polynomial on the right has degree $\dim(M/fM) = d-1$. It follows that the degree of $H_M(n)$ is at least d. $\square$

For emphasis, we state the following consequence separately.

Corollary. *If M is a finitely generated module over the local ring (R, m), and $\mathfrak{A}$ is m-primary, M, $\mathrm{gr}_m(M)$, and $\mathrm{gr}_{\mathfrak{A}}(M)$ have the same Krull dimension.* $\square$

Note that if (R, m, K) is local, for any m-primary ideal $\mathfrak{A}$, we have that $R/\mathfrak{A}^n \cong \widehat{R}/\mathfrak{A}^n\widehat{R}$ (recall that $\mathfrak{A}\widehat{R} \cong \widehat{\mathfrak{A}}$), and that for any finitely generated R-module M, $\widehat{M}/\mathfrak{A}^n\widehat{M} \cong M/\mathfrak{A}^n M$ for all n. The completions referred to here are all m-adic. This shows that we may identify $\mathrm{gr}_{\mathfrak{A}}(R) \cong \mathrm{gr}_{\widehat{\mathfrak{A}}}\widehat{R}$, and $\mathrm{gr}_{\mathfrak{A}}(M) \cong \mathrm{gr}_{\widehat{\mathfrak{A}}}\widehat{M}$; in particular, we have these identifications when $\mathfrak{A} = m$.

We also note:

Proposition. *If (R, m, K) is local and $\mathrm{gr}_m(R)$ is a domain then R and $\widehat{R}$ are domains.*

Proof. The result for R implies the result for $\widehat{R}$, since their associated graded rings are the same. Suppose the result is false, so that $f, g \in m - \{0\}$ are such that $fg = 0$. Since $f \neq 0$, we can choose $s \in \mathbb{N}$ such that $f \in m^s - m^{s+1}$, and, similarly, we can choose $t \in \mathbb{N}$ such that $g \in m^t - m^{t+1}$. Let $[f]$ indicate the class of f in m^s/m^{s+1} and $[g]$ the class of $g \in m^t - m^{t+1}$. Then $[f]$ and $[g]$ are nonzero homogeneous elements of $\mathrm{gr}_m(R)$, and their product is $[fg] = [0]$, contradicting that $\mathrm{gr}_m(R)$ is a domain. $\square$

Note that the completion of a local domain need not be a domain in general. The polynomial $f = y^2 - x^2(1+x)$ is irreducible in the polynomial ring $\mathbb{C}[x, y]$, since $1 + x$ is not a square (even in the fraction field), and so $x^2(1+x)$ is not a square. Thus, it generates a prime ideal which remains prime if we localize at (x, y). Let $R = \mathbb{C}[x, y]_{(x,y)}/(f)$, which is a local domain. Its completion $\widehat{R}$ is $\mathbb{C}[[x, y]]/(f)$, but now f is reducible: $1 + x$ is a perfect square in $\mathbb{C}[[x]]$, by Hensel's lemma (or use Newton's binomial theorem to give an explicit formula for the power series square root of $1 + x$). Instead of $\mathbb{C}$, we could have used any field of characteristic different from 2. In characteristic 2, $y^3 - x^3(1 + x)$ gives a similar example.

We can use associated graded rings to characterize regular local rings.

Theorem. *A local ring (R, m, K) is regular if and only if $\mathrm{gr}_m(R)$ is a polynomial ring in d variables over K, in which case $d = \dim(R)$.*

Proof. Let $x_1, \ldots, x_s$ be a minimal set of generators for m, and note that m/m^2 is the K-vector space of forms of degree 1 in $\mathrm{gr}_m(R)$. Now $d = \dim(R) = \dim\big(\mathrm{gr}_m(R)\big)$. If $\mathrm{gr}_m(R)$ is polynomial, it must be the polynomial ring in s variables, and since it has dimension both s and d we have that $s = d$, which shows that R is regular. If R is regular, we know that $\mathrm{gr}_m(R)$ is generated over K by d one forms, and has dimension d. Thus, it is a homomorphic image of the polynomial ring in d variables over K, where the variables map to the $[x_i]$. Since the dimension of $\mathrm{gr}_m(R)$ is d, there cannot be any kernel: a proper homomorphic image of a polynomial ring in d variables has Krull dimension $< d$. This shows that $\mathrm{gr}_m(R)$ is a polynomial ring in d variables. □

Since the associated graded ring of a regular local ring is a domain, we have at once:

Corollary. *A regular local ring is a domain.* □

Let (R, m, K) be local, let M be a nonzero finitely generated R-module with annihilator I of Krull dimension d, and let $\mathfrak{A} \subseteq R$ be an ideal such that $\mathfrak{A}(R/I)$ is primary to $m/I \subseteq R/I$. We define the multiplicity of M with respect to $\mathfrak{A}$ to be $d!$ times the leading coefficient of the Hilbert function of M. This function is integer-valued, and the equivalent polynomial has degree d, and is therefore a $\mathbb{Z}$-linear combination of the polynomials $\binom{n}{j}$, $0 \leq j \leq d$, and $\binom{n}{d}$ must occur with positive coefficient. Therefore, the multiplicity is a positive integer. It may also be described as

$$d! \lim_{n\to\infty} \frac{\ell(M/\mathfrak{A}^{n+1}M)}{n^d}.$$

If $\mathfrak{A} = m$, we simply refer to the *multiplicity* of M. In particular we may refer to the *multiplicity* of R itself.

We shall be particularly interested in determining multiplicities of rings with respect to parameter ideals, i.e., ideals generated by a system of parameters. In this case, the multiplicity can be recovered as an alternating sum of lengths of homology modules for a certain homology theory, Koszul homology, which can be viewed as a special case of Tor. The proof that we shall give of our result in this direction will depend on the theory of spectral sequences.

We shall also use Tor and related homological ideas to prove properties of regular rings. The only known proofs that a localization of a regular local ring at prime is again regular are by these methods, and the proof of unique factorization also depends on these ideas.

Before beginning the development of these homological methods, we want to make a few more comments about associated graded rings and multiplicities.

Note that the multiplicity of any regular local ring is 1. To check this, observe that the associated graded ring is $K[x_1, \ldots, x_d]$ where d is the dimension, and the Hilbert polynomial corresponds to $\binom{n+d-1}{d-1}$. The Hilbert function of the local ring is obtained by

summing the values of $\binom{t+d-1}{d-1}$ for $t = 0, \ldots, n$. However, we note that the number of monomials in $x_1, \ldots, x_n$ of degree $\leq n$ is the same as the number of monomials of degree precisely n in $x_0, x_1, \ldots, x_d$: there is a bijection obtained by substituting $x_0 = 1$. Thus, the Hilbert function of the regular ring corresponds to $\binom{n+d}{d}$, which has leading coefficient $1/d!$, and this shows that the multiplicity is 1.

Let $R = K[[x_1, \ldots, x_d]]$ and let $f \in R$ have a lowest degree term of degree $\mu > 0$. The multiplicity of the ring R/f is μ. We shall check this by giving a technique for calculating associated graded rings of quotients.

If (R, m, K) is local and $f \in R - \{0\}$, there is always a unique integer $t \in N$ such that $f \in m^t - m^{t+1}$. Then $[f] \in m^t/m^{t+1} = [\mathrm{gr}_m(R)]_t$ is homogeneous and nonzero: we denote this element $\mathcal{L}(f)$, and call it the *leading form* of f. Note that $\mathcal{L}(f)$ is in $\mathrm{gr}_m(R)$, not in R. If $I \subseteq R$, we write $\mathcal{L}(I)$ for the ideal of $\mathrm{gr}_m(R)$ generated by all leading forms of elements of $I - \{0\}$: this is evidently a homogeneous ideal. In attempting to find generators for $\mathcal{L}(I)$, it is not in general sufficient to take the leading forms of a set of generators of I. See problems **1.** and **5.** of Problem Set #2. However, it is easy to see that this is sufficient for a nonzero principal ideal in a formal power series ring $K[[x_1, \ldots, x_d]]$ over a field K: when one multiplies by another nonzero power series, the leading form of the product is the product of the leading forms.

Proposition. *Let (R, m, K) be local and let I be a nonzero ideal of R. Then*

$$\mathrm{gr}_{m/I}(R/I) \cong \mathrm{gr}_m R/\mathcal{L}(I).$$

Proof. We have that

$$[\mathrm{gr}_{m/I}(R/I)]_n = (m/I)^n/(m/I)^{n+1} \cong (m^n + I)/(m^{n+1} + I) \cong m^n/\big(m^n \cap (m^{n+1} + I)\big).$$

But if $u \in m^{n+1}$, $i \in I$, and $u + i \in m^n$, then $u \in m^n$, and so $u \in m^n \cap I$. This shows that $m^n \cap (m^{n+1} + I) = m^{n+1} + (m^n \cap I)$, and so

$$[\mathrm{gr}_{m/I}(R/I)]_n \cong m^n/(m^{n+1} + m^n \cap I) \cong (m^n/m^{n+1})/W_n,$$

where W_n is the image of $m^n \cap I$ in $m^n/m^{n+1} = [\mathrm{gr}_m(R)]_n$. But if $f \in m^n \cap I$, then if $f \in m^{n+1}$ the image of f in $[\mathrm{gr}_m(R)]_n$ is 0, while if $f \notin m^{n+1}$ then $[f] \in m^n/m^{n+1}$ is precisely a nonzero leading form in degree n of an element of I, and the result now follows. $\square$

We now come back to the problem of calculating the associated graded ring of $R = K[[x_1, \ldots, x_d]]/(f)$ where f has nonzero leading form L of degree $\mu \geq 1$. From the remarks we have made, $\mathrm{gr}_m(R) \cong K[x_1, \ldots, x_d]/(L)$. We have a short exact sequence $0 \to T(-\mu) \xrightarrow{L} T \to T/(L) \to 0$, where $T = K[x_1, \ldots, x_d]$. Since the Hilbert function of T corresponds to $\binom{n+d-1}{d-1}$, the Hilbert function of $T/(L)$ corresponds to $\binom{n+d-1}{d-1} - \binom{n-\mu+d-1}{d-1}$. When we sum, we get $\binom{n+d}{d} - \binom{n-\mu+d}{d}$ up to a constant. It is easy to check that if $P(n)$ has leading coefficient a, then $P(n) - P(n-\mu)$ has leading coefficient μa. Thus, the leading coefficient is $\mu/d!$, and so the multiplicity is μ, as asserted earlier.