1. Additive functions

Let R be a ring. We shall call, a collection $\mathcal{M}$ of R modules, an abelian subcategory if, for any $M, N \in \mathcal{M}$, $M \oplus N \in \mathcal{M}$ and for any homomorphism of R modules $f : M \to N$, $\ker(f), \operatorname{coker}(f) \in \mathcal{M}$. This is not a standard definition but we shall use this as terminology for this section. The collection of finite dimensional vector spaces over a field k is an example of an abelian subcategory of vector spaces over k.

Recall the definition of an additive function.

Definition 1: Let A be a ring and $\mathcal{M}$ an abelian subcategory of A modules. A function $\lambda : \mathcal{M} \to \mathbb{Z}$ is called additive if for any exact sequence $0 \to M' \to M \to M'' \to 0$ of modules in $\mathcal{M}$ we have $\lambda(M) = \lambda(M') + \lambda(M'')$.

We showed in class that if we have an arbitrary exact sequence of modules in $\mathcal{M}$

$$0 \to M_1 \to \cdots \to M_n \to 0 \tag{1}$$

then the additive function λ satisfies

$$\sum_{i=1}^{n} (-1)^i \lambda(M_i) = 0.$$

The proof uses the fact that we can break up the exact sequence (1) into short exact sequences using kernels and cokernels and that kernels and cokernels belong to $\mathcal{M}$.

If A is a field then dimension is an example of an additive function on finite dimensional A vector spaces.

Definition 2: Let M be an R module. A chain of submodules is a finite sequence $(M_0, \ldots, M_n)$ of submodules of M such that

$$M = M_0 \supset M_1 \supset \ldots \supset M_n = 0 (\text{strict inclusions}).$$

The length of the chain is the number n.

A chain $(M_i)_1^n$ is called maximal if for any $i = 0, \ldots, n-1$, there is no submodule M_i' of M such that $M_i \supset M_i' \supset M_{i+1}$ and the inclusions are strict.

Remark. Note that if $M = M_0 \supset \ldots \supset M_n = 0$ is a maximal chain in M then each $N_i = M_i/M_{i+1}$ is a simple module, that is the only submodules of N_i are 0 and N_i.

Proposition 3. Let M be an R module. Suppose that a maximal chain of submodules of M has length n, then

(a) every maximal chain has length n,
(b) any chain which has length n is a maximal chain,
(c) every chain can be extended to a maximal chain.

Proof. Let $l(M)$ be the infimum of the lengths of all maximal chains of M. We set $l(M) = \infty$ if M has no maximal chain.

If $N \subset M$ and $M = M_0 \supset \ldots \supset M_n = 0$ is a maximal chain of M. Then let $N_i = M_i \cap N$, clearly $N_i \supset N_{i+1}$ and N_i/N_{i+1} is a submodule of M_i/M_{i+1} which is a simple module. Thus either $N_i/N_{i+1} = 0$ in which case $N_i = N_{i+1}$ or $N_i/N_{i+1} = M_i/M_{i+1}$. Eliminating the repeated terms we thus get a maximal chain of N which has length less than n. Thus $l(N) \leq l(M)$. Moreover if $l(N) = l(M) = n$ then $N_i/N_{i+1} = M_i/M_{i+1}$ for each i, thus $N_{n-1} = M_{n-1}$ implies $N_{n-2} = M_{n-2}$, proceeding in this way we get $N = M$.

Now suppose $M = M_0 \supset \ldots \supset M_k = 0$ is a chain of length k of M. Then $l(M) > l(M_1) > \ldots > l(M_k) = 0$. Thus $l(M) \geq k$. So any chain of submodules of M has length at most $l(M)$.

Thus the length of any maximal chain of M is at most $l(M)$ but it must be equal to $l(M)$ by the definition of $l(M)$. This proves part (a).

Now suppose there is a chain of M of length $l(M)$, then it cannot be extended any more, hence it is maximal. This proves part (b).

Finally if $M = M_0 \supset \ldots \supset M_k = 0$ is a chain of length $k < l(M)$, then it is not maximal. Thus new terms can be inserted in the chain until the length is $l(M)$. □

Definition 4 (length): If an R module M has a maximal chain then it is called a module of finite length. In that case the length of M is defined to be the length of any maximal chain of M and denoted by $l(M)$.

Exercise (i). Let R be a ring. Show that the modules of finite length over R is an abelian subcategory of modules over R.

Proposition 5. The length is an additive function on the modules of finite length over a ring.

Proof. Let $0 \to M' \xrightarrow{a} M \xrightarrow{b} M'' \to 0$ be an exact sequence of finite length R modules. Let $M = M_0 \supset \ldots \supset M_n = 0$ be a maximal chain of M. Let $M_i' = a^{-1}(M_i)$ and $M_i'' = b(M_i)$. Then we have an exact sequence

$$0 \to M_i'/M_{i+1}' \to M_i/M_{i+1} \to M_i''/M_{i+1}'' \to 0.$$

Since M_i/M_{i+1} is simple exactly one of the following is true: $M_i'/M_{i+1}' \cong M_i/M_{i+1} \Rightarrow M_i'' = M_{i+1}''$ or $M_i''/M_{i+1}'' \cong M_i/M_{i+1} \Rightarrow M_i' = M_{i+1}'$.

Let

$$S = \{i \mid 0 \leq i < n,\ M_i' \neq M_{i+1}'\}$$

and

$$T = \{i \mid 0 \leq i < n,\ M_i'' \neq M_{i+1}''\}$$

then $S \cap T = \{0, \ldots, n-1\}$. If $s_0 < \ldots < s_k$ are the elements of S then $M' = M_{s_0}' \supset \ldots \supset M_{s_k+1} = 0$ is a maximal chain for M', thus $l(M') = |S|$. Similarly $l(M'') = |T|$. This completes the proof. □

If R is a field the finite length R modules are precisely the finite dimensional vector spaces and the length then coincides with the dimension.

Exercise (ii). Show that a module has finite length if and only if it is both noetherian and artinian.

Remark. Note that a ring R (for example $R = \mathbb{Z}$) which is not Artinian is not a finite length module over itself by Exercise (ii), however it is of course a finitely generated module over itself. On the other hand if an R module is finite length then it is noetherian hence finitely generated. Hence finite length is stronger than finitely generated.

Exercise (iii). For a ring R, show that any finitely generated module is a module of finite length if and only if R is artinian.

2. Hilbert Polynomial

Let A be a noetherian graded ring. Then we have seen previously that A_0 is noetherian and A is a finitely generated A_0 algebra. Choose homegeneous generators $x_1, \ldots, x_k$ with $x_i \in A_{s_i}$.

Now if M is a graded A module which is finitely generated generated then again we may choose homogeneous generators $m_1, \ldots, m_l$ with $m_i \in M_{t_i}$. If $m \in M_n$ then

$$m = \sum_{i=1}^{l} f_i(x_1, \ldots, x_s) m_i \text{ where } f_i \in A_{n-t_i}.$$

The element $f_i(x_1, \ldots, x_s)$ is thus a homogeneous polynomial in the generators of A which is not necessarily unique. It can thus be seen that the finite set

$$\left\{ x_1^{a_1} \cdots x_k^{a_k} m_j \mid 1 \leq j \leq l,\ \sum_{1}^{k} a_i = n - t_j,\ a_i \geq 0 \right\}$$

generate M_n as an A_0 module. Hence all the M_n are finitely generated modules over A_0.

Let us now fix a noetherian graded ring R and an additive function λ on the collection of finitely generated A_0 modules.

Remark. Note that the collection of finitely generated A_0 modules may not in general be an abelian subcategory of modules over A_0 because kernels may fail to be finitely generated. However is true when A_0 is noetherian, since submodules and quotients of finitely generated modules are again finitely generated for a noetherian ring.

Definition 6: Let M be a graded A module. Then the Poincaré series of M with respect to λ is the power series

$$P_\lambda(M) = \sum_{n=0}^{\infty} \lambda(M) t^n \in \mathbb{Z}[[t]].$$

Exercise (iv). If $0 \to M' \to M \to M'' \to 0$ is an exact sequence of

Example 1. Consider the polynomial ring in k variables $A = k[x_1, \ldots, x_k]$ over a field F and let $M = A$. Here A_0 is a field and let us take λ to be the dimension, then $\dim A_n = \binom{n+k-1}{k-1}$. Thus

$$P_\lambda(A) = \sum_{n=0}^{\infty} \binom{n+k-1}{k-1} t^n = \frac{1}{(1-t)^k}.$$

An ideal $I \subset A$ is called a homogeneous ideal if for any $a \in I$ the homogeneous components of a also belong to I. In this case

$$I = \bigoplus_{n=0}^{\infty} I_n, \text{ where } I_n = I \cap A_n.$$

It can be easily show that an ideal is homogeneous if it can be generated by homogeneous elements. Thus $\left(x_1^2, x_2^3\right)$ is a homogeneous ideal but $\left(x_1^2 + x_2^3\right)$ is not.

If $I \subset A$ is a homogeneous ideal then it is a graded A module and so is A/I. Moreover we have an exact sequence of graded modules $0 \to I \to R \to R/I \to 0$ which implies

$$P_\lambda(R) = P_\lambda(I) + P_\lambda(R/I).$$

Now for example if we take $I = (x_k)$ then $R/I \cong F[x_1, \ldots, x_{k-1}]$ and we have

$$P_\lambda(I) = \frac{1}{(1-t)^k} - \frac{1}{(1-t)^{k-1}} = \frac{t}{(1-t)^k}.$$

Remark. Consider the power series ring $R[[t]]$ over a ring R. Recall that are precisely the elements

$$f(t) = a_0 + a_1 t + a_2 t^2 + \ldots \in R[[t]]$$

is a unit if and only if a_0 is a unit in R. Thus the units of $\mathbb{Z}[[t]]$ are precisely the power series which start with 1 or -1. As an example $(1-t)^{-1} = 1 + t + t^2 + \ldots$.

Theorem 7 (Hilbert, Serre)**.** Let A be a noetherian graded ring generated as an algebra over A_0 by homogeneous elements $x_1, \ldots, x_s$ with $x_i \in A_{k_i}$ and let λ be an additive function on the finitely generated A_0 modules. For any graded A module M, the Poincaré series has the form

$$P_\lambda(M) = \frac{f(t)}{(1-t^{k_1}) \cdots (1-t^{k_s})}$$

where $f(t) \in \mathbb{Z}[t]$ is a polynomial.

Proof. We shall prove this by induction on s the number of generators of A as an A_0 algebra.

If s_0, we have $A = A_0$ and $A_n = 0$ for $n > 0$. Since M is then a finitely generated A_0 module we must have $M_n \neq 0$ for only finitely many $n \geq 0$. Hence, $P_\lambda(M)$ is a polynomial, proving the base case.

Now assume $s > 0$ and that the result is true for $s-1$. Then consider the A module homomorphism $\phi : M \to M$ given by multiplication by x_s. Then $K = \ker(\phi)$ and $L = \operatorname{coker}(\phi)$ are both graded modules A modules and we have an exact sequence of A_0 modules

$$0 \to K_n \to M_n \xrightarrow{\times x_s} M_{n+k_s} \to L_{n+k_s} \to 0.$$

Thus

$$\lambda(M_{n+k_s}) - \lambda(M_n) = \lambda(L_{n+k_s}) - \lambda(K_n)$$

Now multiplying this equation by t^{n+k_s} and summing over n we get

$$\sum_{n=k_s}^{\infty} t^n \lambda(M_n) - t^{k_s} \sum_{n=0}^{\infty} \lambda(M_n) = \sum_{n=k_s}^{\infty} t^n \lambda(L_n) - t^{k_s} \sum_{n=0}^{\infty} t^n \lambda(K_n),$$

which yields

$$(1 - t^{k_s}) P_\lambda(M) = P_\lambda(L) - P_\lambda(K) + g(t)$$

where $g(t)$ is a polynomial.

The ideal (x_s) annihilates both K and L hence they are both $A' = A/(x_s)$ graded modules. Clearly $A'_0 = A_0$ and A' is generated over A_0 by $x_1, \ldots, x_{s-1}$, hence by assumption the result is true for K and L, hence it is also true form M. □

Definition 8: Let A be a noetherian graded ring, λ an additive function on finitely generated A_0 modules and M a finitely generated graded A module. The the Hilbert dimension of M with respect to λ, which we shall denote by $d_{\text{Hilb},\lambda}(M)$ is defined to be the order of the pole of $P_\lambda(M)$ at $t = 1$.

The following corollary is quite useful.

Corollary 9. With the notation from Theorem 7 if $k_i = 1$ for all $i = 1, \ldots, s$, then there is an integer $N \geq 0$ and a polynomial $H_{M,\lambda}(t) \in \mathbb{Q}[t]$ such that for $n > N$

$$\lambda(M_n) = H_{M,\lambda}(n).$$

The polynomial deg $H_{M,\lambda}$ has degree $d_{\text{Hilb},\lambda}(M) - 1$ and is called the Hilbert Polynomial of M.

Proof. By Theorem 7 we have

$$P_\lambda(M) = \frac{f(t)}{(1-t)^s}$$

If $d = d_{\text{Hilb},\lambda}(M)$ then by cancelling common factors we may assume $s = d$ and f is not divisible by $(1 - t)$.

Now if $f(t) = a_0 + a_1 t + \ldots + a_N t^N$ then since

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

we have

$$\lambda(M_n) = \sum_{k=1}^{N} a_k \binom{n-k+d-1}{d-1}.$$

Hence

$$H_{M,\lambda}(t) = \sum_{k=1}^{N} a_k \binom{t-k+d-1}{d-1}$$

is the coveted polynomial with leading term $\frac{(\sum_{k=1}^{N})}{(d-1)!} t^{d-1}$. □

Remark. A polynomial $f(t) \in \mathbb{Q}[t]$ such that $f(n)$ is an integer for ever integer n may not have integral coefficients. For example $P_k(t) = \binom{t}{k} = \frac{1}{k!}t(t-1)\cdots(t-k+1)$ is one such polynomial. In fact the set of such polynomials inside $\mathbb{Q}[t]$ forms a subring which is a free abelian group with integer basis $\{P_k(t) \mid k = 0, 1, \ldots\}$.

Example 2. Let k be a field and $\lambda = \dim$. The polynomial ring $A = k[x_1, \ldots, x_n]$ has Hilbert dimension n and Hilbert polynomial $\binom{t+n-1}{n-1}$. If $I \subset A$ is a homogeneous ideal then

$$H_I(t) + H_{A/I}(t) = \binom{t+n-1}{n-1}.$$

If $I = (f)$ where $f \in A$ is a polynomial of degree d then

$$\dim_k I_m = \begin{cases} 0 & m < d, \\ \binom{m-d+n-1}{n-1} & m \geq d. \end{cases}$$

Hence $H_I(t) = \binom{t-d+n-1}{n-1}$ and the Poincaré series of I is

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

Thus $H_{R/I}(t) = \binom{t+n-1}{n-1} - \binom{t-d+n-1}{n-1}$ and

$$P(R/I) = P(R) - P(I) = \frac{1-t^d}{(1-t)^n} = \frac{1+t+\cdots+t^{d-1}}{(1-t)^{n-1}}.$$

Hence $d_{\text{Hilb}}(R/I) = n - 1$.

3. Hilbert Dimension of Local rings

Let A be a noetherian local ring with maximal ideal $\mathfrak{m}$. Consider the associated graded ring

$$B = G_{\mathfrak{m}}(A) = \bigoplus_{n=0}^{\infty} \mathfrak{m}^n/\mathfrak{m}^{n+1}.$$

Then $B_0 = A/\mathfrak{m}$ is a field and $B_n = \mathfrak{m}^n/\mathfrak{m}^{n+1}$ are finite dimensional B_0 vector spaces.

Definition 10: Let A be a noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field $k = A/\mathfrak{m}$. Let $\lambda(V) = \dim_k(V)$ for finite dimensional k vector spaces. Then we define the Hilbert dimension of A to be

$$d_{\text{Hilb}}(A) = d_{\text{Hilb},\lambda}(G_{\mathfrak{m}}(A)).$$

If $\mathfrak{q} \subset A$ is an $\mathfrak{m}$-primary ideal, then since A is noetherian, it is easy to see that $\mathfrak{m}^{n+1} \subset \mathfrak{q} \subset \mathfrak{m}^n$ for some $n > 0$ and thus $A/\mathfrak{q}$ is an artinian local ring by Proposition 9 in the lecture on artinian rings. Recall that by Exercise (iii), finitely generated $A/\mathfrak{q}$ modules are thus of finite length. Let λ be the additive function length on finitely generated $A/\mathfrak{q}$ modules. Note that when $\mathfrak{q} = \mathfrak{m}$, length coincides with dimension.

By Proposition 2 in the lecture on associated graded rings, $B = G_{\mathfrak{q}}(A)$ is a noetherian ring and thus a finitely generated algebra over $B_0 = A/\mathfrak{q}$. If M is a finitely generated A module then

$(\mathfrak{q}^n M)_{n\geq 0}$ is a stable $\mathfrak{q}$-filtration of M and the associated graded module

$$G(M) = \mathfrak{q}^n M/\mathfrak{q}^{n+1}M$$

is a finitely generated graded $G_{\mathfrak{q}}(A)$ algebra. Thus each $\mathfrak{q}^n M/\mathfrak{q}^{n+1}M$ is a finitely generated A/q algebra.

We want to show that $d_{\text{Hilb}}(A) = d_{\text{Hilb},\lambda}(G_{\mathfrak{m}}(A)) = d_{\text{Hilb},\lambda}(G_{\mathfrak{q}}(A))$.

Proposition 11. Let A be a noetherian local ring with maximal ideal $\mathfrak{m}$ and $\mathfrak{m}$-primary ideal $\mathfrak{q}$. Let M be a finitely generated A module. Then:

(a) The A module $M/\mathfrak{q}^n M$ has finite length ,
(b) There is a polynomial $\chi_{\mathfrak{q}}^M(t) \in \mathbb{Q}[t]$ and an integer $N \geq 0$ such that for $n > N$,

$$l(M/\mathfrak{q}^n M) = \chi_{\mathfrak{q}}^M(n).$$

Moreover if s is the least number of generators of q then $\deg \chi_{\mathfrak{q}}^M \leq s$.

Proof. Part (a): Since each $\mathfrak{q}^n M/\mathfrak{q}^{n+1}M$ is finitely generated A module annihilated by $\mathfrak{q}$ hence it is a finitely generated module over the artinian ring $A/\mathfrak{q}$ hence has finite length. Since $M/\mathfrak{q}^n M \supset \mathfrak{q}M/\mathfrak{q}^n M \supset \ldots \supset \mathfrak{q}^{n-1}M/\mathfrak{q}^n M \supset 0$ and the successive quotients are all of finite length we can prove by induction that $M/\mathfrak{q}^n M$ is of finite length and

$$l_n = l(M/\mathfrak{q}^n M) = l(M/\mathfrak{q}M) + l(\mathfrak{q}M/\mathfrak{q}^2 M) + \ldots + l(\mathfrak{q}^{n-1}M/\mathfrak{q}^n M).$$

Part (b): Let $x_2, \ldots, x_s$ generate q, then the images $\overline{x}_i \in \mathfrak{q}/\mathfrak{q}^2$ generate $G_{\mathfrak{q}}(A)$ as a A/q algebra. These generators are all homogeneous of degree 1, thus by Corollary 9, there is some integer $N \geq 0$ such that

$$l(\mathfrak{q}^n M/\mathfrak{q}^{n+1}M) = H_{G_{\mathfrak{q}}(A)}(n) \text{ for } n \geq N.$$

Moreover $\deg H_{G_{\mathfrak{q}}(A)}(t) \leq s-1$. Let $H_{G_{\mathfrak{q}}(A)}(t) = a_0 + a_1 t + \ldots + a_{s-1}t^{s-1}$ (we are not claiming that $a_{s-1} \neq 0$). Now since

$$l_{n+1} - l_n = H_{G_{\mathfrak{q}}(A)}(n), \text{ for } n \geq N$$

for any $n \geq N$ we have

$$\begin{aligned} l_n &= l_N + H_{G_{\mathfrak{q}}(A)}(N) + \ldots + H_{G_{\mathfrak{q}}(A)}(n-1) \\ &= r + \sum_{k=0}^{n-1} H_{G_{\mathfrak{q}}(A)}(k) \qquad \text{(for some integer } r\text{)} \\ &= r + a_0 n + a_1 \sum_{k=0}^{n-1} k + \ldots + a_{s-1} \sum_{k=0}^{n-1} k^{s-1}. \end{aligned}$$

The expression

$$\chi_{\mathfrak{q}}^M(n) = r + a_0 n + a_1 \sum_{k=0}^{n-1} k + \ldots + a_{s-1} \sum_{k=0}^{n-1} k^{s-1}$$

is a polynomial in n of degree at most s since a_{s-1} may be 0 and $l(M/\mathfrak{q}^n M) = \mathfrak{q}^M(n)$ for $n \geq N$. □

Remark. For any positive integer k the sum of the k-th powers of the first $n-1$ positive integers is a polynomial function of n of degree $k+1$. This was shown by Bernoulli who also found the polynomial explicitly:

$$1^k + \ldots + n^k = \frac{1}{k+1}\sum_{j=0}^{k}\binom{k+1}{j}B_j n^{k+1-j},$$

where B_j is the j-th Bernoulli number. See for instance `https://www.isibang.ac.in/~sury/bernoullizeta.pdf` for a proof.

Definition 12: With the notation of Proposition 11 if $M = A$ then $\chi_{\mathfrak{q}}^A$ is called the characteristic polynomial of $\mathfrak{q}$.

Corollary 13. Let A be a noetherian local ring with maximal ideal $\mathfrak{m}$ and $\mathfrak{q}$ is an $\mathfrak{m}$-primary ideal. Then $A/\mathfrak{q}^n$ has finite length and there is a polynomial $\chi_{\mathfrak{q}}^A \in \mathbb{Q}[t]$ and an integer $N \geq 0$ such that

$$l(A/\mathfrak{q}^n) = \chi_{\mathfrak{q}}^A(n) \quad \text{for all } n \geq N.$$

Moreover if s is the least number of generators of $\mathfrak{q}$ then $\deg \chi_{\mathfrak{q}}^A \leq s$.

The next proposition says that the degree of $\chi_{\mathfrak{q}}^A$ is the same for all $\mathfrak{m}$-primary ideals $\mathfrak{q}$ and is equal to the Hilbert dimension of A.

Proposition 14. With the notation as in Corollary 13 we have

$$\deg \chi_{\mathfrak{q}}^A = \deg \chi_{\mathfrak{m}}^A = d_{\mathrm{Hilb}}(A).$$

Proof. We have $m \supset \mathfrak{q} \supset \mathfrak{m}^r$ for some $r > 0$, hence for all $n > 0$ $\mathfrak{m}^n \supset \mathfrak{q}^n \supset \mathfrak{m}^{rn} \Rightarrow A/\mathfrak{m}^n \subset A/\mathfrak{q}^n \subset A/\mathfrak{m}^{rn}$. Hence $\chi_{\mathfrak{m}}^A(n) \leq \chi_{\mathfrak{q}}^A(n) \leq \chi_{\mathfrak{m}}^A(rn)$ for all n sufficiently large.

Thus $\deg \chi_{\mathfrak{m}}^A \leq \deg \chi_{\mathfrak{q}}^A$, however $\deg \chi_{\mathfrak{m}}^A(rt) = \deg \chi_{\mathfrak{m}}^A$ since r is a constant, so $\deg \chi_{\mathfrak{q}}^A \leq \deg \deg \chi_{\mathfrak{m}}^A$.

From the proofs of Corollary 9 and Proposition 11 it is clear that $\deg \chi_{\mathfrak{m}}^A = d_{\mathrm{Hilb}}(G_{\mathfrak{m}}(A)) = d_{\mathrm{Hilb}}(A)$. □

Remark. For a slightly different treatment of Hilbert polynomials you refer to *Algebraic Geometry*, by Robin Hartshorne, Chapter 1, Section 7.