# Lect. 20 Hilbert functions.

**Def** $R$ graded if $R = \bigoplus_{n \geq 0} R_n$, $R_m R_n \subseteq R_{m+n}$.

E.g. $R_0[x]$ is graded with $\deg x = 1$, and similarly $R_0[x_1, x_2, \ldots]$.

$R_0$ is a subring.

**L.** $1 \in R_0$.

**Pf.** Let $1 = \sum x_m$, $x_m \in R_m$. $\forall z \in R$
$z = \sum z_n$, $z_n \in R_n$. Fix $n$. $z_n = 1 \cdot z_n = \sum x_m z_n$
$x_m z_n \in R_{m+n}$. So $\sum_{m>0} x_m z_n = z_n - x_0 z_n \in R_n$.
Hence $x_m z_n = 0$ for $m > 0$.
But $n$ is arbitrary. So $x_m z = 0$ $\forall m > 0$.
But $z$ is arbitrary. So taking $z = 1$ get
$x_m = x_m \cdot 1 = 0$ $\forall m > 0$. So $1 = x_0 \in R_0$.

$M$ an $R$-mod.

**Def.** $M$ (compatibly) graded if $\exists$ additive subgroups $M_n$ s.t. $M = \bigoplus_{n \in \mathbb{Z}} M_n$, $R_m M_n \subseteq M_{m+n}$.
$M_n$ = $n$-th homogeneous component. its elements are said to be homogeneous. Clearly, $M_n$ is an $R_0$-module.

Let $M(m) = \bigoplus_n M_{m+n}$, the same module with shifted grading: $M(m)_n = M_{m+n}$.

**L.** $R$ a graded ring, $M$ a graded $R$-module. If $R$ is a f.g. $R_0$-algebra and $M$ a f.g. $R$-module, then each $M_n$ is a f.g. $R_0$-module.

**Pf.** We can assume generators are homog. in pos. degree. Then have only finitely many monomials in each degree. Also can assume that generators of $M$ are homog. This implies the statement.

**Hilbert functions.** Assume $R_0$ is Artinian, $R$ a f.g. $R_0$-algebra, $M$ a f.g. $R$-module. Then by Lemma $M_n$ is a f.g. $R_0$-module by the above, so of finite length $\ell(M_n)$ by the prev. lecture. We call $n \to \ell(M_n)$ the *Hilbert function* of $M$, and its generating function

$$H(M,t) = \sum_{n \in \mathbb{Z}} \ell(M_n)\, t^n$$

the *Hilbert series* of $M$.

We will show later that this series is a rational function.

If $R = R_0[x_1, \dots, x_r]$ with $x_i \in R_1$ then by a result below, the Hilbert function is, for $n \gg 0$, a polynomial $h(M,n)$, called the Hilbert polynomial of $M$.

Ex: $R = R_0[X_1, \dots, X_r]$ polyn. ring, graded by degree. Then $R_n$ is free over $R_0$ on the monomials of degree $n$, so of rank $\binom{r-1+n}{r-1}$.

Ass. $R_0$ is Artinian. Then $\ell(R_n) = \ell(R_0)\binom{r-1+n}{r-1}$ by additivity of length. Thus the Hilb. fn. is a polyn. of degree $r-1$.

So $H(R,t) = \dfrac{\ell(R_0)}{(1-t)^r}$.

Thm. (Hilbert-Serre). Let $R = \bigoplus R_n$ be a graded ring, and let $M = \bigoplus M_n$ a graded $R$-module. Assume $R_0$ is Artinian, $R$ f.g. $R_0$-alg, $M$ f.g. $R$-module. Then

$$H(M,t) = \frac{e(t)}{t^{\ell}(1-t^{k_1})\cdots(1-t^{k_r})},$$

where $e(t) \in \mathbb{Z}[t]$, $\ell \geq 0$, $k_1, \dots, k_r \geq 1$.

Pf. Say $R = R_0[x_1, \dots, x_r]$, $x_i \in R_{k_i}$.
First assume $r=0$. Say $M$ is generated over

$R$ by $m_1, \dots, m_s$ with $m_i \in M_{l_i}$. Then $R = R_0$.
So $M_n = 0$ for $n < l_0 = \min(l_i)$ and for $n > \max(l_i)$. So $t^{l_0} H(M, t)$ is a polyn.

Next, assume $r \geq 1$ and form an exact sequence

$$0 \to K \to M(-k_1) \xrightarrow{\mu_{x_1}} M \to L \to 0.$$

Where $\mu_{x_1}$ is mult. by $x_1$. Since $x_1 \in R_{k_1}$, the grading on $M$ induces a grading on $K$ and on $L$. Further, $\mu_{x_1}$ acts as $0$ on both $K$ and $L$.

As $R_0$ is Artinian, $R_0$ is Noetherian. So since $R$ is a f.g. $R_0$-algebra, $R$ is Noetherian. Since $M$ is a f.g. module, so is $M(-k_1)$, so $K, L$ are f.g.
Let $R' = R_0[x_2, \dots, x_r]$. Since $x_1$ acts as $0$ on $K$ and $L$, they are f.g. $R'$-modules. So $H(K,t)$, $H(L,t)$ can be written in the desired form by induction in $r$.
So we get

$$(1 - t^{k_1}) H(M,t) = H(L,t) - H(K,t)$$
$$= \frac{e(t)}{t^l (1-t^{k_2}) \cdots (1 - t^{k_r})} \quad \square.$$

Corollary. Let $R = R_0[x_1, \dots, x_r]$, $x_i \in R_1$. Assume $M \neq 0$. Then $H(M,t)$ can be written uniquely in the form

$$H(M,t) = \frac{e(t)}{t^{\ell}(1-t)^d},$$

where $e(t) \in \mathbb{Z}[t]$ and $e(0), e(1) \neq 0$, $\ell \in \mathbb{Z}$, $r \geq d \geq 0$. Also $\exists$ a polyn. $h(M,n) \in \mathbb{Q}[n]$ of degree $d-1$, leading coe. $\frac{e(1)}{(d-1)!}$, and $\ell(M_n) = h(M,n)$, $n \geq \deg(e(t)) - \ell$

Pf. Take $k_i = 1$ in the above thm. Thus $H(M,t)$ has the form $\frac{e(t)(1-t)^s}{t^{\ell}(1-t)^r}$ with $e(0) \neq 0$, $e(1) \neq 0$, $\ell \in \mathbb{Z}$. Set $d = r - s$. Then $d \geq 0$ since $H(M,1) > 0$ as $M \neq 0$. So $H$ has the asserted form.

Let $e(t) = \sum_{i=0}^{N} e_i t^i$. Now $(1-t)^{-d} = \sum \binom{-d}{n} (-t)^n$ $= \sum \binom{d-1+n}{d-1} t^n$. So

$$\ell(M_n) = \sum_{i=0}^{N} e_i \binom{d-1+n+\ell-i}{d-1} \quad \text{for } n+\ell \geq N.$$

But $\binom{d-1+n-i}{d-1} = \frac{n^{d-1}}{(d-1)!} + \cdots$, which implies the statement.

<u>Filtrations</u> $R \supset q$, A ~~stable~~ <u>$q$-filtr.</u> on $M/R$:

$M \supset \cdots \supset F^n M \supset F^{n+1} M \supset \cdots$ $q M_i \subseteq M_{i+1}$.

<u>Stable $q$-filtr</u>: $M = F^n M$ $n \ll 0$,

$q F^n M = F^{n+1} M$, $n \gg 0$. I.e. $\exists \mu, \nu$,

$M = F^{\mu}$, $q^n F^{\nu} M = F^{\nu+n} M$ for $n \geq 0$.

E.g. $q$-adic filtr: $M = F^n M$ if $n \leq 0$,

$F^i M = q^i M$ if $i > 0$.

The $q$-adic filtration on $R$ yields a graded ring $G^{\cdot} R$

$$G^{\cdot} R = \bigoplus_{n \geq 0} G^n R \quad , \quad G^n R = q^n / q^{n+1}.$$

Also can define $G^{\cdot} M = \bigoplus G^n M$,

$G^n M = F^n M / F^{n+1} M$

If this is a $q$-filtration then $G^{\cdot} M$ is an $R/q$-module.

$M[m]$ – shift of filtration

$F^i M[m] = F^{i+m} M$

So $G^n M[m] = G^{n+m} M = (G^n M)(m)$.

If $M/F^m M$ have finite length, call $n \mapsto \ell(M/F^n M)$ the Hilbert–Samuel

function, and call the generating function
$$P(F^\cdot M, t) = \sum_{n \geq 0} \ell(M/F^n M)\, t^n$$
the Hilbert-Samuel series.

If the function $n \mapsto \ell(M/F^n M)$ is, for $n \gg 0$, a polyn. $p(F^\cdot M, n)$, then call it the Hilbert-Samuel polynomial.

If this is the $q$-adic filtration, call $P(F^\cdot M, t)$ ~~als~~ and ~~as~~ $p(F^\cdot M, n)$ as $P_q(M,t)$, $p_q(M,n)$.

<u>L.</u> $R$ Noetherian, $q \subset R$ an ideal, $M$ a f.g. module with a stable $q$-filtration. Then $G^\cdot R$ is generated as an $R/q$-algebra by fin. many elements of $q/q^2$, and $G^\cdot M$ is a f.g. $G^\cdot R$-module.

<u>Pf.</u> $R$ Noetherian $\Rightarrow$ $q$ is a f.g. ideal, say, by $x_1, \dots, x_r$. Then clearly the residues of the $x_i$ in $q/q^2$ generate $G^\cdot R$ as an $R/q$-algebra. By stability, $\exists\, \mu, \nu$ with $F^\mu M = M$ and $q^n F^\nu M = F^{\nu+n} M$ for $n \geq 0$. Hence $G^\cdot M$ is generated by

$F^{\mu}M/F^{\mu+1}M, \ldots, F^{\nu}M/F^{\nu+1}M$ over $G^{\cdot}R$.
But $R$ is Noetherian and $M$ f.g/$R$.
So each $F^{n}M/F^{n+1}M$ is f.g. over $R/q$.
(as $F^{n}M$ is f.g. over $R$). So $G^{\cdot}M$ is
a f.g. $G^{\cdot}R$-module. □

<u>Thm.</u> (Samuel). $R$ Noetherian, $q$ an ideal,
$M$ a f.g. module with a stable $q$-filtr. $F^{\cdot}M$.
Assume $\ell(M/qM) < \infty$. Then $\ell(F^{n}M/F^{n+1}M) < \infty$
and $\ell(M/q^{n}M) < \infty$ $\forall n \geq 0$; further,

$$P(F^{\cdot}M, t) = H(G^{\cdot}M, t)\frac{t}{1-t}.$$

<u>Pf.</u> Let $\mathfrak{a} = \mathrm{Ann}\, M$, $R' = R/\mathfrak{a}$, $q' = \mathfrak{a}+q/\mathfrak{a}$.
Then $R'$ is Noetherian, and $M$ a f.g. $R'$-mod,
$F^{\cdot}M$ a stable $q'$-filtr. So $G^{\cdot}R'$ is gen. as an
$R'/q'$ alg. by fin. many elts of deg 1,
and $G^{\cdot}M$ is a f.g. $G^{\cdot}R'$-module.
So $F^{n}M/F^{n+1}M$ is a f.g. $R'/q'$-module
by the above.

Now, $V(\mathfrak{a}+q) = V(\mathfrak{a}) \cap V(q) = \mathrm{Supp}\, M \cap V(q)$
$= \mathrm{Supp}(M/qM)$. Hence, $V(\mathfrak{a}+q)$ consists
entirely of max. ideals

Since $\ell(M/qM) < \infty$. So $\dim(R'/q') = 0$.
But $R'/q'$ is Noetherian. So $R'/q'$ is Artinian by the Akizuki-Hopkins thm.
Thus, $\ell(F^nM/F^{n+1}M) < \infty$ $\forall n$, so $\ell(M/F^{n}M) < \infty$ $\forall n$, as

$$\ell(F^nM/F^{n-1}M) = \ell(M/F^{n+1}M) - \ell(M/F^nM).$$

This implies the Hilbert-Samuel series f-la by taking generating functions.

<u>Cor.</u> Assume $q$ is generated by $r$ elements and $M \neq 0$. Then $P(F^{\cdot}M, t)$ can be written uniquely as

$$P(F^{\cdot}M, t) = \frac{e(t)}{t^{\ell-1}(1-t)^{d+1}}$$

with $e(t) \in \mathbb{Z}[t]$, $e(0), e(1) \neq 0$, $\ell \in \mathbb{Z}$, $r \geq d \geq 0$.
Also there is a polynomial $p(F^{\cdot}M, n) \in \mathbb{Q}[n]$ with degree $d$ and leading coeff. $e(1)/d!$ such that $\ell(M/F^nM) = p(F^{\cdot}M, n)$ for $n \geq \deg e(t) - \ell + 1$.
Finally, $P_q(M, n) - p(F^{\cdot}M, n)$ is a polynomial with degree $\leq d-1$ and positive leading coeff.
also $d$ and $e(1)$ are the same for every $q$-filtration.

<u>Pf.</u> This follows from previous results on the Hilbert series.

Finally, if $F^{\cdot}M$ is a stable $q$-filtration, then there is an $m$ s.t.

$$F^nM \supset q^nM \supset q^nF^mM = F^{n+m}M$$

for all $n \geq 0$. So we get

$$\ell(M/F^nM) \leq \ell(M/q^nM) \leq \ell(M/F^{n+m}M) \Rightarrow$$

$$P(F^{\cdot}M, n) \leq P_q(M,n) \leq P_q(F^{\cdot}M, n+m).$$

The two extremes are polynomials with the same degree $d$ and the same leading coefficient $c$, where $c = \frac{e(1)}{d!}$

Dividing by $n^d$ and letting $n \to \infty$, we conclude that the polynomial $P_q(M,n)$ also has degree $d$ and leading coeff. $c$.

Thus degree and leading coeff. are the same for any stable $q$-filtr.

Also $P_q(M,n) - p(F^{\cdot}M, n)$ has degree $\leq d-1$ and leading coef. $\geq 0$. D.

---

Rees Algebras. $R$ a ring, $q$ an ideal.

The sum $\mathcal{R}(q) = \bigoplus_{n \in \mathbb{Z}} \mathcal{R}_n(q)$, $\mathcal{R}_n(q) = \begin{cases} R, & n \leq 0 \\ q^n, & n \geq 0 \end{cases}$

is canonically an algebra, known as the extended Rees algebra of $q$.

Let $M$ be a module with a $q$-filtr. $F^{\cdot}M$.

Then can define

$$\mathcal{R}(F^{\cdot}M) = \bigoplus_{n \in \mathbb{Z}} F^nM$$

an $R(q)$-module called the Rees module of $M$.

<u>Lemma</u>. Let $R$ be Noetherian, $q \subset R$ an ideal, $M$ a f.g. module with a $q$-filtration $F^\bullet M$. Then $R(q)$ is algebra finite over $R$.
Also $F^\bullet M$ is stable $\Longleftrightarrow$ $R(F^\bullet M)$ is module finite over $R(q)$ and $\bigcup_{n \in \mathbb{Z}} F^n M = M$.

<u>Pf.</u> As $R$ is Noetherian, $q$ is fin.gen, say, by $x_1, .., x_r$. View $x_i$ as in $R_1(q)$ and $1 \in R$ as in $R^{-1}(q)$. These $r+1$ elements generate $R(q)$ over $R$.

Supp $F^\bullet M$ is stable, say $F^\mu M = M$ and $q^n F^\nu M = F^{n+\nu} M$ for $n > 0$. Then $\bigcup F^n M = M$. Als $R(F^\bullet M)$ is generated by $F^\mu M, .., F^\nu M$ over $R(q)$. But $R$ is Noeth and $M$ is f.g$/R$. So each $F^n M$ is f.g.$/R$. So $R(F^\bullet M)$ is a f.g. $R(q)$-module.

Conversely, supp. $R(F^\bullet M)$ is f.gen., over $R(q)$ by $m_1, .., m_s$. Say $m_i = \sum_{j=\mu}^{\nu} m_{ij}$, $m_{ij} \in F^j M$ for some $\mu \leq \nu$ (indep. of $i$). Then $\forall n$, any $m \in F^n M$ can be written as $m = \sum f_{ij} m_{ij}$ with $f_{ij} \in R_{n-j}(q)$. So if $n \leq \mu$, $F^n M \subset F^\mu M$.
Supp. $\bigcup F^n M = M$. Then $F^\mu M = M$. But if $j \leq \nu \leq n$ then $f_{ij} \in q^{n-j} = q^{n-\nu} q^{\nu - j}$. So $q^{n-\nu} F^\nu M = F^n M \Rightarrow F$ is $q$-stable

<u>Lemma.</u> (Artin-Rees). $R$ Noetherian, $M$ a f.gen. module, $N$ a submodule, $q$ an ideal, $F^\bullet M$ stable $q$-filtr. Set $F^nN = N \cap F^nM \; \forall n \in \mathbb{Z}$. Then $F^nM$ is a stable $q$-filtr.

<u>Pf.</u> Consider the extended Rees algebra $\mathcal{R}(q)$. It is fin.gen/$R$, so by the Hilbert basis thm it is Noetherian. Thus, $R(F^\bullet M)$ is f.g / $\mathcal{R}(q)$ by the above, so Noetherian. Clearly, $F^\bullet N$ is a $q$-filtration. So $\mathcal{R}(F^\bullet N)$ is a submodule of $\mathcal{R}(F^\bullet M)$ so f.gen. But $\bigcup F^nM = M$, so $\bigcup F^nN = N$. Thus $F^\bullet N$ is stable by the above. $\square$.

<u>Prop.</u> Let $R$ be a Noetherian ring, $q$ an ideal, $0 \to M' \to M \to M'' \to 0$ an exact sequence of f.gen. modules. Then $M/qM$ has finite length iff $M'/qM'$ and $M''/qM''$ have finite length. If so, then the polynomial
$$P_q(M',n) - P_q(M,n) + P_q(M'',n)$$
has degree at most $\deg P_q(M,n) - 1$ and has positive leading coefficient. Also then
$$\deg P_q(M,n) = \max(\deg P_q(M',n), \deg P_q(M'',n)).$$

Pf. $\operatorname{Supp} M/qM = \operatorname{Supp} M \cap V(q) = (\operatorname{Supp} M' \cup \operatorname{Supp} M'') \cap V(q)$
$= \operatorname{Supp} M' \cap V(q) \quad \cup \operatorname{Supp} M'' \cap V(q) =$
$= \operatorname{Supp}(M'/qM') \cup \operatorname{Supp}(M''/qM'')$

So $M/qM$ has finite length $\Leftrightarrow$ $M'/qM'$ and $M''/qM''$ do.

For $n \in \mathbb{Z}$, set $F^nM' = M' \cap q^nM$
Then by the Artin-Rees lemma, $F^nM'$ is a stable $q$-filtration. We have a comm. diagr.

$$\begin{tikzcd} 0 \arrow[r] & F^nM' \arrow[r] \arrow[d] & q^nM \arrow[r] \arrow[d] & q^nM'' \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & M' \arrow[r] & M \arrow[r] & M'' \arrow[r] & 0 \end{tikzcd}$$

with exact rows. So the Nine lemma gives an exact sequence

$$0 \to M'/F^nM' \to M/q^nM \to M''/q^nM'' \to 0$$

Assume $M/qM$ has finite length.
Then
$$p(F^\cdot M', n) - P_q(M, n) + P_q(M'', n) = 0.$$

So $P_q(M', n) - P_q(M, n) + P_q(M'', n) = P_q(M', n) - p(F^\cdot M', n)$

But it was shown above that the latter has degree at most $P_q(M', n) - 1$ and positive leading coeff.

Finally, $\deg p_q(M,n) = \max(\deg p(F^\circ M';n), \deg p_q(M'';n))$ by the above identity, as the leading coef of $p(F^\circ M';n)$ and $p(M'';n)$ are both positive, so cannot cancel. But $\deg p(F^\circ M';n) = \deg p_q(M';n)$ by the above, completing the proof.