1 Hilbert function

1.1 Graded rings

Let G be a commutative semigroup. A commutative ring R is called *G-graded* when it has a (weak) direct sum decomposition $R = \sum_{i \in G} R_i$ (that is, the R_i are additive subgroups, and every element r of R can be written in a unique way as finite sum $r = r_1 + ... + r_m$ where the r_j are nonzero and belong to distinct R_i) and moreover $R_i R_j \subseteq R_{i+j}$.

Elements that belong to one of the R_i are called *homogeneous*. The r_j that occur in the unique representation of r are called the *homogeneous components* of r.

Exercise *Give an example of a graded commutative ring R that has an identity element 1 that is not homogeneous. Show that this cannot happen when R is $\mathbf{N}$-graded.*

Now let G be a commutative monoid. A commutative ring R with identity 1 is called *G-graded* when it is G-graded as commutative ring, and moreover $1 \in R_0$, where 0 is the zero element of G.

Clearly, if H is a monoid containing G, and R is G-graded, then R is also H-graded.

Example A polynomial ring $R = k[x_1, ..., x_m]$ is $\mathbf{N}$-graded (and therefore also $\mathbf{Z}$-graded): Take for R_i the set of all polynomials that are homogeneous of total degree i. It is also $\mathbf{N}^m$-graded: Take for R_i the set of all polynomials that are homogeneous of multidegree i.

1.2 Graded modules

Let R be G-graded, and let H be a monoid containing G. An R-module M is called *H-graded* when it has a (weak) direct sum decomposition $M = \sum_{i \in H} M_i$ such that $R_i M_j \subseteq M_{i+j}$.

For example, it is natural to work with $\mathbf{N}$-graded rings and $\mathbf{Z}$-graded modules. Or perhaps $\mathbf{N}^n$-graded rings and $\mathbf{Z}^n$-graded modules.

An important special case of a graded R-module, is R itself, but with shifted grading: put $M = R$ and $M_j = R_{h+j}$. Let us call this module $R^{(h)}$.

A submodule N of M is called a graded submodule when it is generated by the intersections $N_i = N \cap M_i$. (Then it is called *homogeneous*.) If this is the case, then the quotient module M/N is graded, with grading $(M/N)_i = M_i/N_i$.

Example In $k[x, y, z]$ the ideal $(x^2 + y^3 + z^5)$ will be homogeneous if we choose the grading that assigns degrees 15, 10, 6 to x, y, z, respectively.

1.3 Hilbert function

Consider the situation of a G-graded k-algebra R: all R_i are vector spaces over k. Given an H-graded R-module M, put

$$F(M, \lambda) = \sum_{i \in H} H(M, i) \lambda^i$$

where $H(M, i) = \dim_k M_i$.

The function $H(M, .)$ from H to $\mathbf{N}$ is called the *Hilbert function* of M.

Theorem 1.1 *Suppose R is finitely generated by homogeneous elements r_1, ..., r_s of degrees g_1, ..., g_s, respectively. If M is finitely generated H-graded R-module, where H is an additive group, then*

$$F(M, \lambda) = \frac{P(M, \lambda)}{\prod_{j=1}^{s}(1 - \lambda^{g_j})}$$

for some finite sum $P(M, \lambda) = \sum_h a_h \lambda^h$ with integral coefficients a_h.

Proof: Induction on the number s of generators of the k-algebra R. If $s = 0$, then $R = R_0 = k$, and $F(M, \lambda)$ has only finitely many terms.

If $s > 0$, then let r be one of the generators of R (of degree g, say). The module M/rM is a finitely generated S-module, where S is the subring of R generated by the generators different from r. By induction $F(M/rM, \lambda)$ has a representation of the required form.

Next, consider $K_r = \{m \in M \mid rm = 0\}$. Again, this is a finitely generated S-module, so $F(K_r, \lambda)$ has the required form.

Finally, all will be proved if we show that

$$F(M, \lambda) = \frac{F(M/rM, \lambda) - \lambda^g F(K_r, \lambda)}{1 - \lambda^g}$$

But that is the same as saying that

$$F(M, \lambda) - F(M/rM, \lambda) = \lambda^g (F(M, \lambda) - F(K_r, \lambda))$$

that is,

$$\dim(rM)_{j+g} = \dim(M)_j - \dim(K_r)_j$$

and that is clear (since $i + g = j + g$ implies $i = j$). □

1.4 Examples

Below, R will be $\mathbf{N}$-graded.

Consider $R = k$. We have $F(R, \lambda) = 1$.

Consider $R = k[x]$. We have $F(R, \lambda) = 1 + \lambda + \lambda^2 + ... = 1/(1 - \lambda)$.

Consider $R = k[x, y]$. We have $F(R, \lambda) = 1 + 2\lambda + 3\lambda^2 + 4\lambda^3 + ... = 1/(1 - \lambda)^2$.

And indeed, for $R = k[x_1, ..., x_m]$ we have $F(R, \lambda) = 1/(1 - \lambda)^m$.

Consider $R = k[x, y]/(xy)$. We have $F(R, \lambda) = 1 + 2\lambda + 2\lambda^2 + 2\lambda^3 + ... = (1 + \lambda)/(1 - \lambda)$.

Consider $R = k[x, y]/(x^2 + y^2)$. We have $F(R, \lambda) = 1 + 2\lambda + 2\lambda^2 + 2\lambda^3 + ... = (1 + \lambda)/(1 - \lambda)$.

1.5 Automated examples

When the rings are more complicated, it is easier to let a computer algebra package do the work. Fetch Macaulay from `http://www.math.uiuc.edu/Macaulay2`.

First repeat the above calculation. In the above the field k does not play any role. Let us take $k = \mathbf{F}_{101} = \mathbf{Z}/101\mathbf{Z}$.

```
% ./M2
Macaulay 2, version 0.9
i1 : R=ZZ/101[x,y]
o1 = R
o1 : PolynomialRing

i2 : Q=R/ideal(x^2+y^2)
o2 = Q
o2 : QuotientRing

i3 : poincare Q
             2
o3 = 1 - $T
o3 : ZZ[ZZ^1]
```

The output of the function `poincare` is the numerator of the righthand side fraction in the theorem above. So, $1-T^2$ really means $(1-T^2)/(1-T)^2$ since we have two variables, both of degree 1. And that is indeed the same as the $(1+T)/(1-T)$ that we found above.

1.6 Geometric significance

Given a projective variety X, with homogeneous coordinate ring $R = k[X_0, ..., X_m]/I(X)$, the dimension $H(R, i) = \dim R_i$ tells us how many independent functions of degree i there are on X.

That gives geometric information. For example, if X is a set of three points in the plane, then $H(R, 1)$ will be 2 if the three points are collinear, and 3 otherwise. On the other hand, $H(R, n)$ will be 3 for $n > 1$.

Let us confirm using Macaulay. We expect to find either $1+2\lambda+3\lambda^2+3\lambda^3+...$ or $1+3\lambda+3\lambda^2+3\lambda^3+...$, that is, either $(1+\lambda+\lambda^2)/(1-\lambda)$ or $(1+2\lambda)/(1-\lambda)$.

```
i1 : R=ZZ/101[x,y,z]
o1 = R
o1 : PolynomialRing

i2 : S=ideal(x,y)*ideal(x,z)*ideal(x,y+z)
             3   2     2    2               2   2      2                  2       2
o2 = ideal (x , x y + x z, x z, x*y*z + x*z , x y, x*y  + x*y*z, x*y*z, y z + y*z )
o2 : Ideal of R

i3 : T=radical S
                  2       2
o3 = ideal (x, y z + y*z )
o3 : Ideal of R

i4 : Q=R/T
o4 = Q
o4 : QuotientRing

i5 : poincare Q
```

```
                3     4
o5 = 1 - $T - $T  + $T
o5 : ZZ[ZZ^1]
```

That was the case of three collinear points, and we find $(1-T-T^3+T^4)/(1-T)^3 = (1+T+T^2)/(1-T)$, as expected. And for three non-collinear points:

```
...
i2 : S=ideal(x,y)*ideal(x,z)*ideal(y,z)
...
            2      3
o5 = 1 - 3$T  + 2$T
```

That is, we find $(1-3T^2+2T^3)/(1-T)^3 = (1+2T)/(1-T)$, as expected.

Exercise *Show that if X is a set of n points in projective space, then $H(R,i) = n$ for sufficiently large i. How large?*

1.7 The Hilbert polynomial

Consider $R = k[x_1, ..., x_m]/I(X)$ with $\mathbf{N}$-grading. Looking at the values that the Hilbert function $H(R,i)$ takes, we see that they are a bit messy for small i, and then are described by a polynomial in i for sufficiently large i. This polynomial is called the *Hilbert polynomial.*

The special case of Theorem 1.1 where $R = k[x_1, ..., x_m]/I$ and we use the $\mathbf{Z}$-grading where all x_i have degree 1, says for any finitely generated $\mathbf{Z}$-graded R-module that

$$F(M,\lambda) = \frac{P(M,\lambda)}{(1-\lambda)^m}$$

for some finite sum $P(M,\lambda) = \sum_h a_h \lambda^h$ with integral coefficients a_h.

Now $F(M,\lambda) = \sum_{i \geq i_0} H(M,i)\lambda^i$ and $1/(1-\lambda)^m = \sum_{j \geq 0} \binom{j+m-1}{m-1} \lambda^j$, so $F(M,\lambda) = \sum_{j \geq 0} \sum_h a_h \binom{j+m-1}{m-1} \lambda^{j+h}$ and

$$H(M,i) = \sum_{h \leq i} a_h \binom{i-h+m-1}{m-1}.$$

This shows that for sufficiently large i (namely, for $i \geq \max\{h | a_h \neq 0\}$) we have $H(M,i) = p(i)$, where $p(i)$ is the polynomial $p(i) = \sum_h a_h \binom{i-h+m-1}{m-1}$. This is the Hilbert polynomial.

We see that the leading coefficient of the Hilbert polynomial is $(\sum_h a_h)/(m-1)!$. If $\sum_h a_h = 0$, then $P(M,\lambda)$ has a factor $(1-\lambda)$ and we can first simplify the expression for $F(M,\lambda)$. This shows that if the Hilbert polynomial has degree d, then its leading coefficient $(\sum_h a_h)/d!$ is an integer divided by $d!$.

1.8 Properties of the Hilbert polynomial

The degree of the Hilbert polynomial is the dimension of X.

Thus, for a finite set the Hilbert polynomial will be a constant, namely the size of the set.

For a curve the Hilbert polynomial is linear, say of the form $ai + b$, and the value $1 - b$ is called the *arithmetic genus* of the curve.

A third invariant that can be read off from the Hilbert polynomial is the degree of the variety. If a projective variety X has dimension d and lives in $\mathbf{P}^m$ then a general linear subspace of dimension $m - d$ will hit X in finitely many points, and the number of points is called the *degree* of X. Now if X has degree c, the leading coefficient of the Hilbert polynomial will be $c/d!$.

Let us do an example. If X is a conic in the plane, then we expect to see dimension 1, genus 0, degree 2, so the Hilbert polynomial should be $2i + 1$. And for X given by $x^2 + y^2 = z^2$ we find Hilbert function $(1 - T^2)/(1 - T)^3 = 1 + 3T + 5T^2 + 7T^3 + ...$, indeed with Hilbert polynomial $2i + 1$.

Or, with X a cubic curve in the plane we expect dimension 1, genus 1, degree 3, so the Hilbert polynomial should be $3i$. And for X given by $x^3 + y^3 + z^3 = 0$ we find Hilbert function $(1-T^3)/(1-T)^3 = 1+3T+6T^2+9T^3+...$, as expected.

1.9 Dimension

Above we said that the degree of the Hilbert polynomial equals the dimension of the variety. Let us prove this for varieties embedded in a projective space $\mathbf{P}^n$.

As definition of dimension we use: a variety X embedded in $\mathbf{P}^n$ has dimension d when there is a linear subspace of projective dimension $n - d - 1$ in $\mathbf{P}^n$ disjoint from X while all linear subspaces of projective dimension $n - d$ meet X.

So, let U be a linear subspace of projective dimension $n - d - 1$ disjoint from X. The quotient space $\mathbf{P}^n/U$ is a projective space $\mathbf{P}^d$. We find a map $\pi : X \to \mathbf{P}^d$ by sending $x \in X$ to the $(n - d)$-space spanned by x and U. This map is onto, since no $(n-d)$-space is disjoint from X. Now π^* is an injection of $k[X_0, ..., X_d]$ into the coordinate ring R of X, so $H(R, i) \geq \binom{i+d}{d}$ for all i, and the Hilbert polynomial of X has degree not less than d.

Now conversely. This time we use as definition of dimension: the transcendence degree of its function field over k. (In the projective setting we can take as the function field the homogeneous part of degree 0 of the quotient field of R.)

Let S be the isomorphic image of $k[X_0, ..., X_d]$ in R. Now R is finitely generated as S-module because R and S have the same transcendence degree over k.

If R has generators y_j of degrees d_j over S, so that every element of R can be written in the form $\sum s_j y_j$ with $s_j \in S$, then we find a degree-preserving surjection $\oplus S^{(-d_j)} \to R$ given by $(s_j)_j \mapsto \sum s_j y_j$.

It follows that $H(R, i) \leq \sum \binom{i+d-d_j}{d}$, and the Hilbert polynomial of X has degree not larger than d. □