MAT 4200 Commutative algebra

Part 7, Dimension Theory (Chapt. 13, 15, 16)

October, 29, - November, 5, 2020

October, 29, 2020

We define Krull dimension of a ring.

13

Let A be a ring. We consider strictly ascending and finite chains $\{\mathfrak{p}_i\}$ of prime ideals

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_\nu$$

The integer ν is called **the length** of the chain; it is one less than the number of prime ideals.
The **Krull dimension** of A will be the supremum of the lengths of all such chains. It is denoted by $\dim(A)$.
A chain is said to be **saturated** if there are no prime ideals in A lying strictly between two of the terms.
It is **maximal** if additionally the chain cannot be lengthened, neither upwards nor downwards;

Proposition

Let A be a ring and $\mathfrak{p}$ a prime ideal. Then

$$dim(A_{\mathfrak{p}}) + dim(A/\mathfrak{p}) \leq dim(A).$$

Proof. Any chain $\{\mathfrak{p}_i\}$ of prime ideals in A may be broken in two at any stage, say at $\mathfrak{p} = \mathfrak{p}_\nu$, and thus be presented as the concatenation of a lower chain, formed by the members of the chain contained in $\mathfrak{p}$, and an upper chain, formed by those containing $\mathfrak{p}$. A chain thus split, appears as:

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_{\nu-1} \subset \mathfrak{p}_\nu = \mathfrak{p} \subset \mathfrak{p}_{\nu+1} \subset \ldots \subset \mathfrak{p}_n.$$

Now, the primes contained in $\mathfrak{p}$ are in a one-to-one correspondence with the prime ideals in the localization $A_{\mathfrak{p}}$, hence the lower chains correspond to chains in $A_{\mathfrak{p}}$. In similar a way, prime ideals containing $\mathfrak{p}$ correspond to prime ideals in the quotient $A/\mathfrak{p}$, hence the upper chains correspond to chains in $A/\mathfrak{p}$. □

Proposition

If $\{\mathfrak{p}_i\}$ *are the minimal primes of* A*, then* $dim(A) = \sup_i dim(A/\mathfrak{p}_i)$*.*

Proof. The intersection of the prime ideals in a chain being prime, any maximal chain starts at minimal prime. Furthermore, chains of prime ideals beginning at a prime $\mathfrak{p}$ are in a one-to-one correspondence with chains of prime ideals in $A/\mathfrak{p}$. $\square$

It is common usage to call $\dim(A_{\mathfrak{p}})$ the **the height** of $\mathfrak{p}$, or more generally for any ideal $\mathfrak{a}$ in A the heigh is the least height of any prime ideal containing $\mathfrak{a}$; that is

$$\mathrm{ht}(\mathfrak{a}) = \min_{\mathfrak{a}\subset\mathfrak{p}} \mathrm{ht}(\mathfrak{p}).$$

One speaks also about the **height of** $\mathfrak{p}$ *over* $\mathfrak{q}$ when $\mathfrak{q} \subset \mathfrak{p}$ are two primes. It equals the supremum of lengths of chains connecting $\mathfrak{q}$ to $\mathfrak{p}$; or equivalently to $\dim((A/\mathfrak{q})_{\mathfrak{p}})$.

Example

Let $A = k[x,y]$ with constituting relations $xy = y(y-1) = 0$. It is the coordinate ring of the algebraic subset V of $\mathbb{A}_k^2$ equal to the union of the x-axis and the point $(0,1)$. The primary decomposition of the zero ideal in A is given as $(0) = (y) \cap (x, y-1)$. Hence (y) and $(x, y-1)$ are the minimal prime ideals in A. Now, $(x-a, y)$ is a maximal ideal for any $a \in k$, so A possesses saturated chains

$$(y) \subset (x-a, y),$$

and therefore $dim(A) = 1$. On other hand $(x, y-1)$ is clearly a maximal ideal, and hence it is both maximal and minimal. So V, even though it is one-dimensional, has a component of dimension zero.

Proposition

Let $A \subset B$ be an integral extension of rings. Then $dim(A) = dim(B)$.

Proof. This is a direct consequence of the Going-Up theorems as formulated in the last section. Indeed, let $\{\mathfrak{q}_i\}$ be a chain of length ν in B and consider the prime ideals $\mathfrak{p}_i = \mathfrak{q}_i \cap A$. They form a chain in A whose length is ν since no two $\mathfrak{q}_i$'s intersect A in the same ideal according to Lying-over. This shows that $\dim B \leq \dim A$. On the other hand, by every chain in A has a chain in B lying over it, which means that $\dim B \leq \dim A$. □

Proposition

Let A be ring of finite Krull dimension and let $f \in A$ be an element not belonging to any minimal prime ideal in A, then $dim(A/(f)) < dim(A)$.

Proof. Chains of prime ideals in $A/(f)$ are in one-to-one correspondence with chains in A all whose members contain f. Moreover, a prime ideal $\mathfrak{p}$ that is minimal over (f), is by hypothesis not minimal in A, and therefore properly contains a minimal prime $\mathfrak{q}$ of A. Consequently any ascending chain in A emanating from $\mathfrak{p}$ can be lengthened downwards by appending $\mathfrak{q}$. □

With Krull's Principal Ideal Theorem in hand and with some additional conditions on A and f, we can in fact prove equality; $\dim(A/(f)) = \dim(A) - 1$.

Theorem (Krull's Principal Ideal Theorem)

Let A be a Noetherian ring and x an element from A. Assume that $\mathfrak{p}$ is a prime ideal in A which is minimal over (x). Then $ht(\mathfrak{p}) \leq 1$.

$$(x) \subseteq \mathfrak{p}$$

In the proof we are obliged to use the symbolic powers of a prime ideal $\mathfrak{q}$ in A as a substitute for the actual powers. The symbolic power $\mathfrak{q}^{(n)}$ is defined as $\mathfrak{q}^{(n)} = \mathfrak{q}^n A_\mathfrak{q} \cap A$ and that it has the virtue of being $\mathfrak{q}$-primary, which $\mathfrak{q}^n$ generally is not. But don't be panic-stricken by the appearance of these gizmos: A part from $\mathfrak{q}^{(n+1)}$ being contained in $\mathfrak{q}^{(n)}$, their only property we need is that from $cx \in \mathfrak{q}^{(n)}$, but $x \notin \mathfrak{q}$, follows that $c \in \mathfrak{q}^{(n)}$. Indeed, x is invertible in the localization $A_\mathfrak{q}$ as it does not lie in $\mathfrak{q}$, so $c \in \mathfrak{q}^n A_\mathfrak{q}$ follows from $cx \in \mathfrak{q}^n A_\mathfrak{q}$.

Proof.

1. We are to show that there are no chain of prime ideals of length two of shape $\mathfrak{q}' \subset \mathfrak{q} \subset \mathfrak{p}$. By passing to the quotient $A/\mathfrak{q}'$ and subsequently localizing in $\mathfrak{p}/\mathfrak{q}'$, we may assume that A is a local domain with maximal ideal $\mathfrak{p}$, and our task is to prove that if $\mathfrak{q} \subset \mathfrak{p}$, then $\mathfrak{q} = 0$.

2. The first observation is that, since $\mathfrak{p}$ is minimal over (x), the ring A/xA has only one prime ideal. Being Noetherian, it is Artinian, and we have the opportunity to activate the descending chain condition. The chain to exploit, is the descending chain $\{(x) + \mathfrak{q}^{(n)}\}_n$, where $\mathfrak{q}^{(n)}$ is the n-th symbolic power of $\mathfrak{q}$. The chain $\{(x) + \mathfrak{q}^{(n)}\}$ corresponds to the descending chain $\{((x) + \mathfrak{q}^{(n)})/(x)\}$ in A/xA and must eventually be stable as A/xA is Artinian. Hence there is an n so that

$$(x) + \mathfrak{q}^{(n+1)} = (x) + \mathfrak{q}^{(n)}.$$

□

Proof. [continue]

3. This entails that if $a \in \mathfrak{q}^{(n)}$, one may write $a = b + cx$ with $b \in \mathfrak{q}^{(n+1)}$, so that $cx \in \mathfrak{q}^{(n)}$. From this it follows that $c \in \mathfrak{q}^{(n)}$ since $x \notin \mathfrak{q}$, and consequently it holds true that $\mathfrak{q}^{(n)} \subset \mathfrak{q}^{(n+1)} + x\mathfrak{q}^{(n)} \subset \mathfrak{q}^{(n)}$. Nakayama's lemma yields that $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$. In its turn, this yields that $\mathfrak{q}^n A_{\mathfrak{q}} = \mathfrak{q}^{n+1} A_{\mathfrak{q}}$, and appealing once more to Nakayama's lemma, we may conclude that $\mathfrak{q} A_{\mathfrak{q}} = 0$; that is, $\mathfrak{q} = 0$.

$\square$

Proposition

Let A be a Noetherian ring and f an element that is not a unit and does not belong to any minimal prime of A. Then $dim(A/(f)) = dim(A) - 1$.

Proof. Let d be the dimension of $A/(f)$ and consider the inverse image

$$\mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_d$$

of a maximal chain in $A/(f)$. It holds that $(f) \subset \mathfrak{p}_0$ and $\mathfrak{p}_0$ is minimal over (f). Moreover, $\mathfrak{p}_0$ is of height at most one by Krull's Principal Ideal Theorem and it is not a minimal prime since f does not belong to any such. Hence $\mathrm{ht}(\mathfrak{p}_0) = 1$, and $\dim(A) = d + 1$. □

Theorem (The Height Theorem)

Let A be a Noetherian ring and let $\mathfrak{p}$ be a prime ideal minimal over an ideal $\mathfrak{a}$ generated by r elements. Then $ht(\mathfrak{p}) \leq r$.

Proof.

1. Let $\mathfrak{a} = (a_1, \ldots, a_r)$. The proof goes by induction on r, and heading for a contradiction, we assume that there is a chain $\{\mathfrak{p}_i\}$ in A of length $d > r$ ending at $\mathfrak{p}$.
2. Because $\mathfrak{a}$ is not contained in $\mathfrak{p}_{d-1}$, we may assume that a_1 does not lie in $\mathfrak{p}_{d-1}$, and so there is no prime lying properly between $(a_1) + \mathfrak{p}_{d-1}$ and $\mathfrak{p}$. The radical of $(a_1) + \mathfrak{p}_{d-1}$ therefore equals $\mathfrak{p}$, and a power of $\mathfrak{p}$ is contained in $(a_1) + \mathfrak{p}_{d-1}$. Since $\mathfrak{a} \subset \mathfrak{p}$ we may for ν sufficiently big, write
$$a_i^\nu = c_i a_1 + b_i$$
with $b_i \in \mathfrak{p}_{d-1}$, and we let $\mathfrak{b} = (b_2, \ldots, b_r)$. Then $\mathfrak{b}$ is contained in $\mathfrak{p}_{d-1}$.

Proof. [continue]

3. We contend that there is prime ideal $\mathfrak{q}$ lying between $\mathfrak{b}$ and $\mathfrak{p}_{d-1}$, properly contained in $\mathfrak{p}_{d-1}$; indeed, if $\mathfrak{p}_{d-1}$ were minimal over $\mathfrak{b}$, the height of $\mathfrak{p}_{d-1}$ would be at most $r-1$ by induction, but being next to the top in a chain of length d, the ideal $\mathfrak{p}_{d-1}$ is of height at least $d-1$, and $r-1<d-1$.

4. Now, the idea is to pass to the ring $A/\mathfrak{q}$. The ideal $\mathfrak{q}+(a_1)$ contains a power of $\mathfrak{a}$, hence there is no prime ideal between $\mathfrak{q}+(a_1)$ and $\mathfrak{p}$, which means that the ideal $\mathfrak{p}/\mathfrak{q}$ is minimal over the principal ideal $\mathfrak{q}+(a_1)/\mathfrak{q}$, and therefore of height one after the Principal Ideal Theorem, but there is also the chain $0 \subset \mathfrak{p}_{d-1}/\mathfrak{q} \subset \mathfrak{p}/\mathfrak{q}$. Contradiction.

□

Proposition

A local Noetherian ring is of finite Krull dimension bounded by the number of generators of the maximal ideal.

Proof. It ensues from the Height Theorem that any local Noetherian ring A has a finite Krull dimension. Indeed, the maximal ideal $\mathfrak{m}$ is finitely generated, and by the Height Theorem the height of $\mathfrak{m}$, which is the same as $\dim(A)$, is bounded by the number of generators. $\square$

Proposition

Let A be a Noetherian ring and let $\mathfrak{q} \subset \mathfrak{p}$ be two prime ideals. If there is a prime ideal lying strictly between $\mathfrak{p}$ and $\mathfrak{q}$, there will be infinitely many.

Proof. Assume there is a prime ideal strictly between $\mathfrak{p}$ and $\mathfrak{q}$ which means that the $\mathfrak{p}$ is of height at least two over $\mathfrak{q}$. If there were only finitely many prime ideals, say $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, lying strictly between $\mathfrak{p}$ and $\mathfrak{q}$, there would by prime avoidance be an element $x \in \mathfrak{p}$ not lying in any of the $\mathfrak{p}_i$ since by assumption $\mathfrak{p}$ is not contained in any of the $\mathfrak{p}_i$'s. Then $\mathfrak{p}$ would be minimal over $\mathfrak{q} + (x)$, and by the Principal Ideal Theorem $\mathfrak{p}$ would be of height one over $\mathfrak{q}$; contradiction. $\square$

Proposition (Dimension of Polynomial Rings)

Let k be a field. The Krull dimension of the polynomial ring $k[x_1, \dots, x_n]$ in n variables equals n; that is, $dim(k[x_1, \dots, x_n]) = n$.

Proof.

1. We can form a chain of prime ideals

$$(0) \subset (x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, x_2, \dots, x_n)$$

showing that the Krull dimension of $k[x_1, \dots, x_n]$ is at least n.

□

Proof.

2. Assume that
$$(0) \subset \mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \ldots \subset \mathfrak{p}_d$$
is a chain with $\mathfrak{p}_1$ minimal over (0). Pick a non-zero irreducible element f in $\mathfrak{p}_1$; because the polynomial ring is a UFD the ideal (f) is a prime and so $(f) = \mathfrak{p}_1$.
3. Consider the quotient algebra $A = k[x_1, \ldots, x_n]/(f)$. It is a domain, and since we have imposed a non-trivial condition on the variables, its fraction field is of transcendence degree at most $n-1$. By Noether's Normalization Lemma it follows that A is finite over a polynomial ring in at most $n-1$ variables, and hence by the Going–Up Theorem the dimension of A is at most $n-1$ as well.
4. Now, the chain induces a chain in A shaped like
$$(0) \subset \mathfrak{p}_2/\mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_d/\mathfrak{p}_1,$$
and it follows that $n-1 \geq \dim(A) \geq d-1$, and consequently it holds true that $\dim(k[x_1, \ldots, x_n]) \leq n$.

$\square$

Corollary

Let A be a domain finitely generated over the field k whose field of fractions is K. Then $dim(A) = tr.deg_k(K)$

Proof. If $n = \mathrm{tr.deg}_k(K)$, there is by Noether's Normalization Lemma a polynomial ring $k[x_1, \ldots, x_n] \subset A$ over which A is finite, hence $\dim(A) = \dim(k[x_1, \ldots, x_n]) = n$ by Going–Up III. □

Corollary

Let A be a domain finitely generated over the field k and let $f \in A$ be a non-zero element. Then $dim(A_f) = dim(A)$.

Proof. The algebra A_f is finitely generated over k and has the same fraction field as A. □

Lemma

Let k be a field and $f \in k[x_1, \dots, x_n]$ an irreducible polynomial. It then holds true that $dim(k[x_1, \dots, x_n]/(f)) = n - 1$.

Proof.

1. If K denotes the fraction field of $A = k[x_1, \dots, x_n]/(f)$, it will, according to the Corollary above be sufficient to see that $\mathrm{tr.deg}_k(K) = n - 1$.
2. The proof goes by induction on the number n of variables, the case $n = 1$ being trivial.
3. Assume first that the class of x_1 in A is algebraic over k. The minimal polynomial of x_1 is an irreducible polynomial $g(x_1)$ that lies in the ideal (f), and since f is irreducible, it ensues that f and g differ by a constant factor. Consequently f only depends on x_1. The remaining variables will then be algebraically independent in A since any irreducible polynomial inducing a relation among them would lie in (f), hence be a scalar multiple of f, which manifestly is absurd.

Proof.

4. In the case that x_1 is transcendental, the rational function field $k(x_1)$ is contained in K and, in fact, K is also the fraction field of $k(x_1)[x_2, \ldots, x_n]/(f)$. By induction $\operatorname{tr.deg}_{k(x_1)}(K) = n-2$, and since $\operatorname{tr.deg}_k(K) = \operatorname{tr.deg}_{k(x_1)}(K)+1$, we are through.

$\square$

November, 4, 2020

We introduce Hilbert functions and look at their basic properties.
But first we close our study of Krull dimension.

13, 15.1-15.2

The inclusion $A \hookrightarrow A[t]$ induces map

$$\pi : \mathrm{Spec}(A[t]) \to \mathrm{Spec}(A)$$

We are interested in the fibers of this map.

Proposition

Let A be a ring and let $\mathfrak{p} \subset A$ be a prime ideal. Denote by $K_{\mathfrak{p}}$ the fraction field of $A/\mathfrak{p}$. There is a one-to-one inclusion preserving correspondence between the lattice of primes in $A[t]$ contracting to $\mathfrak{p}$ and the lattice of prime ideals in the polynomial ring $K_{\mathfrak{p}}[t]$.

Lemma

Let A be a domain with fraction field K. Sending $\mathfrak{p}$ to $\mathfrak{p}K[t]$ sets up a one a one to one correspondence between non-zero prime ideals $\mathfrak{p}$ in $A[t]$ such that $\mathfrak{p} \cap A = 0$ and the non-zero prime ideals in $K[t]$.

Proof. Observe that $K[t]$ equals the localisation $S^{-1}A[t]$ where S is the multiplicative set $S = A \setminus \{0\}$. The lemma follows from the property of primes in localizations. □

Notice the following:

1. Each prime ideal $\mathfrak{p}$ in A gives rise to an ideal $\mathfrak{p}^+ = \mathfrak{p}A[t]$, which is formed by the polynomials $\sum_i a_i t^i$ having all coefficients in $\mathfrak{p}$ and such that $\mathfrak{p}^+ \cap A = \mathfrak{p}$.
2. Consider the map $A[t] \to A/\mathfrak{p} \otimes_A A[t]$. It is surjective with kernel $\mathfrak{p}A[t]$ and we have an isomorphism

$$A[t]/\mathfrak{p}A[t] \simeq A/\mathfrak{p} \otimes_A A[t] \simeq (A/\mathfrak{p})[t]$$

3. The ring $(A/\mathfrak{p})[t]$ is an integral domain, and the ideal $\mathfrak{p}^+$ is a prime ideal, contained in the fiber $\pi^{-1}(\mathfrak{p})$.

Proposition

Let A be a ring and let $\mathfrak{p} \subset A$ be a prime ideal. Denote by $K_{\mathfrak{p}}$ the fraction field of $A/\mathfrak{p}$. There is a one-to-one inclusion preserving correspondence between the lattice of primes in $A[t]$ contracting to $\mathfrak{p}$ and the lattice of prime ideals in the polynomial ring $K_{\mathfrak{p}}[t]$.

Proof. If $\mathfrak{q} \cap A = \mathfrak{p}$ it holds that $\mathfrak{p}^+ \subset \mathfrak{q}$. So prime ideals in $A[t]$ that intersects A in $\mathfrak{p}$ are in one-to-one correspondence with prime ideals in $A[t]/\mathfrak{p}A[t]$ whose intersection with $A/\mathfrak{p}$ is the zero-ideal.

Hence by replacing A by $A/\mathfrak{p}$ we place ourselves in the situation of the previous lemma. With the notation $K_{\mathfrak{p}}$ for the fraction field of $A/\mathfrak{p}$, the proposition follows. $\square$

Example

Consider the inclusion $\mathbb{C}[x] \subset \mathbb{C}[x,y]$*, whose geometric incarnation we denote by* $\pi : Spec(\mathbb{C}[x,y]) \to Spec(\mathbb{C}[x])$*. The maximal ideals in* $\mathbb{C}[x,y]$ *are of the form* $(x-a, y-b)$ *and constitute a* $\mathbb{C}^2$*, while those in* $\mathbb{C}[x]$ *are shaped like* $(x-a)$ *and constitute a* $\mathbb{C}$*. Restricted to the set of maximal ideals the map* π *is, of course, just the first projection* $\mathbb{C}^2 \to \mathbb{C}$*; indeed,* $(x-a, y-b) \cap \mathbb{C}[x] = (x-a)$ *(trivial since* $(x-a)$ *is maximal in* $\mathbb{C}[x]$*). The fibre over* $(x-a)\mathbb{C}[x]$ *consists of the point* $(x-a)^+ = (x-a)\mathbb{C}[x,y]$*, whose vanishing locus is the line* $x = a$*, and the maximal ideals* $(x-a, y-b)$ *corresponding to points on that line, these are all, since the irreducible polynomials in* $\mathbb{C}[y,x]/(x-a) \simeq \mathbb{C}[y]$ *are linear. The fibre of* π *over the zero ideal* (0) *comprises all the principal prime ideals, i.e. those shaped like* $(f(x,y))$ *with* f *irreducible, and additionally the zero ideal.*

Numerical functions are functions $h\colon \mathbb{Z} \to \mathbb{Z}$. They turn out have the very special property of behaving as a polynomial for sufficiently large arguments: There is a polynomial $P \in \mathbb{Q}[t]$ so that $h(n) = P(n)$ for $n >> 0$. The polynomial P is necessarily a so-called **numerical polynomial** in that it takes integral values on the integers.

A numerical function h has a "discrete derivative" defined as

$$\Delta h(t) = h(t) - h(t-1).$$

It shares the property with the usual calculus-derivative that $\Delta h = 0$ is equivalent with h being constant.

Well-known prototypes of numerical polynomials are the binomial coefficients given by

$$\binom{t+n}{n} = \frac{(t+n)(t+n-1)\dots(t+1)}{n!},$$

where n is any non-negative integer. It is well known that the polynomial takes integral values on the integers, and it is of degree n with leading coefficient $\frac{1}{n!}$.

Proposition

The following two assertions hold true:

1. *A numerical polynomial of degree n has a development*

$$h(t) = a_0\binom{t+n}{n} + a_1\binom{t+n-1}{n-1} + \ldots + a_{n-1}\binom{t+1}{1} + a_n$$

   where the coefficients a_i are uniquely defined integers and $a_0 \neq 0$.

2. *A numerical function $h(t)$ equals a numerical polynomial of degree n for for $t >> 0$ if and only if $\Delta h(t)$ equals one for $t >> 0$.*

Proof.

1. The proofs go by induction on n, the crucial observation being the identity we know from Pascals triangle

$$\Delta\binom{t+n}{n} = \binom{t+n-1}{n-1}.$$

2. Obviously a polynomial of the form as in the proposition is numerical and of the degree n.

3. To prove the converse, assume h is a numerical polynomial of degree n; then the derivative Δh will be of degree $n-1$, and by induction we may express Δh as

$$\Delta h(t) = \sum_{0 \le i \le n-1} a_i \binom{t+i}{i}.$$

$\square$

Proof. [Continue]

4. Consequently the difference

$$h(t) - \sum_{0 \leq i \leq n-1} a_{i+1} \binom{t+i+1}{i+1}$$

has a vanishing derivative and is therefore constant; with a_d being that constant value, the equality in the proposition holds true.

□

Graded ring:

$$A = \bigoplus_i A_i, \quad x = \sum_i x_i$$

with each $x_i \in A_i$ being homogeneous of degree i, only finitely many of them being non-zero.
The non-zero x_i's are called the **homogenous components** of x of degree i.
The decomposition is compatible with the multiplication;

$$A_i A_j \subset A_{i+j}$$

for all i and j.
The graded piece A_0 of degree zero will be a subring of A, and each A_i is a module over A_0.
A graded ring A is said to be **positively graded** if $A_i = 0$ for $i < 0$.

Example

The archetype of a graded ring is of course the polynomial ring $R = R_0[x_0, \ldots, x_n]$ *over some ring* R_0 *with the standard grading, the one giving all the variable* x_i *the degree one. The homogenous part* R_i *degree* i *has an* R_0*-basis which consists of the monomials of degree* i*, and hence is a free* R_0*-module of rank* $\binom{n+i}{i}$*. In most examples occurring in algebraic geometry the ring* R_0 *will be a field.*

Lemma

If A is a positively graded Noetherian ring, then A is a finitely generated algebra over A_0. Moreover, each graded piece A_d is a finite A_0-module.

Proof.

1. Since A is Noetherian, the ideal A_+ is finitely generated, say by elements $x_1, \dots, x_r$, and they may be assumed homogeneous.
2. Let $x \in A$ be a homogeneous element. By induction we may assume that all elements of degree lower than x lie in $A_0[x_1, \dots, x_r]$. Now $x \in A_+$, and hence $x = \sum a_i x_i$, with $\deg a_i + \deg x_i = \deg x$. Thus $\deg a_i < \deg x$; by induction we infer that a_i belongs to $A_0[x_1, \dots, x_r]$, and we are done.
3. The degree of a monomial $x^\alpha = x_1^{\alpha_1} \dots x_r^{\alpha_r}$ is equal to $\sum \alpha_i \deg x_i$, and since $\deg x_i > 0$, there are only finitely many multi-indices α such that $\deg x^\alpha = d$ for a given d; in other words is, the module A_d is finite over A_0.

Definition

A graded module over A is a module whose underlying additive group decomposes as $M = \bigoplus_{i\in\mathbb{Z}} M_i$ in way compatible with the action of A on M. That is, the following condition is satisfied

$$A_i M_j \subset M_{i+j}.$$

Notice that each homogenous component M_j will be a module over A_0. It turns out to be important to allow elements of negative degree, and as long as the degrees are bounded away from $-\infty$, this does not pose serious problem; we say that M is **bounded from below** if $M_i = 0$ for $i < \delta$.

Definition

A morphism between two graded A-modules M and M' is an A-homomorphism $\phi\colon M \to M'$ that respects the grading, i.e.

$$\phi(M_n) \subseteq M'_n$$

Definition

For each graded module M and each integer $m \in \mathbb{Z}$ there is graded module $M(m)$ associated to a graded module M. The **shifted module** *$M(m)$ has the same module structure as M, but new degrees defined by*

$$M(m)_d = M_{m+d}.$$

One simple reason for introducing the shift operators, is to keep track of the degrees of generators. If the the generators are $f_1, \dots, f_r$ and their degrees $d_1, \dots, d_r$, the module M will be a quotient of the direct sum $\bigoplus_{1 \leq i \leq r} A(-d_i)$, an element x in the summand $A(-d_i)$ is sent to xf_i, and the shifts make the quotient map homogenous of degree zero.

Example

For instance, when $m > 0$*, the shifted polynomial ring* $A(-m)$ *has no elements of degree* d *when* $d < m$*, indeed,* $A(m)_d = A_{d-m}$*, and the ground field* k *sits as the graded piece of degree* m*. Whereas the twisted algebra* $A(m)$ *has non-zero homogeneous elements of degrees down to* $-m$ *with the ground field sitting as the piece of degree* $-m$*.*

Lemma

Let A be a Noetherian graded ring. If M is a graded module finitely generated over A, then all graded pieces M_d are finitely generated over A_0. In particular, if A_0 is Artinian, each M_d will be of finite length.

Proof. This is more or less obvious. It is true for A itself by a previous lemma, hence for all shifted modules $A(m)$, hence for finite direct sums $\bigoplus_i A(-d_i)$. And if M is a quotient of $\bigoplus_i A(-d_i)$, the graded piece M_d of M of degree d is a quotient of the graded piece $\bigoplus_i A(-d_i)_d$. □

When A_0 is Artinian, this lemma enables us to define the important invariant h_M, the **Hilbert function** of such modules by putting $h_M(d) = \ell_{A_0}(M_d)$. It is a numerical function of d and is additive in M. This means that if

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0 \tag{1}$$

is an exact sequence of graded A-modules, then we have the equality $h_M = h_{M/N} + h_N$, and for each d the pieces of degree d in the sequence live in the exact sequence of A_0-modules

$$0 \longrightarrow N_d \longrightarrow M_d \longrightarrow (M/N)_d \longrightarrow 0.$$

Example

Consider the principle ideal (F) in the polynomial ring $R = k[x_0, \ldots, x_n]$ where F is a homogeneous form of degree m. Multiplication by F induces a homogeneous isomorphism between $R(-m)$ and (F) since for an element $a \in R(-m)_d$ it holds that $deg(a) = d - m$ and consequently $deg(aF) = d$. The classical short exact sequence is therefore an exact sequence of graded modules:

$$0 \longrightarrow R(-m) \xrightarrow{\mu} R \longrightarrow R/(F) \longrightarrow 0,$$

where the map μ is multiplication by F. Hence we find that

$$h_{R/(F)}(t) = \begin{cases} 0 & \textit{if } t < 0; \\ \binom{n+t}{t} & \textit{if } 0 \leq t < m; \\ \binom{n+t}{t} - \binom{n+t-m}{t} & \textit{if } t \geq m. \end{cases}$$

Example (Continue)

One observes that the function $h_{R/(F)}$ *piecewise is a polynomial, and that for* $t \geq m$ *it is equal to the polynomial*

$$\chi_M(t) = \binom{n+t}{t} - \binom{n+t-m}{t} = mt^{n-1}/n! + \dots$$

whose degree is one less than the dimension of $R/(F)$*. This is a general feature of Hilbert functions as we shall see in the next theorem, and the arising polynomials are called* **Hilbert polynomials***. We also observe that the leading coefficient, up to the factor* $1/n!$*, equals the degree of* F*. In general this coefficient will be of the form* $d/n!$ *with* d *a natural number simply because the Hilbert polynomials are numerical polynomials.*

Example

Let k be a field, and R the graded ring given by

$$R = k[x,y,z]/(x^2 - y^2, y^2 - z^2)$$

Let $A = k[x,y,z]$, and $B = A/(x^2 - y^2)$. Then we have an exact sequence

$$0 \to A(-2) \xrightarrow{\cdot(x^2-y^2)} A \to B \to 0$$

which gives for the Hilbert function

$$\begin{aligned} h_B(n) &= h_P(n) - h_P(n-2) \\ &= \frac{1}{2}(n+2)(n+1) - \frac{1}{2}n(n-1) = 2n+1 \end{aligned}$$

Example (Continue)

Next, we have

$$0 \to B(-2) \xrightarrow{\cdot(z^2-y^2)} B \to R \to 0$$

which gives

$$\begin{aligned} h_R(n) &= h_B(n) - h_B(n-2) \\ &= 2n+1-(2(n-2)+1) = 4 \end{aligned}$$

November, 5, 2020

The last topic is the study of Hilbert polynomials and Hilbert–Poincaré series,

15.2

The main result in this lecture is that the Hilbert function associated with a graded module M finite over a Noetherian ring A generated in degree one and with A_0 Artinian, is equal to a polynomial for large values of the variables. This polynomial is called the **Hilbert polynomial** of M. It is a numerical polynomial whose coefficients are important invariants of the graded module M.

The most common application of the Hilbert polynomial is in cases when A is a polynomial ring over a field with all the variables being of degree one.

Recall that the dimension $\dim(M)$ of a module M finite over a Noetherian ring A by definition equals the dimension of its support; that is, it is equal to $\dim(A/\mathrm{Ann}(M))$. Moreover, $\dim(M) = 0$ if and only if M is a module of finite length.

Theorem

Let A be a Noetherian graded ring A_0 being Artinian which is generated in degree one. Assume that M is a finitely generated graded A-module. Then the Hilbert function $h_M(\nu)$ equals a polynomial $\chi_M(\nu)$ for $\nu >> 0$. The degree n of χ_M equals $dim(M) - 1$ and its leading coefficient is of shape $d/n!$ with $d \in \mathbb{N}$.

Proof.

1. The proof goes by induction on $\dim(M)$, and the induction can begin because $\dim(M) = 0$ implies the module M is of finite length so that $h_M(\nu) = 0$ for $\nu >> 0$.
2. In a general finitely generated module M there is a finite descending chain $\{M_i\}$ of M of graded submodules whose subquotients are of the form $A/\mathfrak{p}_i$ with the $\mathfrak{p}_i$'s being homogeneous prime ideals. Taking the grading into account we arrive at a series of exact sequences of graded A-modules, one for each $0 \leq i \leq r$;
$$0 \longrightarrow M_{i+1} \longrightarrow M_i \longrightarrow A/\mathfrak{p}_\mathfrak{i}(m_i) \longrightarrow 0.$$
Moreover, it holds that $M_{r+1} = M$ and $M_0 = 0$.
3. This shows that the dimension of the support $\mathrm{Supp}(M)$ is equal to the maximum of the dimensions $\dim(A/\mathfrak{p}_i)$ of the subquotients, and the additivity of the Hilbert function yields the equality $h_M(\nu) = \sum_{1 \leq i \leq r} h_{A/\mathfrak{p}_i}(\nu + m_i)$. It will thus suffice to show the proposition for quotients $A/\mathfrak{p}$ with $\mathfrak{p}$ being a homogeneous prime ideal.

Proof. [Continue]

4. To that end, pick any $x \in A_1$ not lying in $\mathfrak{p}$ (we may safely assume that $\dim(A/\mathfrak{p}) > 0$ so that $\mathfrak{p} \subsetneq A_+$) and form the exact sequence

$$0 \longrightarrow A/\mathfrak{p}(-1) \xrightarrow{\cdot x} A/\mathfrak{p} \longrightarrow A/\mathfrak{p} + (x) \longrightarrow 0.$$

5. By the Hauptidealsatz $\dim(A/\mathfrak{p} + (x)) = \dim(M) - 1$, induction applies to $A/\mathfrak{p} + (x)$ and $\Delta h_{A/\mathfrak{p}}(\nu) = h_{A/\mathfrak{p}+(x)}(\nu)$ equals a polynomial of degree $\dim(M) - 1$ for $\nu >> 0$. Thus $h_{A/\mathfrak{p}}(\nu)$ is a polynomial of degree $\dim(M)$ for large values of ν.

$\square$

Lemma

Let A be a Noetherian graded ring with A_0 Artinian which is generated by s elements of degree one. Then the Hilbert polynomial $\chi_A(v)$ is of degree less than s unless A is isomorphic to the polynomial ring in s variables over A_0, in which case $deg(\chi_A) = s$.

Proof.

1. Assume that the elements $x_1, \dots, x_s$ generate A_1 over A_0. Let $X_1, \dots, X_n$ be variables and define a map $\phi \colon A_0[X_1, \dots, X_s] \to A$ by sending X_i to x_i. This is a map of graded rings which is surjective since A_1 is supposed to generate A as an A_0-algebra. It follows that $h_A(\nu) \leq \binom{\nu+s}{s}$ for all ν.
2. If the map ϕ is not injective, we may chose a non-zero homogeneous polynomial F from its kernel. Then ϕ factors through $B = A_0[X_1, \dots, X_s]/(F)$ and consequently $h_A(\nu) \leq h_B(\nu)$ for all ν. We have seen that $\dim(B) \leq s-1$, and by the proposition above χ_B is of degree at most $s-1$, so that $\deg(\chi_A) \leq s-1$.

$\square$

Example

Given a natural number d. Consider the subalgebra $A = k[u^d, u^d v, \ldots, uv^{d-1}, v^d]$ of the polynomial ring $R = k[u, v]$ generated by all monomials of degree d. It is a graded subalgebra, and A decomposes as $A = \bigoplus_i R_{id}$; i.e., as the sum of the homogeneous pieces of R of degree a multiple of d. Changing the degrees of the elements in A by factoring out d, the algebra A will be generated in degree one, and by the decomposition of A above we find $dim(A) = 2$ and $\chi_A(t) = \chi_R(dt) = dt + 1$.

Example

More generally, let $R = k[u_0, \ldots, u_n]$ *and consider the subalgebra* A *of* R *generated by all the monomials of degree* d*; i.e. those shaped like* $u^\alpha = u^{\alpha_0} \cdot \ldots \cdot u_r^{\alpha_r}$ *with* $\sum_i \alpha_i = d$*. Just as in the previous case, the decomposition of* A *into homogeneous pieces appears as* $A = \bigoplus_i R_{id}$*, form which ensues the identity*

$$\chi_A(t) = \chi_R(dt) = \binom{dt+n}{n} = d^n t^n / n! + \ldots.$$

We conclude that $dim(A) = n+1$ *and its degree is* d^n*.*

There is another way of encoding the sizes of the graded pieces of graded modules by forming the generating series, the so called Hilbert-Poincare series. This not only works well for positivily graded rings which are not generated by elements of degree one, but also reveals structures not easily detected by the Hilbert functions.

So let A a positively graded Noetherian ring with A_0 artinian and let M be a finite A-module. The graded pieces A_d are the of finite length over A_0, and we may form the formal Laurent series

$$P(M,t) = \sum_{i\in\mathbb{Z}} \ell_{A_0}(M_d)t^d.$$

As M finite over A, which is positively graded, M will be bounded below, and the series has only finitely many non-zero terms with negative exponents, in other words, it is a Laurent series.

The Hilbert–Poincaré series are clearly additive invariants; indeed, an exact sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

of graded A-modules is exact degree by degree, and hence $P(M,t) = P(M',t) + P(M'',t)$. Moreover, they are well behaved with respect to the shift operators:

UNIVERSITETET I OSLO

Lemma

$$P(M(m), t) = t^{-m} P(M, t)$$

Proof. It holds true that $M(m)_d = M_{d+m}$ so that

$$P(M(m), t) = \sum \ell_{A_0}(M(m)_d) t^d = \sum_d \ell_{A_0}(M_{d+m}) t^d$$

and changing the summation variable by putting $d' = d + m$ one obtains

$$\sum \ell_{A_0}(M_{d'}) t^{d'-m} = P(M, t) t^{-m}$$

□

Theorem

Let A be a graded ring with A_0 being Artinian. Assume that A is generaed over A_0 by elements $x_1, \ldots, x_r$ whose degrees are $d_1, \ldots, d_r$, all being positive. Let M be a finite A-module. Then the Hilbert–Poincare series $P(M,t)$ of M is a rational function of the type

$$P(M,t) = \frac{f(M,t)}{t^m \prod_i (1 - t^{d_i})} \tag{2}$$

where $f(M,t)$ is a polynomial with integral coefficients. If M is positively generated as well, then $m = 0$.

UNIVERSITETET I OSLO

Proof.

1. Since $P(M,t)$ is additive in M, it is enough to consider $M = A/\mathfrak{p}$ with $\mathfrak{p}$ a prime ideal.
2. If $A_+ \subset \mathfrak{p}$, we are done.
3. If not, one of the generators does not belong to $\mathfrak{p}$, and one may form the following exact sequence of graded A-modules:

$$0 \longrightarrow A/\mathfrak{p}[-d_i] \xrightarrow{x_i} A/\mathfrak{p} \longrightarrow A/\mathfrak{p}+(x_i) \longrightarrow 0. \qquad (3)$$

and it ensues that $P(A/\mathfrak{q},t) - t^{d_i}P(A/\mathfrak{p},t) = P(A/\mathfrak{p}+(x_i),t)$. Consequently

$$P(A/\mathfrak{p},t) = \frac{P(A/\mathfrak{p}+(x_i),t)}{(1-t^{d_i})}$$

and we are done since the right hand side by induction on the number of generators is of the desired shape.

□

As a corollaries of the proof we have

Corollary

Let $k[x_1, \ldots, x_r]$ be a polynomial ring given a grading by letting x_i be of degree d_i. Then

$$P(R,t) = \prod (1 - t^{d_i})^{-1}$$

Proof. Induction on r, succesively kiling each x_i. □

Corollary

Let A be positively graded Noetherian ring with A_0 Artinian and M a graded module finite over A_0. Then the pole order of $P(M,t)$ at $t=1$ equals the dimension $dim(M)$.

Proof.

1. By the additivity property it suffices to verify the claims for the quotients $A/\mathfrak{p}$ where $\mathfrak{p}$ is a homogeneous prime; indeed, if $A/\mathfrak{p}_\mathfrak{i}(m_i)$ with $1 \leq i \leq r$ are the arising subquotients, it holds that

$$P(M,t) = \sum_{1 \leq i \leq r} P(A/\mathfrak{p}_\mathfrak{i}, t)t^{-m_i}.$$

2. The pole order of the sum equals the maximum of the pole orders of the summands, which by the quotient case equals $\max \dim(A/\mathfrak{p}_\mathfrak{i})$; but this maximum is also equal to the dimension $\dim(M)$.
3. The pole order of the Hilbert–Poincare series goes up by one when one passes from $A/\mathfrak{p} + (x_i)$ to $A/\mathfrak{p}$, hence by induction, the dimension and the pole order agree.

□

Example

Let k be a field, and R the graded ring given by

$$R = k[x,y,z]/(x^2 - y^2, y^2 - z^2)$$

Let $A = k[x,y,z]$, and $B = A/(x^2 - y^2)$. Then we have an exact sequence

$$0 \to A(-2) \xrightarrow{\cdot(x^2-y^2)} A \to B \to 0$$

which gives for the Hilbert function

$$\begin{aligned} P(B,t) &= P(A,t) - t^2 P(A,t) \\ &= \frac{1}{(1-t)^3} - \frac{t^2}{(1-t)^3} = \frac{1+t}{(1-t)^2} \end{aligned}$$

Example (Continue)

Next, we have

$$0 \to B(-2) \xrightarrow{\cdot(z^2-y^2)} B \to R \to 0$$

which gives

$$\begin{aligned} P(R,t) &= P(B,t) - t^2 P(B,t) \\ &= \frac{1+t}{(1-t)^2} - \frac{t^2(1+t)}{(1-t)^2} = \frac{(1+t)^2}{(1-t)} \\ &= (1+t)^2(1+t+t^2+t^3+\dots) \\ &= (1+t+t^2+t^3+\dots) + 2(t+t^2+t^3+\dots) + (t^2+t^3+\dots) \\ &= 1+3t+4t^2+4t^3+4t^4+\dots \end{aligned}$$

which agree with the Hilbert function $h_R(n) = 4$ *and* $dim(R) = 1$.

Example (Continue)

The primary decomposition of the ideal

$$\mathfrak{a} = (x^2 - y^2, y^2 - z^2) = ((x+y)(x-y), (y+z)(y-z))$$

is given by

$$\mathfrak{a} = (x+y, y+z) \cap (x-y, y+z) \cap (x+y, y-z) \cap (x-y, y-z)$$

which corresponds to the four lines through the origin in $\mathbb{A}^3$*;*

$$x = -y = z, \quad x = y = -z, \quad x = -y = -z, \quad x = y = z$$