MA4J8 Commutative algebra II

4 Weeks 4–5: Dimension theory

4.1 Introductory discussion

I treat dimension theory (originally due to Krull) following [Matsumura, Chap. 5] and [A&M, Chap. 11]. I mainly work with Noetherian local rings. These conditions are convenient to use, and cover most of the cases we need in practice.

Depending on what branch of mathematics we study, dimension means different things: until recently, applied math textbooks commonly used phrases like "∞^2 solutions", to indicate that points depend on 2 continuous parameters. The number of algebraically independent variables in a ring or field extension. And so on. The following three different interpretations hint at what I am trying to do in commutative algebra. I will set them up correctly later in this chapter. The main point is to establish that three alternative technical definition of dimension of Noetherian local ring coincide in appropriate situations.

Informal view of dimension

(1) Dimension n means that a ball of radius r has volume const. $\times\, r^n$. Or the number of lattice points in a simplex of size n grows as

$$\sim \binom{r + \text{a bit}}{n} \sim \frac{r^n}{n!} + \text{lower order terms.} \tag{4.1}$$

(2) You can cut down an n-dimensional body by a hyperplane (setting a single equation equal to zero) to get down to $n-1$ dimensions, and so on to dimension 0, meaning a point or a finite set of points.

(3) We have already seen Krull dimension n, the length of the longest chain of prime ideals $P_0 \subset P_1 \subset \cdots \subset P_n$ in a ring, or the longest chain of irreducible subvarieties

$$\text{point} \subset \text{curve} \subset \text{surface} \subset \cdots \subset n\text{-fold} \tag{4.2}$$

in a variety. Krull dimension 0 (together with Noetherian) is a characterisation of an Artinian ring (or field if it is an integral domain), and Krull dimension 1 is part of the characterisation of DVRs or Dedekind domains.

4.2 Graded rings

I work mostly with $\mathbb{N}$-graded rings and modules, where $N = \{0, 1, 2, \dots\}$. (Gradings by more general semigroups are also useful in other contexts.)

A *graded ring* is a ring $R = \bigoplus_{n\geq 0} R_n$, where the R_n are additive subgroups and the ring multiplication takes $R_{n_1} \times R_{n_2} \to R_{n_1+n_2}$.

It follows of course that R_0 is a subring, with $1_R \in R_0$, and each R_n is an R_0-module. Also, $J = \sum_{n\geq 0} R_n$ is an ideal and $R/J = R_0$. Elements of R_n are *homogeneous* of degree n. Any $f \in R$ is uniquely expressible as a finite sum $f = \sum_n f_n$ with f_n homogeneous of degree n. It is the *homogeneous component* or *homogeneous piece* of f.

For dimension theory, we almost always restrict to the case that R_0 is an Artinian ring, or even just $R_0 = k$ is a field. (More general rings are used in other contexts.)

Lemma 4.1 (Standard fact) *A graded ring R is Noetherian if and only if*

(i) the subring R_0 is Noetherian , and

(ii) R is generated as an R_0 algebra by finitely many homogeneous elements $x_i \in R_{d_i}$.

Both implications are straightforward – please think them through as an exercise.

Why graded rings? A general point in algebra is that a grading on a vector space or on a module is more or less the same thing as a representation of the multiplicative group $\mathbb{G}_m(k) = \mathrm{GL}(1, k)$, or more familiarly, $\mathbb{C}^\times$. The most common such representation is the equivalence relation defining $\mathbb{P}^n$.

Projective space $\mathbb{P}^n = \left(k^{n+1} \setminus \{0\}\right)/\sim$, where $\sim$ is the equivalence class $\boldsymbol{x} \sim \lambda\boldsymbol{x}$ for $\lambda \in \mathbb{G}_m(k)$, has homogeneous coordinates $(x_0, \dots, x_n)$: a point $P \in \mathbb{P}^n$ corresponds to a ratio $(x_0 : x_1 : \cdots : x_n)$. Like the sound of one hand clapping, the individual x_i is not a meaningful function (it varies in an equivalence class), but the ratio $x_i : x_j$ or the "rational function" x_i/x_j is (partially defined and) well defined where $x_j(P) \neq 0$.

If $f \in k[x_0, \dots, x_n]$ is homogeneous of degree d, changing all $x_i \mapsto \lambda x_i$ changes $f(x_0, \dots, x_n) \mapsto \lambda^d f$, so the condition $f(P) = 0$ is well defined. The degree d homogeneous component of $k[x_0, \dots, x_n]$ thus appears as the λ^d eigenspace of the action of λ, or the character space of the $\mathbb{G}_m$ action on $k[x_0, \dots, x_n]$.

Implicit in this is the key point that the algebraic group $\mathbb{G}_m$ is *reductive*. A representation of $\mathbb{G}_m$ splits into 1-dimensional representations, and every 1-dimensional representation of $\mathbb{G}_m$ is a dth power homomorphism

$$\mathbb{G}_m \to \mathbb{G}_m = \mathrm{GL}(1,k), \quad \text{given by } z \mapsto z^d \text{ for some } d \in \mathbb{Z}. \tag{4.3}$$

The informative slogan "a grading on a module or vector space is the same thing as a representation of $\mathbb{G}_m$" is also a useful formal result:

Proposition 4.2 *Making a vector space V into a representation of $\mathbb{G}_m$ is exactly the same thing as putting a $\mathbb{Z}$-grading on V, that is, writing*

$$V = \bigoplus_{d\in\mathbb{Z}} V_d, \quad \textit{where } \lambda \in \mathbb{G}_m \textit{ acts on } V_d \textit{ by } v \mapsto \lambda^d v. \tag{4.4}$$

4.3 Graded modules and graded ideals

Given R as above, a graded module over R is an R-module M with a grading $M = \bigoplus_n M_n$, with the ring operation doing $R_{n_1} \times M_{n_2} \to M_{n_1+n_2}$. We sometimes need to allow the grading of M to have finitely many negative pieces M_n with $-s \le n < 0$. Worrying about the negative terms tends to mess up the statement of results, and we mostly assume $n \ge 0$. (It's not a big deal, since we can always shift the degrees by passing from M to $M[d] = \bigoplus M_{d+n}$.)

A *homogeneous ideal* or *graded ideal* $I \subset R$ is a particular case of graded submodule. It is an ideal $I \subset R$ with the property that $I = \sum I_n$ where $I_n = I \cap R_n$. Another way of saying this: for every element $f \in I$, write $f = \sum f_n$ in the graded structure of R; then all the homogeneous pieces f_n of $f \in I$ are also in I.

In the $I \longleftrightarrow V$ correspondence between subvarieties $V \subset \mathbb{P}^n_k$ and graded ideals I in $k[x_0, \dots, x_n]$ (the homogeneous coordinate ring of $\mathbb{P}^n$), graded ideals I with $V(I) = \{0\} \subset k^{n+1}$ define $\emptyset \subset \mathbb{P}^n_k$, and we usually disparage them as "irrelevant ideals", and ignore them. The Nullstellensatz implies that

$$I \text{ is irrelevant} \iff (x_0, \dots, x_n)^N \subset I \text{ for some } N, \tag{4.5}$$

that is, $(x_0, \dots, x_n) \subset \mathrm{rad}(I)$.

A relevant graded ideal defines an invariant subvariety $V_{\mathrm{aff}}(I) \subset k^{n+1}$ made up of nonzero orbits of the $\mathbb{G}_m$ action (lines through $0 \in k^{n+1}$), so points of $\mathbb{P}^n$. This is the *affine cone* over the projective subvariety $V_{\mathrm{proj}}(I) \subset \mathbb{P}^n$.

4.4 Hilbert series

For the present, consider an $\mathbb{N}$-graded ring $R = \sum R_n$ with the additional condition that R_0 is Artinian (the model case is simply a field). A finite module N over R_0 has finite length $l(N) = \text{length}_{R_0}(N)$ (it is finite over an Artinian ring). If $R_0 = k$ is a field, $l(N)$ is just the k-vector space dimension of N.

Suppose also that R is Noetherian, so generated over R_0 by finitely many homogeneous elements $\{x_i \in R_{d_i}\}$: then

$$R = R_0[x_1, \dots, x_r]/I_R, \tag{4.6}$$

where I_R is the ideal of all relations in R between the x_i.

The usual "straight" case is when all $d_i = 1$. When the d_i take different values, we use *weight* (or *weighted degree*) as another word for degree, to avoid the ambiguity between homogeneous and weighted homogeneous monomial: a monomial $\prod x_i^{a_i}$ has weight $\sum a_i d_i$.

For given weight n, there are only finitely many monomials $\prod x_i^{a_i}$ of weight $\sum a_i d_i = n$, so each homogeneous piece R_n of R is a finite module over R_0, therefore of finite length $l(R_n)$. This gives us something to count.

The same applies to a finite R-module M: each M_n is a finite R_0-module, because M_n is generated by finitely elements of degree $\geq -s$ for some integer s (usually $s = 0$). In any case R_n is generated over the Artinian ring R_0 by finitely many module monomials, so that $\text{length}(M_n)$ is a finite number.

Definition 4.3 (Hilbert series) Assume for simplicity that $M_n = 0$ for $n < 0$. Write

$$\begin{aligned} P_n(M) &= \text{length}_{R_0}(M_n) \quad \text{for } n \in \mathbb{Z}, \text{ and} \\ P(M,t) &= \sum_{n=0}^{\infty} P_n(M) t^n. \end{aligned} \tag{4.7}$$

The integer valued function $n \mapsto P_n(M)$ is the *Hilbert function* of M. The generating series $P(M,t)$ for the $P_n(M)$ is the *Hilbert series* of M. It is a formal power series in t. Its big selling point is that it holds the infinitely many coefficients $P_n(M)$ in a closed form, giving a lot of useful information for little effort.

If M has homogeneous pieces M_n in negative degrees with $-s \leq n < 0$, the result is similar, but we need to replace the formal power series with a formal *Laurent* power series (starting with $P_{-s}(M)t^{-s}$).

Theorem 4.4 *Let R be as in (4.6) and M a finite R-graded module (and again for simplicity, $M_n = 0$ for all $n < 0$). Then the formal power series $P(M,t)$ is a rational function of t with denominator $\prod_{i=1}^r (1 - t^{d_i})$, where $d_i = \text{weight}\, x_i$. That is,*

$$P(M,t) = \frac{H(M,t)}{\prod_{i=1}^r (1 - t^{d_i})}, \tag{4.8}$$

with $H(M,t) \in \mathbb{Z}[t]$ a polynomial with integer coefficients. In different contexts, we call it the Hilbert numerator *of M.*

As before, if M has nonzero pieces M_n with $-s \le n < 0$, a similar result still holds, but with $H(m,t) \in \mathbb{Z}[t, t^{-1}]$ a Laurent polynomial with terms of negative degree down to $-s$.

The "straight" homogeneous case Although it is not the only case of interest, a key case for graded rings and modules is when all the generators x_i have degree $d_i = 1$. It is a "well known fact" (proved below) that

$$\frac{1}{(1-t)^{r+1}} = \sum_{n \ge 0} \binom{n+r}{n} t^n. \tag{4.9}$$

To get the hang of this, write it out for $r = 0, 1, 2$. The formula is memorable for me as the *number of forms of degree n on $\mathbb{P}^r$*.

Corollary 4.5 *Assume that the numerator $H(M,t)$ of $P(M,t)$ is a polynomial of degree D and that all the $d_i = 1$. Then for $n \ge D$, the term $P_n(M)$ is a polynomial in n.*

In this case after we cancel powers of $1-t$, (4.8) can be rewritten as $\frac{N(t)}{(1-t)^d}$ with N a polynomial in t not divisible by $1-t$, so that $N(1) \ne 0$. Then $N(1) > 0$, and the order of growth of $P_n(M)$ for $n \gg 0$ is

$$N(1) \cdot \frac{n^{d-1}}{(d-1)!} + \textit{lower order terms.} \tag{4.10}$$

The number d in Corollary 4.5 (with $M = R$) is the dimension of the graded ring R. It can also be defined as 1 plus the order of pole at $t = 1$ of $P(R,t)$ in (4.8). The order of growth, the dimension d and the leading term $N(1)$ in (4.10) are key ingredients in the main theorem of this chapter.

Proof of corollary Write

$$H(M,t) = a_0 + a_1 t + \cdots + a_D t^D \tag{4.11}$$

for the numerator. The power series expansion of $P(M,t) = \frac{H(M,t)}{(1-t)^{r+1}}$ is then the product of the polynomial (4.11) times the power series (4.9)

For $n \geq D$, the t^r term in this product is the sum of $D+1$ terms

$$\sum_{i=0}^{D} a_i t^i \times \binom{n-i+r}{n} t^{n-i} \tag{4.12}$$

Each summand here is a coefficient that is a polynomial in n multiplied by t^n. Therefore the coefficient of t^n is a polynomial in n. (For $n < D$ the formula handles the terms with $i < D - n$ incorrectly.) Q.E.D.

Proof of Theorem 4.4 The method of proof is induction over the number r of generators of R. If $r = 0$ then M is a finite graded module over the Artinian ring R_0, so it is a sum of finite length R_0-modules M_n in finitely many degrees n, and $P(M,t)$ is just a polynomial (or a Laurent polynomial if M has some pieces M_n in degree $n < 0$).

Inductive step The main step in the proof is the following induction: consider the multiplication map by x_r:

$$m_{x_r} \colon M \to M \tag{4.13}$$

This increases degrees by d_r. It defines the exact sequence

$$0 \to K \to M \xrightarrow{x_r} M \to N \to 0. \tag{4.14}$$

Now the kernel $K = \ker m_{x_r} \subset M$ is the submodule annihilated by x_r. Therefore it is a graded module over $\overline{R} = R/(x_r)$. Also, by construction, $N = \operatorname{coker} m_{x_r} = M/(x_r M)$ is a graded R-module annihilated by x_r.

Note that M is a graded module over R, whereas by what I just said, K and N are graded modules over the quotient ring $\overline{R} = R/(x_r)$, which is a graded R_0-algebra of the same shape as (4.6), but now with only $r-1$ generators.

Thus by induction on r, I can assume that the result is already known for both K and N, so their Hilbert series are of the form

$$\begin{aligned} P(K,t) &= \frac{H(K,t)}{\prod_{i=1}^{r-1}(1-t^{d}i)}, \\ P(N,t) &= \frac{H(N,t)}{\prod_{i=1}^{r-1}(1-t^{d}i)}. \end{aligned} \tag{4.15}$$

where the numerators are polynomials with integer coefficients.

Since m_{x_r} increases degrees by d_r, the exact sequence (4.14) breaks up according to weighted degrees as exact sequences

$$0 \to K_{n-d_r} \to M_{n-d_r} \xrightarrow{x_r} M_n \to N_n \to 0. \tag{4.16}$$

of R_0-modules of finite length, one for each n.

This implies the equality

$$l(M_n) - l(M_{n-d_r}) = N_n - K_{n-d_r} \quad \text{for each } n. \tag{4.17}$$

Now summing (4.17) times t^n gives

$$(1 - t^{d_r})P(M, t) = P(N, t) - t^{-d_r} P(K, t). \tag{4.18}$$

This is the result we wanted. Indeed, both terms on the r-h.s. are of the form polynomial (or possibly Laurent polynomial) divided by $\prod^{r-1}(1 - t_i^d)$. Therefore $P(M, t)$ is a polynomial divided by $\prod^r(1 - t^{di})$. Q.E.D.

4.5 From graded to filtered: Hilbert–Samuel function

The aim is to apply the theory of graded rings and modules and their Hilbert functions and Hilbert series to general Noetherian local rings.

A basic step is the passage from

(1) a Noetherian local ring A, m to

(2) the same ring with an I-adic filtration $\{I^n\}$ (for an ideal I not too far from the maximal ideal, see below), and on to

(3) the associated graded ring $R = \operatorname{Gr}_I A = \bigoplus_{n=0}^{\infty} I^n/I^{n+1}$

We will see that the graded ring $\operatorname{Gr}_I A$ satisfies the assumptions of Section 4.4, so that the results on its Hilbert series are applicable to derive results on A. The Hilbert–Samuel function of A and I is defined and calculated in terms of the Hilbert series of $\operatorname{Gr}_I A$.

Definition 4.6 (m-primary ideal) Let A, m, k be a Noetherian local ring. An ideal I of A is *m-primary* if $m^n \subset I \subset m$ for some $n \geq 1$. It is equivalent to say that $I \subsetneq A$ and $\operatorname{rad} I = m$, or that $m = (x_1, \ldots, x_k)$ and I contains some power $x_i^{m_i}$ of every generator of m.

Background An ideal I is *primary* if $fg \in I$ implies either $f \in I$ or $g^N \in I$ for some $N > 0$. In other words, the only way of getting into I by multiplication is to multiply by an element of $\operatorname{rad} I$. If I is primary then $P = \operatorname{rad} I$ is prime (check this if you haven't seen it before) and we say that I is P-primary. In our context, it is straightforward to check that m-primary is equivalent to the above definition. See [UCA, Chap. 7] for a more leisurely treatment of primary ideals and primary decomposition.

For example: if $P \in X$ is a point on an affine algebraic variety over k, and $A = \mathcal{O}_{X,P}$ the local ring of X at P, then

$$I \subset A \text{ is } m\text{-primary} \iff \begin{array}{l}\text{every } f \in I \text{ has } f(P) = 0, \text{ and}\\ \text{every } x_i \in m_P \text{ has some power } x_i^{n_i} \in I.\end{array} \tag{4.19}$$

In the geometric example, by the Nullstellensatz, this means $P \in X$ is an isolated point component of the algebraic set $V(I)$.

The quotient m/m^n is an A-module of finite length: in fact, each m^i/m^{i+1} is a finite dimensional vector space over the residue field $k = A/m$. If I is m-primary, the quotients A/I^n (together with their submodules or quotient modules) are Artinian, that is, 0-dimensional, and do not have any associated primes P other than m.

Every Jordan-Hölder sequence for A/I^n has all quotients isomorphic to the residue field $k = A/m$. The length of an I-primary module is the number of occurrences of $k = A/m$ as M_i/M_{i+1} in a JH filtration.

We work with the I-adic filtration $A \supset I \supset \cdots \supset I^n \supset \cdots$ and its associated graded ring $R = \operatorname{Gr}_I A = \bigoplus_{n\ge 0} I^n/I^{n+1}$. Its degree 0 term $R_0 = A/I$ is Artinian, and R is generated in degree 1 over R_0.

It might be natural for some purposes to work only with $I = m$. However, some proofs require that the order of growth is independent of which primary ideal we take. If I and J are two m-primary ideals then there are natural numbers a, b such that $I^a \subset J$ and $J^b \subset I$.

Definition 4.7 The *Hilbert–Samuel function* of A with respect to I is defined by

$$\operatorname{HS}_A^I(n) = \operatorname{length}(A/I^{n+1}) = \sum_{i=0}^{n} l(I^i/I^{i+1}). \tag{4.20}$$

(Both [A&M] and [Ma] use χ_A^I.) The r-h.s. says that this is the cumulative sum of the Hilbert series of the associated graded ring $\operatorname{Gr}_I(A)$.

It is often a headache to decide between d and $d+1$. The Hilbert function $P_n(\operatorname{Gr}_A^I)$ of (4.7) is the length of the graded piece I^n/I^{n+1}, so is an individual term in a sum. It has the leading term $N(1)\cdot\frac{n^{d-1}}{(d-1)!}$ of (4.10). The HS function of (4.20) is the cumulative total of these $\sum_{i\le n}\text{length}(I^i/I^{i+1})$, and has leading term $N(1)\cdot\frac{n^d}{d!}$.

For example, consider $A = k[x_1,\dots,x_r]$ with I equal to the maximal ideal $m = (x_1,\dots,x_r)$. The Hilbert function counts the homogeneous monomials in $(x_1,\dots,x_r)$ of degree equal to s, whereas the Hilbert–Samuel function counts the homogeneous monomials of degree $\le s$. Thus

$$\begin{aligned} P_s(A) &= \binom{r+s-1}{s} = \binom{r+s-1}{r-1} \\ \text{with cumulative sum}\quad \mathrm{HS}_A^m &= \binom{r+s}{s} = \binom{r+s}{r}. \end{aligned} \tag{4.21}$$

The HS function of a finite A-module M is defined in the same way in terms of the I-adic filtration I^nM and the associated graded module $\mathrm{Gr}_I(M) = \bigoplus (I^iM)/(I^{i+1}M)$.

When discussing completion, we have so far been interested in the inverse system A/I^n and the inverse limit $\widehat{A} = \varprojlim A/I^n$ that defines the I-adic completion. The focus here is on the *associated graded ring* $R = \mathrm{Gr}_I A = \sum_{n\ge 0} I^n/I^{n+1}$ and its modules $\sum I^nM/I^{n+1}M$.

Lemma 4.8 *Let A, m, k be a Noetherian local ring and I and m-primary ideal. Then $R = \mathrm{Gr}_I A = \bigoplus_{n=0}^\infty I^n/I^{n+1}$ is a graded ring of the form* (4.6)*, with all generators in degree* 1.

Proof The degree 0 piece of $\mathrm{Gr}_I A$ is $R_0 = A/I$, which is an Artinian ring as discussed above.

The degree 1 piece is $R_1 = I/I^2$. The ideal I is finitely generated (since A is Noetherian). Each I^n/I^{n+1} is a module over $R_0 = A/I$, because multiplication by an element of I takes I^n to I^{n+1}, so to 0 in I^n/I^{n+1}. Moreover the degree n part I^n/I^{n+1} of $\mathrm{Gr}_I R$ is generated by monomials of degree n in the generators of I, so is a finite R_0 module, and is also of finite length. This proves the lemma. □

Check up on prerequisites From now on, I assume known the theory of Hilbert series of a graded ring (as in 4.2–4.4 above) and the Hilbert–Samuel function of an I-adic filtration. Also, the material around Definition 4.6 of an m-primary ideal I.

Our trio of definitions Let A, m, k be a Noetherian local ring. We work with the 3 following quantities:

$d(A) =$ order of growth of $l(A/m^n)$, or of the Hilbert–Samuel function $\mathrm{HS}_n(A)$. Or the order of pole at $t = 1$ of the Hilbert–Samuel function $\mathrm{HS}_A(t)$. This is called the HS *dimension* of A.

$\delta(A) =$ smallest number of generators of an m-primary ideal $I = (s_1, \dots, s_\delta)$. Any such set $\{s_1, \dots, s_\delta\}$ is called a *system of parameters*, and δ is the *s.o.p. dimension* of A

This means that we can take the quotient $A/(s_1, \dots, s_\delta)$ and get an Artinian or 0-dimensional ring, and δ is the minimum such number.

$\dim A =$ Krull dimension, the maximum length of chain of prime ideals.

In what follows, we eventually prove the $\dim A \le d(A) \le \delta(A) \le \dim A$. Of these, the first inequality is the hardest. It uses the numerical properties of $\mathrm{HS}(A)$ in a rather subtle way. The remaining equalities are comparatively simple follow-your-nose kind of algebraic arguments.

It follows directly from the definition that if I, J are both m-primary then there are a, b such that

$$I^a \subset m^a \subset J \quad \text{and} \quad J^b \subset m^b \subset I. \tag{4.22}$$

Thus the order of growth of the Hilbert–Samuel function and the I-adic topology of a finite module M is independent of the choice of I.

Proposition 4.9 (Definition of HS dimension $d(A)$) *The* HS *function* $\mathrm{HS}^I_A(n)$ *is a polynomial of degree d in n for $n \gg 0$. Its leading term is* $N(1) \cdot \frac{n^d}{d!}$ *with $N(1) > 0$, where that of the Hilbert function of* $\mathrm{Gr}_I(A)$ *is* $\frac{N(t)}{(1-t)^d}$ *(see Corollary 4.5).*

The same statement holds for modules: the HS *function* $\mathrm{HS}^I_M(n)$ *is a polynomial for $n \gg 0$, of degree d and with leading term $N(1) \cdot \frac{n^d}{d!}$ where* $P(\mathrm{Gr}_I(M), t) = \frac{N(t)}{(1-t)^{d-1}}$.

The d appearing here is the HS dimension $d(A)$, respectively $d(M)$, one of the above trio of definitions.

Using HS dimension to bound dimension The following lemma is clever bean-counting on the numerics of $\mathrm{HS}^I_A(M)$. It is the first step in the technical proof of $\dim M \le d(M)$.

Lemma 4.10 ([Ma, Theorem 13.3]) *A, I as above, M a finite module and $N \subset M$ a submodule with quotient M/N. Then the* HS *dimensions of these three modules satisfy*

$$d(M) = \max\{d(N), d(M/N)\}. \tag{4.23}$$

Morever, in the case of equality $d(N) = d(M/N)$, the leading coefficient of $\mathrm{HS}(M)$ *equals the sum of leading coefficients of the submodule* $\mathrm{HS}(N)$ *and the quotient module* $\mathrm{HS}(M/N)$*.*

The proof is a skillful application of the full form of the Artin–Rees lemma.

Proof Take the I-adic filtration of the terms in the short exact sequence $0 \to N \to M \to M/N \to 0$. Starting with the quotient,

$$(M/N) \,/\, I^n(M/N) = M/(N + I^n M). \tag{4.24}$$

Viewing $N + I^n M$ as an intermediate submodule

$$I^n M \subset N + I^n M \subset M \tag{4.25}$$

expresses $M/I^n M$ as an extension of the successive quotients

$$(N + I^n M) \,/\, I^n M \quad \text{and} \quad M/(N + I^n M). \tag{4.26}$$

The second term is the r-h.s. of (4.24). The first term is isomorphic to $N/(I^n M \cap N)$ by the second isomorphism theorem. Putting this together gives

$$l(M/I^n M) \;=\; l\big(N/(I^n M \cap N)\big) + l\big((M/N)/I^n(M/N)\big). \tag{4.27}$$

The l-h.s. is $\mathrm{HS}_M(n)$ (ignore the n in place of $n+1$), and the equation displays it as a sum of the first term, which *is something to do with* the I-adic filtration on N, plus $\mathrm{HS}_{M/N}(n)$.

Now the Artin–Rees lemma gives a precise relation between the growth of the first term $l\big(N/(I^n M \cap N)\big)$ and that of $\mathrm{HS}_N(n) = l(N/I^n N)$: there exists c such that $I^n M \cap N = I^{n-c}(I^c M \cap M)$ for all $n \ge c$. Hence

$$I^n N \subset I^n M \cap N \subset I^{n-c} N, \tag{4.28}$$

and the length of $N/(I^n M \cap N)$ is sandwiched between $\mathrm{HS}_N^I(n-c)$ and $HS_N^I(n)$. Therefore it has the same order of growth as the polynomial $\mathrm{HS}_N^I(n)$, and the same leading term.

Now (4.27) gives that the HS dimension $d(M)$, equal to the order of growth of $l(M/I^n)$, is the maximum of the order of growth of the two terms on the right, which is the maximum of $d(N)$ and $d(M/N)$. This is (4.23). Moreover, if all three of the HS have the same order of growth, (4.27) gives that the leading terms must add up. This proves the lemma. $\square$

Corollary 4.11 *Let A be a local Noetherian integral domain and $x \in A$ a nonzero element. Then the* HS *dimensions satisfy*

$$d(A/(x)) \leq d(A) - 1. \tag{4.29}$$

Proof Apply the lemma to the ideal $xA \subset A$, and the quotient module $A/(x)$. Since A is an integral domain and $x \neq 0$, the principal ideal $(x) = xA$ is a submodule of A isomorphic to A.

This implies they have the same HS dimension, the same order of growth of $\mathrm{HS}(n)$ and the same leading term. Therefore, by the lemma, $A/(x)$ must have smaller order of growth.

In more detail, write $\mathrm{HS}(A) = \frac{N_A}{(1-t)^d}$ and $\mathrm{HS}(xA) = \frac{N_{xA}}{(1-t)^d}$ for the Hilbert–Samuel functions of A and xA. The numerators N_A and N_{xA} are polynomials of the same degree with the same leading term $N(1) > 0$, so subtracting one from the other cancels the leading term. Therefore $N_A(1) - N_{xA}(1) = 0$ and so $N_A - N_{xA}$ is divisible by $1-t$. This cancels one power of $(1-t)$ in the denominator. Thus $A/(x)$ has HS dimension $d(A/(x)) \leq d(A) - 1$. $\square$

4.6 Proof of $\dim A \leq d(A)$

This is the hard implication of the main theorem: the Krull dimension $\dim A$ of a Noetherian local ring A is bounded by its HS dimension $d(A)$. The proof is by induction on the HS-dimension $d(A)$.

0th Step. $d(A) = 0$ implies $\dim A = 0$. If $d(A) = 0$ then $l(A/m^n)$ is eventually constant. Therefore $m^{n+1} = m^n$, and Nakayama's lemma gives $m^n = 0$. Then m is the only prime ideal of A so $\dim A = 0$. In fact if $P \subsetneq m$ is a prime ideal, an element $x \in m \setminus P$ maps to a nonzero element of the integral domain A/P, which contradicts x nilpotent in A.

Induction step Suppose now that $d(A) > 0$. If $\dim A = 0$ we are home, so assume that $\dim A > 0$. Let

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_e \tag{4.30}$$

be an increasing chain of prime ideals of A.

For the induction, pick $x \in P_1 \setminus P_0$. It maps to a nonzero element $y = \overline{x}$ of the integral domain A/P_0, and we apply Corollary 4.11 to $y \in A/P_0$.

To do this, set $B = A/(P_0 + xA) = (A/P_0)/(y)$ and write $\pi \colon A \to B$ for the quotient map. Corollary 4.11 gives $d(B) \leq d(A) - 1$, so induction gives $\dim B \leq d(B)$. Now consider the rest of the chain

$$P_1 \subsetneq \cdots \subsetneq P_e. \tag{4.31}$$

For $i > 0$, the images $\pi(P_i)$ are ideals of B with $B/\pi(P_i) = A/P_i$, so they are prime, and form a chain of prime ideals of B of length $e - 1$.

Therefore $e - 1 \leq \dim B \leq d(B) \leq d(A) - 1$, which gives $e \leq d(A)$. This applies to every strictly increasing chain of prime ideals of A, therefore $\dim A \leq d(A)$. Q.E.D.

The same result holds for a finite module M over A, arguing on $\operatorname{Ass} M$ so that M has a module isomorphic to A/P, and applies the result for A itself – [Ma], p. 99 says "it is easy to see".

Theorem 4.12 (Main theorem) *The* 3 *definitions of dimension coincide*

$$\begin{aligned} \dim A &= \textit{Krull dimension: maximum length of chain of primes} \\ d(A) &= \mathrm{HS} \textit{ dimension: order of growth of } \mathrm{HS}(n) = l(A/I^{n+1}). \\ \delta(A) &= \textit{minimal number of generators} \\ &\qquad \textit{of an } m\textit{-primary ideal } I = (x_1, \dots, x_\delta). \end{aligned} \tag{4.32}$$

We have already done $\dim A \leq d(A)$. The other implications are more straightforward and formal.

Proof of $d(A) \leq \delta(A)$ Suppose that $\delta(M) = \delta$, and let $I = (x_1, \dots, x_\delta)$ be an m-primary ideal. Then A/I has finite length $l(A/I)$, and I^i/I^{i+1} is generated as A/I-module by monomials in $(x_1, \dots, x_\delta)$ of degree $\leq n$ for all $i < n$. We know that the number of these is at most $\binom{\delta+n}{n}$, so that $\mathrm{HS}^I_A(n) \leq l(A/I)\binom{\delta+n}{n}$, and therefore $d(A) \leq \delta(A)$

Proof of $\delta(A) \le \dim A$ If $\dim A = 0$ then m is nilpotent, so that 0 is already m-primary, that is $\delta(A) = 0$. So we can assume that $\dim A = s > 0$.

The argument is just a couple of lines, but it assumes some background points. Let's do the overall argument first, then explain the prerequisites that are involved.

Step 1 There are chains of prime ideals $P_0 \subset \cdots \subset P_s$ of length s. Only finitely prime ideals $P_0^{(i)}$ can be the bottom of such a chain. In fact P_0 must be a minimal prime, since otherwise the chain would extend down to a chain of length $s+1$. A Noetherian ring has only finitely many minimal primes. (See Appendix on Zariski topology for this.)

Step 2 Each of the $P_0^{(i)}$ is strictly contained in m. Therefore there exists $x \in m$ not contained in any P_i. (See Appendix on prime avoidance for this.)

Step 3 If $x \in m$ but $x \notin \bigcup P_0(i)$ then $\dim A/x \le s-1$. In fact write $\pi\colon A \to A/x$; then a prime Q of A/x has inverse image $\pi^{-1}(Q)$ in A that contains x, and this excludes all the bottom $P_0(i)$. Therefore a chain of them cannot start at any of the $P_0(i)$, so has length $\le s-1$.

Step 4 Complete the proof. By induction, we can assume that $\delta(A/x) \le \dim A/x \le s-1$. This means that the local ring $A/x, m/x$ has an $(m/(x))$-primary ideal with generators $x_2, \dots, x_s$. Therefore $(x, x_2, \dots, x_s)$ is an m-primary ideal of A, m generated by s elements, so $\delta(A) \le s$.

This completes the proof of the main theorem.

Appendix: Reminder on Zariski topology The statement is: *A Noetherian ring A has only finitely many minimal prime ideals P_i.* This as an exercise in the Zariski topology – I should have done it in the prerequisites at the start of the course. The prime ideals correspond to the irreducible components of the Zariski topology on $\operatorname{Spec} A$.

The Zariski topology on $\operatorname{Spec} A$ has closed sets $V(I)$. If A is Noetherian, this is a Noetherian topology – any descending chain of closed sets eventually terminates (because they are $V(I)$, and the I have the a.c.c.) The d.c.c. implies that any set of closed sets has a minimal element.

A closed set is *irreducible* if $V(I)$ is not $V(I_1) \cup V(I_2)$ with strictly smaller closed sets $V(I_i)$. This holds if and only if $V(I) = V(P)$ for a prime ideal V (the argument is the same as for affine varieties). It follows that every closed set is a finite union of irreducible closed sets. So the whole of Spec A is a finite union of $V(P_i)$ where the P_i are the minimal primes.

If you find this problematic, either take it on trust, or see [UCA, 5.12–5.13].

Appendix: Prime avoidance If $I, J_1, J_2 \subset A$ are subgroups in an Abelian group, it is more-or-less obvious that $I \subset J_1 \cup J_2$ implies that $I \subset J_1$ or $I \subset J_2$.

For pick $x_1 \in I \setminus J_2$ and $x_2 \in I \setminus J_1$. If $I \subset J_1 \cup J_2$ we must have $x_1 \in J_1$ and $x_2 \in J_2$. Now $x_1 + x_2 \in I$, and hence $x_1 + x_2 \in J_1$ or J_2. This contradicts the choice of either x_1 or x_2.

The result for more than 2 prime ideals is [A&M, 1.11, p. 8], but I always find it an absolute bastard to remember or to figure out from scratch.

Lemma 4.13 *If an ideal I is contained in a finite union of prime ideals $\bigcup_{i=1}^n P_i$ then I is contained in one of the P_i.*

The contrapositive: if I is not contained in any of the P_i, then I is not contained in their union.

We can assume by induction that I is not in the union of any $n-1$ of the P_i. So for each i, pick $x_i \in I \setminus \bigcup_{j \neq i} P_j$. Since $x_i \in \bigcup_{i=1}^n P_i$, necessarily $x_i \in P_i$.

Now $x_j \notin P_i$ for all $j \neq i$, so the product $\prod_{j \neq i} x_j$ is not in P_i (here we use the assumption that the P_i are prime). Now the sum of the products

$$\sum_i \prod_{j \neq i} x_j \tag{4.33}$$

is a sum of element in I (in fact in I^{n-1}) but is not in any P_i. (All but one term is in P_i, and the nth definitely not.) This contradicts the assumption that $I \subset \bigcup P_i$.