Dimension II

The dimension theory of commutative rings is essentially a local theory. Indeed, the Krull dimension of a ring Noetherian A (always commutative) is defined to be the supremum of the lengths of saturated chains of prime ideals:

$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_d.$$

(Nagata gave an example of a Noetherian ring with infinite Krull dimension but these do not usually arise in practice.) Since the chain is saturated $\mathfrak{m} = \mathfrak{p}_d$ must be maximal, and the local ring $A_{\mathfrak{m}}$ clearly has the same Krull dimension as A.

In these notes we will prove a main result of dimension theory, Krull's Dimension theorem. This requires some digressions that are of interest beyond the Dimension Theorem, the primary decomposition for Noetherian rings, and the Hilbert and Hilbert-Samuel polynomials. The proof of the Dimension Theorem involves an interesting mixture of different techniques to prove the equivalence of three different definitions of dimension.

The syllabus recommends Matsumura's book on Commutative Algebra for Dimension Theory. Another good reference is the last chapter of the book Atiyah and Macdonald, which also has a good discussion of the primary decomposition. Atiyah and Macdonald is notable for being short and always going to the heart of the matter, so we recommend it. Both books of Matsumura and Atiyah and Macdonald are available on-line through the Stanford Libraries.

Primary Decomposition

The primary decomposition was proved by Emmanuel Lasker while he was still world Chess Champion. It was generalized to Noetherian rings by Emmy Noether.

If A is a Dedekind domain, every nonzero ideal $\mathfrak{a}$ can be written as the product of ideals $\mathfrak{q}_i$, each of which is a power $\mathfrak{p}_i^{e_i}$ of a prime ideal $\mathfrak{p}_i$. Since the $\mathfrak{q}_i$ are coprime, this is the same as the intersection:

$$\mathfrak{a} = \bigcap_{i=1}^{m} \mathfrak{q}_i.$$

This useful fact generalizes to arbitrary ideals in a commutative ring. In contrast with the case of a Dedekind domain, the corresponding *primary decomposition* is not unique, but it has some uniqueness properties.

An ideal $\mathfrak{q}$ in a ring A is *primary* if $xy \in \mathfrak{q}$ implies that either $x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some n. Equivalently, every zero divisor in $A/\mathfrak{q}$ is nilpotent.

Lemma 1. *If $\mathfrak{q}$ is primary then $r(\mathfrak{q})$ is prime.*

Proof. Suppose that $xy \in r(\mathfrak{q})$. Then $x^N y^N \in \mathfrak{q}$ for some N. Thus either $x^N \in \mathfrak{q}$ or $(y^N)^n \in \mathfrak{q}$ for some n. Thus either $x \in r(\mathfrak{q})$ or $y \in r(\mathfrak{q})$. □

If $\mathfrak{q}$ is primary and $r(\mathfrak{q}) = \mathfrak{p}$ then we say that $\mathfrak{q}$ is $\mathfrak{p}$-*primary*.

Lemma 2. *Suppose that $\mathfrak{q}_1, \mathfrak{q}_2$ are $\mathfrak{p}$-primary ideals. Then $\mathfrak{q}_1 \cap \mathfrak{q}_2$ is also $\mathfrak{p}$-primary.*

Proof. We have $r(\mathfrak{q}_1 \cap \mathfrak{q}_2) = r(\mathfrak{q}_1) \cap r(\mathfrak{q}_2) = \mathfrak{p} \cap \mathfrak{p} = \mathfrak{p}$. To show $\mathfrak{q}_1 \cap \mathfrak{q}_2$ is $\mathfrak{p}$-primary, suppose that $xy \in \mathfrak{q}_1 \cap \mathfrak{q}_2$ but $x \notin \mathfrak{q}_1 \cap \mathfrak{q}_2$. Then either $x \notin \mathfrak{q}_1$ or $x \notin \mathfrak{q}_2$. By symmetry, we may assume that $x \notin \mathfrak{q}_1$. Then since $xy \in \mathfrak{q}_1$ which is $\mathfrak{p}$-primary, we have $y \in \mathfrak{p} = r(\mathfrak{q}_1) = r(\mathfrak{q}_1 \cap \mathfrak{q}_2)$. □

Lemma 3. *If $\mathfrak{q}$ is an ideal such that $r(\mathfrak{q})$ is maximal, then $\mathfrak{q}$ is primary.*

Proof. See Homework 5, Problem 1. □

Lemma 4. *Suppose that A is Noetherian and $\mathfrak{m}$ is maximal. If $\mathfrak{a}$ is any ideal of A, then $\mathfrak{a}$ is $\mathfrak{m}$-primary if and only if $\mathfrak{m} \supseteq \mathfrak{a} \supseteq \mathfrak{m}^n$ for some n.*

Proof. Suppose that $\mathfrak{a}$ is $\mathfrak{m}$-primary. Then $r(\mathfrak{a}) = \mathfrak{m}$ so $\mathfrak{m} \supseteq \mathfrak{a}$. To show that $\mathfrak{a} \supseteq \mathfrak{m}^n$ for some n let $x_1, \ldots, x_r$ be generators of $\mathfrak{m}$. Then $x_i^k \in \mathfrak{a}$ for some k. Now $\mathfrak{m}^n$ is generated by elements of the form $x_1^{a_1} \cdots x_r^{a_r}$ where $\sum a_i = n$. If $n \geqslant kr$ this forces some $a_i \geqslant k$ so $\mathfrak{a} \supseteq \mathfrak{m}^n$.

Conversely, suppose that $\mathfrak{m} \supseteq \mathfrak{a} \supseteq \mathfrak{m}^n$. Then

$$\mathfrak{m} = r(\mathfrak{m}) \supseteq r(\mathfrak{a}) \supseteq r(\mathfrak{m}^n) = \mathfrak{m},$$

so $r(\mathfrak{a}) = \mathfrak{m}$ is maximal and therefore $\mathfrak{a}$ is $\mathfrak{m}$-primary by Lemma 3. □

Theorem 5. *If A is Noetherian, then every ideal $\mathfrak{a}$ may be expressed as a finite intersection of primary ideals.*

Proof. Let us define an ideal $\mathfrak{q}$ to be *irreducible* if whenever $\mathfrak{q}$ is written as an intersection of two ideals, $\mathfrak{q} = \mathfrak{b} \cap \mathfrak{c}$ either $\mathfrak{q} = \mathfrak{b}$ or $\mathfrak{q} = \mathfrak{c}$. For example a maximal ideal is irreducible.

We may write any ideal $\mathfrak{a}$ as an intersection of irreducible ideals. Indeed, if this is not so let $\mathfrak{a}$ be a maximal counterexample. Then $\mathfrak{a}$ is not irreducible so we may write $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ with $\mathfrak{b}$ and $\mathfrak{c}$ strictly larger. But since $\mathfrak{a}$ is a maximal counter example, both $\mathfrak{b}$ and $\mathfrak{c}$ can be written as intersections of irreducible ideals, and hence so can $\mathfrak{a}$. This is a contradiction.

Hence it will be sufficient to show that an irreducible ideal $\mathfrak{q}$ is primary. Assume that $\mathfrak{q}$ is irreducible. Hence in the ring $\overline{A} = A/\mathfrak{q}$, the ideal (0) is irreducible. If we show that (0) is primary in $\overline{A}$, it will follow that $\mathfrak{q}$ is primary in A. So we may assume that $\mathfrak{q} = 0$.

Thus suppose that (0) is an irreducible ideal in A. We will show that $xy = 0$ implies $y = 0$ or $x^n = 0$ for some n. Assume that $y \neq 0$. We consider the ideals $\mathfrak{a}_n = \{z \in A | zx^n = 0\}$. Since

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots$$

and A is Noetherian, this chain stabilizes and $\mathfrak{a}_n = \mathfrak{a}_{n+1}$ for some n. We will show that $x^n = 0$.

Let us show that $(y) \cap (x^n) = 0$. Indeed, if a is in this intersection we may write $a = yz = wx^n$. Since $xy = 0$ we have $xa = xyz = 0$ and so $wx^{n+1} = 0$. This means that $w \in \mathfrak{a}_{n+1}$. Since $\mathfrak{a}_{n+1} = \mathfrak{a}_n$ we see that $wx^n = 0$, that is $a = 0$.

Now (0) is irreducible and $(y) \cap (x^n) = 0$. Since $(y) \neq 0$ we have $(x^n) = 0$ proving $x^n = 0$. We have shown that (0) is primary, as required. □

By Lemma 2 we may combine all primary ideals with a given radical, and hence in the decomposition

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i, \qquad \mathfrak{q}_i \text{ primary}, \tag{1}$$

we may assume that the $r(\mathfrak{q}_i)$ are distinct. We may also discard any $\mathfrak{q}_i$ if removing it does not change the intersection, so we may assume $\mathfrak{q}_i$ does not contain $\bigcap_{j \neq i} \mathfrak{q}_j$. With these assumptions we call the representation of $\mathfrak{a}$ in (1) a (reduced) *primary decomposition*.

Example 6. *The primary decomposition may not be unique. For example in the polynomial ring $k[x, y]$, where k is a field, the ideal $\mathfrak{a} = (x^2, xy)$ has two distinct primary decompositions:*

$$\mathfrak{a} = (x) \cap (x^2, y) = (x) \cap (x^2, xy, y^2).$$

Both decompositions are primary. Indeed (x) is prime, hence primary, while (x^2, y) and (x^2, xy, y^2) are primary by Lemma 3 since their radical (x, y) is maximal.

If $\mathfrak{a}$ is an ideal and $x \in A$ let

$$(\mathfrak{a} : x) = \{y \in A | xy \in \mathfrak{a}\} .$$

It is an ideal of A containing $\mathfrak{a}$.

Lemma 7. *Suppose that $\mathfrak{q}$ is $\mathfrak{p}$-primary. Then*
(i) if $x \in \mathfrak{q}$ then $(\mathfrak{q} : x) = A$;
(ii) if $x \notin \mathfrak{q}$ then $r\big((\mathfrak{q} : x)\big) = \mathfrak{p}$;
(iii) if $x \notin \mathfrak{p}$ then $(\mathfrak{q} : x) = \mathfrak{q}$.

Proof. This is easy and we leave it to the reader. □

Although the primary decomposition is not unique, it has some uniqueness properties. In particular:

Theorem 8. *Let $\mathfrak{a} = \bigcap \mathfrak{q}_i$ be a reduced decomposition into primary ideals. Then the prime ideals $\mathfrak{p}_i = r(\mathfrak{q}_i)$ are independent of the choice of decomposition.*

The $\mathfrak{p}_i = r(\mathfrak{q}_i)$ are called the *associated primes* of the ideal $\mathfrak{a}$, and the theorem shows that they do not depend on the choice of reduced primary decomposition.

Proof. We note that

$$r\big((\mathfrak{a} : x)\big) = \bigcup_{x \notin \mathfrak{q}_i} \mathfrak{p}_i. \tag{2}$$

Indeed the left-hand side is $\bigcap_i r\big((\mathfrak{q}_i : x)\big)$ so this follows from the Lemma.

Using (2) we may show that the $\mathfrak{p}_i$ are precisely the prime ideals that occur among the $r((\mathfrak{a} : x))$ as x runs through the elements of A. First note that since the decomposition is reduced, there exists $x \notin \mathfrak{q}_i$ such that $x \in \mathfrak{q}_j$ for all $j \neq i$. (Otherwise we could omit $\mathfrak{q}_i$ from the intersection $\mathfrak{a} = \cap \mathfrak{q}_i$.) Then $r((\mathfrak{q}_i)) = \mathfrak{p}_i$ by the Lemma. Conversely, suppose that $\mathfrak{p} := r((\mathfrak{a} : x))$ is prime: we claim that $\mathfrak{p}$ is one of the $\mathfrak{p}_i$. Indeed, by (2) $\mathfrak{p}$ contains the intersection of some of the $\mathfrak{p}_i$. We write $\mathfrak{p} = \bigcap_{i \in S} \mathfrak{p}_i$. If $\mathfrak{p}$ is not one of the $\mathfrak{p}_i$, then for each $i \in S$ we may find $x \in \mathfrak{p}_i - \mathfrak{p}$ and then $\prod x_i$ will be in $\bigcap_{i \in S} \mathfrak{p}_i$ but not in $\mathfrak{p}$, which is a contradiction.

Since we have an intrinsic characterization of the $\mathfrak{p}_i$ independent of the decomposition, the theorem is proved. □

Proposition 9. *Let $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ be a primary decomposition, and let $\mathfrak{p}_i = r(\mathfrak{q}_i)$ be the associated primes. Then any prime ideal $\mathfrak{p}$ that contains $\mathfrak{a}$ contains one of the $\mathfrak{p}_i$.*

Proof. First note that $\mathfrak{p} \supseteq \mathfrak{q}_\mathfrak{i}$ for some i. Indeed, if not let $x_i \in \mathfrak{q}_\mathfrak{i} \backslash \mathfrak{p}$ for each i. Then $\prod x_i$ is an element of $\mathfrak{a} = \bigcap \mathfrak{q}_i$ that is not in $\mathfrak{p}$, which is a contradiction. Then $\mathfrak{p} = r(\mathfrak{p}) \supseteq r(\mathfrak{q}_\mathfrak{i}) = \mathfrak{p}_i$. □

This shows that there are a finite number of minimal primes containing $\mathfrak{a}$, and that these are precisely the primes that are minimal among the associated primes $\mathfrak{p}_i = r(\mathfrak{q}_i)$. (Example 6 shows that there may be inclusion relations among the $\mathfrak{p}_i$, so the minimal associated primes may not be all of them.) Indeed, the Proposition immediately implies:

Corollary 10. *Let $\mathfrak{a}$ be an ideal in a Noetherian ring. Then there are a finite number of prime ideals that are minimal among the prime ideals containing $\mathfrak{a}$. These are the minimal $r(\mathfrak{q}_i)$ for a primary decomposition $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$.*

This fact has a geometric meaning.

Corollary 11. *Let $A = \mathcal{O}(X)$ be the affine algebra of affine algebraic variety, and let $Y = V(\mathfrak{a})$ be a Zariski-closed subset, for some ideal $\mathfrak{a}$ in A. Then Y has a unique decomposition into a union of maximal closed irreducible subsets $Y_i = V(\mathfrak{p}_i)$ where $\mathfrak{p}_i$ are the minimal associated primes.*

Hilbert Polynomial

Let G be a Noetherian graded ring. This means that G is a ring and that we have a decomposition $G = \bigoplus_{k=0}^{\infty} G_k$ into additive subgroups G_k such that $G_k G_l \subseteq G_{k+l}$. Thus G_0 is a subring and G is an G_0-algebra. At first we will assume that $G_0 = k$ is a field, and later relax this assumption. If $x \in G_i$ we say x is *homogeneous of degree i*.

Let M be a graded G-module. This means M itself has a decomposition $M = \bigoplus_{k=0}^{\infty} M_k$ and that $G_k M_l \subseteq M_{k+l}$. We assume that M is finitely-generated. This implies that $\dim(M_k) < \infty$ and we define the *Hilbert series* to be the formal power series

$$P_M(t) = \sum_{k=0}^{\infty} \dim(M_k) t^k.$$

Theorem 12. *Suppose that G is generated as a k-algebra by elements x_i that are homogeneous of degree d_i $(i = 1, \cdots, r)$. Then*

$$P_M(t) = \frac{g(t)}{(1 - t^{d_1}) \cdots (1 - t^{d_r})}$$

where $g(t)$ is a polynomial.

Proof. Let $G' = k[x_1, \cdots, x_{r-1}]$. It too is a graded k-algebra.

Multiplication by x_r is a graded G-module endomorphism of M of degree d_r; this means that it maps M_i into M_{i+d_r}. Let K and Q be the kernel and cokernel of this endomorphism. Then we have an exact sequence

$$0 \longrightarrow K_i \longrightarrow M_i \xrightarrow{x_r} M_{i+d_r} \longrightarrow Q_{i+d_r} \longrightarrow 0.$$

Since M is Noetherian, K and Q are finitely generated as G-modules. We thus have

$$\dim(K_i) - \dim(M_i) + \dim(M_{i+d_r}) - \dim(Q_{i+d_r}) = 0.$$

Multiplying this identity by t^{i+d_r} and summing over i gives

$$t^{d_r} P_K(t) - t^{d_r} P_M(t) + P_M(t) - P_Q(t) = 0$$

or

$$P_M(t) = \frac{P_Q(t) - t^{d_r} P_K(t)}{1 - t^{d_r}}.$$

We wish to apply induction and substitute the Hilbert series for $P_Q(t)$ and $P_K(t)$. Now think of $G = G'[x_r]$ as a graded ring generated over G' by one variable x_r. Both modules Q and K are annihilated by x_r so the Hilbert series for them is the same whether we compute it as G-modules or as G'-modules. Thus only factors $1 - t^{d_1}, \cdots, 1 - t^{d_{r-1}}$ appear in their denominators. □

We recall the notion of *length* of a module. A module M over a ring is *simple* if it is nonzero, but has no proper, nonzero submodules. Thus a vector space is simple if it is one-dimensional. A *composition series* for a module M has a filtration by submodules:

$$0 = M_0 \subsetneqq M_1 \subsetneqq \cdots \subsetneqq M_\ell = M$$

The *Jordan-Hölder theorem* asserts that if M has a composition series, then all composition series have the same length $\ell = \ell(M)$. This is the *length* of M. The Jordan-Hölder series is

proved for groups (where there is an analogous assertion) in Lang's *Algebra*, Chapter 1. The proof for modules is omitted in Lang, but it is identical to the group case. If the module has no composition series we write $\ell(M) = \infty$.

The length is additive in the sense that if we have a short exact sequence

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

then M has a composition series if and only if both M' and M'' do, and $\ell(M) = \ell(M') + \ell(M'')$.

Now let A be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Then $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is a vector space over $k = A/\mathfrak{m}$. Its length as an A-module equals its dimension as a k-vector space. On the other hand $A/\mathfrak{m}^i$ is not a vector space over k. It is, however an A-module and

$$\ell(A/\mathfrak{m}^n) = \sum_{k=0}^{n-1} \ell(\mathfrak{m}^k/\mathfrak{m}^{k+1}) = \sum_{k=0}^{n-1} \dim(\mathfrak{m}^k/\mathfrak{m}^{k+1}). \tag{3}$$

Theorem 13. *Suppose that A is a Noetherian local ring with maximal ideal $\mathfrak{m}$. Then there exists a polynomial $\chi_{\mathfrak{m}}(n)$ such that if n is sufficiently large, then $\ell(A/\mathfrak{m}^n) = \chi_{\mathfrak{m}}(n)$. If $r = \dim(\mathfrak{m}/\mathfrak{m}^2)$ then the degree of $\chi_{\mathfrak{m}}$ is $\leqslant r$.*

The polynomial $\chi_{\mathfrak{m}}$ is called the *Hilbert-Samuel polynomial*.

Proof. Define a graded algebra $G = G_{\mathfrak{m}}(A)$ as follows. The homogenous part of degree i is

$$G_i = \mathfrak{m}^i/\mathfrak{m}^{i+1}$$

and the multiplication $G_i \times G_j \longrightarrow G_{i+j}$ is induced by the multiplication $\mathfrak{m}^i \times \mathfrak{m}^j \longrightarrow \mathfrak{m}^{i+j}$. We treat G as a module over itself and consider its Hilbert series. Now G is generated by its elements of degree 1, and r is the number of generators needed, so the Hilbert series has the form

$$\sum_{i=0}^{\infty} \dim(\mathfrak{m}^i/\mathfrak{m}^{i+1})t^i = \frac{f(t)}{(1-t)^r} = f(t) \sum_{i=0}^{\infty} \binom{r+i-1}{i} t^i.$$

Now if $f(t) = \sum a_i t^i$ then comparing the coefficients of t^n we obtain (provided $n \geqslant \deg(f)$) the identity

$$\dim(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = \sum_{j=0}^{\deg(f)} a_j \binom{r+n-j-1}{n-j}.$$

Here $\binom{r+n-j-1}{n-j}$ is a polynomial of degree $r-1$. Thus there exists a polynomial p of degree $\leqslant r-1$ such that for sufficiently large n we have

$$\dim(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = p(n).$$

Using (3) implies that there exists a polynomial $\chi_{\mathfrak{m}}$ of degree $\leqslant r$ such that if n is sufficiently large, then $\ell(A/\mathfrak{m}^n) = \chi_{\mathfrak{m}}(n)$. □

The Krull Dimension Theorem

We may now define two more invariants of the Noetherian local ring A. First, let $d(A) = \deg(\chi_{\mathfrak{m}})$. Second, let $\delta(A)$ be the minimal number of generators required for an $\mathfrak{m}$-primary ideal. We may now state the main theorem of dimension theory.

Theorem 14 (Krull Dimension Theorem)**.** *Let A be a Noetherian local ring. Then*

$$\dim(A) = \delta(A) = d(A)$$

Proof. To prove this, we will have to prove inequalities

$$d(A) \leqslant \delta(A), \qquad \delta(A) \leqslant \dim(A), \qquad \dim(A) \leqslant d(A).$$

Each inequality uses a different technique.

The inequality $d(A) \leqslant \delta(A)$

It may be true that the degree of the polynomial $\chi_{\mathfrak{m}}(n)$ is less than $\dim(\mathfrak{m}/\mathfrak{m}^2)$. For example, consider the local ring at $(0,0)$ of the curve $y^2 = x^2(x+1)$. Then $\mathfrak{m}/\mathfrak{m}^2$ requires two generators, so $r = 2$. However if $i \geqslant 1$ then $\dim(\mathfrak{m}^i/\mathfrak{m}^{i+1})$ is two dimensional, spanned by x^i and $x^{i-1}y$. Using (3) it follows that $\chi_{\mathfrak{m}}(n) = 2n - 1$, which has degree 1, not 2. Let $d(A)$ be the degree of the polynomial $\chi_{\mathfrak{m}}$. Eventually we will show that this equals $\dim(A)$, and this statment is part of the Krull dimension theorem.

However we can improve Theorem 13. Note that $\dim(\mathfrak{m}/\mathfrak{m}^2)$ is the number of elements required to generate $\mathfrak{m}$. So we have proved that $\deg(\chi_{\mathfrak{m}})$ is $\leqslant$ the number of elements required to generate $\mathfrak{m}$. This number can be optimized by considering instead of $\mathfrak{m}$ itself, an $\mathfrak{m}$-primary ideal $\mathfrak{q}$.

Theorem 15. *Let $\mathfrak{q}$ be an $\mathfrak{m}$-primary ideal, and suppose that $\mathfrak{q}$ can be generated by r elements. Then $\deg(\chi_{\mathfrak{m}}) \leqslant r$.*

Proof. We may define a graded ring $G_{\mathfrak{q}}(A)$ as before. The homogeneous part is $G_i = \mathfrak{q}^i/\mathfrak{q}^{i+1}$. The main difference is that now $G_0 = A/\mathfrak{q}$ is no longer a field, so we will have to replace dimensions by lengths in the preceding arguments, but the same proof shows that there is a polynomial $p_{\mathfrak{q}}$ of degree $\leqslant r$ such that

$$\ell(\mathfrak{q}^n/\mathfrak{q}^{n+1}) = p_{\mathfrak{q}}(n) \tag{4}$$

for sufficiently large n, and we deduce that there exists a polynomial $\chi_{\mathfrak{q}}$ such that $\ell(A/\mathfrak{q}^n) = \chi_{\mathfrak{q}}(n)$. Since $r(\mathfrak{q}) = \mathfrak{m}$ and $\mathfrak{q}$ is finitely generated, we have $\mathfrak{q}^k \subseteq \mathfrak{m}$ for some k. On the other hand, every generator of $\mathfrak{q}$ has degree 1 in the graded ring $G_{\mathfrak{q}}(A)$. So again the form of the Hilbert series is $g(t)/(1-t)^r$ for some polynomial t, leading to (4) and the bound $\deg(p_{\mathfrak{q}}) \leqslant r - 1$. As before this implies that there is a polynomial $\chi_{\mathfrak{q}}(n)$ of degree $\leqslant r$ such that

$$\ell(A/\mathfrak{q}^n) = \chi_{\mathfrak{q}}(n)$$

for sufficiently large n.

Now since $\mathfrak{q}$ is $\mathfrak{m}$-primary there exists an N such that $\mathfrak{m} \supseteq \mathfrak{q} \supseteq \mathfrak{m}^N$. There

$$\mathfrak{m}^n \supseteq \mathfrak{q}^n \supseteq \mathfrak{m}^{Nn}$$

so $\chi_{\mathfrak{m}}(n) \leqslant \chi_{\mathfrak{q}}(n) \leqslant \chi_{\mathfrak{m}}(Nn)$. This implies that $\deg(\mathfrak{m}) = \deg(\mathfrak{q})$ proving that $\deg(\chi_{\mathfrak{m}}) \leqslant r$. □

The inequality $\delta(A) \leqslant \dim(A)$

We define the *height* of a prime ideal $\mathfrak{p}$ in a ring A to be the length d of the longest possible chain of prime ideals

$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \mathfrak{p}_2 \subsetneqq \cdots \subsetneqq \mathfrak{p}_d = \mathfrak{p}.$$

Thus the Krull dimension of A the maximal height of any prime in A, and if A is local the Krull dimension is the height of its prime ideal $\mathfrak{m}$.

Lemma 16. *Suppose that $\mathfrak{a}$ is an ideal and $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ are prime ideals such that $\mathfrak{a}$ is not contained in any $\mathfrak{p}_i$. Then $\mathfrak{a}$ is not contained in $\bigcup_i \mathfrak{p}_i$.*

Proof. This is clearly true if $n = 1$. By induction, we suppose it is true for $n - 1$. Arguing by contradiction, suppose that $\mathfrak{a} \subseteq \bigcup_i \mathfrak{p}_i$. But for each $1 \leqslant j \leqslant n$, we have $\mathfrak{a} \nsubseteq \bigcup_{i \neq j} \mathfrak{p}_i$, so we take an element x_i that is in $\mathfrak{a}$ but not $\bigcup_{i \neq j} \mathfrak{p}_i$. Then x_i must be in $\mathfrak{p}_j$ since $\mathfrak{a} \subseteq \bigcup_i \mathfrak{p}_i$. Now consider

$$x = \sum_{j=1}^{n} \prod_{i \neq j} x_i.$$

This is in $\mathfrak{a}$ so it must be in some $\mathfrak{p}_k$. We write

$$x = \prod_{i \neq k} x_i + x_k \sum_{j \neq k} \prod_{i \neq j,k} x_i.$$

Since x and x_k are in $\mathfrak{p}_k$ we must have $\prod_{i \neq k} x_i \in \mathfrak{p}_k$. But this is a contradiction since $x_i \notin \mathfrak{p}_k$ if $i \neq k$, and $\mathfrak{p}_k$ is prime. □

Proposition 17. *Let A be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Let $d = \dim(A) = \operatorname{height}(\mathfrak{m})$. Then there exists a sequence $x_1, \cdots, x_d \in \mathfrak{m}$ such that every prime ideal containing $(x_1, \cdots, x_i)$ has height $\geqslant i$ and such that the ideal $(x_1, \cdots, x_d)$ is $\mathfrak{m}$-primary.*

Proof. Suppose that $x_1, \cdots, x_i$ are constructed with $i < d$. We will show how to construct x_{i+1}. From Corollary 10 there are only a finite number of minimal primes containing $(x_1, \cdots, x_i)$. Let S be the set of such minimal primes that have height exactly i. (The set S may be empty.) Note that if $(x_1, \cdots, x_i) \subseteq \mathfrak{p}$ and $\mathfrak{p} \notin S$ then $\operatorname{height}(\mathfrak{p}) > i$.

Since $i < d$ and $d = \operatorname{height}(\mathfrak{m})$, none of the primes in S are $\mathfrak{m}$, so by the Lemma, $\mathfrak{m}$ is not contained in the union of the primes in S. Therefore we may choose $x_{i+1} \in \mathfrak{m}$ such that x_{i+1} is not in any of the primes in S. Now let $\mathfrak{p}$ be any prime ideal containing $(x_1, \cdots, x_{i+1})$. We

must show that height$(\mathfrak{p}) \geqslant i+1$. The prime $\mathfrak{p}$ contains one of the primes $\mathfrak{p}'$ that is minimal among those containing $x_1, \cdots, x_i$. If $\mathfrak{p}' \in S$ then $\mathfrak{p} \supsetneqq \mathfrak{p}'$ so height$(\mathfrak{p}) >$ height$(\mathfrak{p}') = i$. On the other hand, if $\mathfrak{p}' \notin S$, then height$(\mathfrak{p}) > i$ also, and so we are done.

We have constructed $x_1, \cdots, x_d$ inductively. Any prime ideal containing all of them has height d, and since $\mathfrak{m}$ is the unique ideal of height d, we see that $r((x_1, \cdots, x_d)) = \mathfrak{m}$. Therefore $(x_1, \cdots, x_d)$ is $\mathfrak{m}$-primary. □

Corollary 18. *Let A be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Then A has an $\mathfrak{m}$-primary ideal that is generated by r elements, where $r \leqslant \dim(A)$. Hence $\delta(A) \leqslant \dim(A)$.*

The inequality $\dim(A) \leqslant d(A)$

We recall the *Artin-Rees* Lemma.

Proposition 19 (Artin-Rees Lemma)**.** *Let A be a Noetherian ring and M a finitely-generated A-module. Let N be a submodule of M and let $\mathfrak{a}$ be an ideal of A. Then there exists a constant r such that*

$$\mathfrak{a}^n M \cap N = \mathfrak{a}^{n-r}(\mathfrak{a}^r M \cap N)$$

for all $n \geqslant r$.

Proof. See Lang's *Algebra*, Corollary X.5.5 on page 429. □

Theorem 20. *Let A be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Then* $\dim(A) \leqslant d(A)$*, where we recall that $d(A)$ is the degree of the polynomial $\chi_{\mathfrak{m}}$ such that $\chi_{\mathfrak{m}}(n) = \ell(A/\mathfrak{m}^n)$ for n large.*

Proof. Let $\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_d$ be a saturated chain of prime ideals such that $\mathfrak{p}_d = \mathfrak{m}$, where $d = \dim(A)$. We will show $d \leqslant d(A)$.

Note that we may replace A by $A/\mathfrak{p}_0$. Indeed, inside of $A/\mathfrak{p}_0$ we have a chain of prime ideals $\mathfrak{p}_i/\mathfrak{p}_0$, so if we can prove the result with this assumption we will have $d \leqslant d(A/\mathfrak{p}_0) \leqslant d(A)$. Thus we may assume that $\mathfrak{p}_0 = 0$ and that A is an integral domain.

Let $0 \neq a \in \mathfrak{p}_1$. Let $\mathfrak{a} = (a)$ and let $\overline{A} = A/\mathfrak{a}$. We will denote the image of $\mathfrak{m}$ in $\overline{A}$ as $\overline{\mathfrak{m}}$. Since $\overline{A}$ has a chain of prime ideals of length $\dim(A) - 1$, we see that $\dim(A) \leqslant \dim\left(\overline{A}\right) + 1$. By induction on $\dim(A)$ we may assume that $\dim\left(\overline{A}\right) \leqslant d\left(\overline{A}\right)$ so it will be sufficient to show that $d\left(\overline{A}\right) \leqslant d(A) - 1$.

By the Artin-Rees Lemma there exists a constant k such that $\mathfrak{a} \cap \mathfrak{m}^n = \mathfrak{m}^{n-k}(\mathfrak{a} \cap \mathfrak{m}^k)$ for $k \geqslant n$. We have a surjective homomorphism $A/\mathfrak{m}^n \longrightarrow \overline{A}/\overline{\mathfrak{m}}^n$ and the kernel is

$$(\mathfrak{a} + \mathfrak{m}^n)/\mathfrak{m}^n \cong \mathfrak{a}/(\mathfrak{a} \cap \mathfrak{m}^n).$$

Thus for sufficiently large n

$$\chi_{\overline{\mathfrak{m}}}(n) = \ell\left(\overline{A}/\overline{\mathfrak{m}}^n\right) = \ell(A/\mathfrak{m}^n) - \ell(\mathfrak{a}/(\mathfrak{a} \cap \mathfrak{m}^n)) = \chi_{\mathfrak{m}}(n) - \ell(\mathfrak{a}/(\mathfrak{a} \cap \mathfrak{m}^n)). \tag{5}$$

This proves that there exists a polynomial $f(n)$ such that for sufficiently large n

$$\ell(\mathfrak{a}/(\mathfrak{a} \cap \mathfrak{m}^n)) = f(n).$$

We will argue that the polynomials f and $\chi_{\mathfrak{m}}$ have the same degree and leading coefficients, so that when they are subtracted, the leading terms cancel. If this is true we will have prove that $d\left(\overline{A}\right) < d(A)$, and we will be done.

By the Artin-Rees Lemma there exists an r such that if $n > r$ then

$$\mathfrak{a} \cap \mathfrak{m}^n = \mathfrak{m}^{n-r}(\mathfrak{a} \cap \mathfrak{m}^r),$$

so

$$f(n) = \ell(\mathfrak{a}/\mathfrak{m}^{n-r}(\mathfrak{a} \cap \mathfrak{m}^r)).$$

We have

$$\mathfrak{a}\mathfrak{m}^r \subseteq \mathfrak{a} \cap \mathfrak{m}^r \subseteq \mathfrak{a}$$

so

$$\mathfrak{a}\mathfrak{m}^n \subseteq \mathfrak{m}^{n-r}(\mathfrak{a} \cap \mathfrak{m}^r) \subseteq \mathfrak{m}^{n-r}\mathfrak{a}$$

so

$$\ell(\mathfrak{a}/\mathfrak{m}^{n-r}\mathfrak{a}) \leqslant \ell(\mathfrak{a}/\mathfrak{m}^{n-r}(\mathfrak{a} \cap \mathfrak{m}^r)) \leqslant \ell(\mathfrak{a}/\mathfrak{m}^n). \tag{6}$$

Now the ideal $\mathfrak{a} = (a)$ is principal so $\mathfrak{a} \cong A$ as a module and

$$\ell(\mathfrak{a}/\mathfrak{m}^n\mathfrak{a}) = \ell(A/\mathfrak{m}^n) = \chi_{\mathfrak{m}}(n)$$

for sufficiently large n. Thus (6) reads

$$\chi_{\mathfrak{m}}(n-r) \leqslant f(n) \leqslant \chi_{\mathfrak{m}}(n).$$

Since we know *a priori* that $f(n)$ is a polynomial, this inequality shows that its degree and leading coefficient are the same as $\chi_{\mathfrak{m}}$. Writing (5) as

$$\chi_{\overline{\mathfrak{m}}}(n) = \chi_{\mathfrak{m}}(n) - f(n)$$

it follows that $d\left(\overline{A}\right) = \deg\left(\chi_{\overline{\mathfrak{m}}}\right) < \deg(\chi_{\mathfrak{m}}) = d(A)$, as required. □

We have now proved all three inequalities

$$\dim(A) \leqslant d(A) \leqslant \delta(A) \leqslant \dim(A)$$

and the Krull dimension theorem is now proved. □