Commutative algebra: some basics on Krull dimension

Paul Nelson

May 21, 2023

Contents

1 Introduction

We recall some definitions and background, record proofs of some of the main theorems regarding Krull dimension, and give some of their geometric interpretations. We mainly follow the course reference by Bosch.

2 Basic definitions

Let A be a ring (always commutative and with identity). In what follows, the symbols $\mathfrak{p}$ or $\mathfrak{p}_i$ always denote prime ideals. We set

$$\dim(A) := \sup\{n \geq 0 : \exists \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n\}.$$

For a prime ideal $\mathfrak{p}$ of A, we set

$$\operatorname{height}(\mathfrak{p}) := \sup\{n \geq 0 : \exists \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subseteq \mathfrak{p}\},$$

$$\operatorname{coheight}(\mathfrak{p}) := \sup\{n \geq 0 : \exists \mathfrak{p} \subseteq \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n\}.$$

For a general ideal $\mathfrak{a}$, we set

$$\operatorname{height}(\mathfrak{a}) := \inf_{\mathfrak{p} \supseteq \mathfrak{a}} \operatorname{height}(\mathfrak{p}),$$

$$\operatorname{coheight}(\mathfrak{a}) := \sup_{\mathfrak{p} \supseteq \mathfrak{a}} \operatorname{coheight}(\mathfrak{p}) = \sup\{n \geq 0 : \exists \mathfrak{a} \subseteq \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n\}.$$

Since prime ideals in the localization $A_{\mathfrak{p}}$ correspond to the primes in A contained in $\mathfrak{p}$, we have

$$\text{height}(\mathfrak{p}) = \dim(A_{\mathfrak{p}}).$$

Since prime ideals in the quotient $A/\mathfrak{a}$ correspond to the primes in A containing $\mathfrak{a}$, we have

$$\text{coheight}(\mathfrak{a}) = \dim(A/\mathfrak{a}).$$

We note the following easy inequality:

Lemma 1. $\text{height}(\mathfrak{a}) + \dim(A/\mathfrak{a}) \leq \dim(A)$.

Proof. It suffices to show that if $\text{height}(\mathfrak{a}) \geq r$ and $\dim(A/\mathfrak{a}) \geq s$, then $\dim(A) \geq r+s$. By hypothesis, we may find primes $\mathfrak{a} \subseteq \mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_s$. Then $\text{height}(\mathfrak{q}_0) \geq \text{height}(\mathfrak{a}) \geq r$, so we may find primes $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r = \mathfrak{q}_0$. Then

$$\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r = \mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_s$$

is a chain of primes in A of length $r+s$. □

We also note:

Lemma 2. *Let* $(A, \mathfrak{m})$ *be a local ring. Then* $\dim(A) = \text{height}(\mathfrak{m})$.

Proof. Let $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ be a chain of primes in A. By enlarging this chain if necessary, we may assume that $\mathfrak{p}_r = \mathfrak{m}$. Thus the suprema in the definitions of $\dim(A)$ and $\text{height}(\mathfrak{m})$ may be taken over the same chains of primes. □

3 Geometric interpretations

Reference for this section: exercises in Chapter 1 of Atiyah–Macdonald.

Let A be a ring. Recall that $\text{Spec}(A)$ denotes the set of prime ideals $\mathfrak{p}$ in A. Each $f \in A$ defines a function

$$f|_{\text{Spec}(A)} : \text{Spec}(A) \to \bigsqcup_{\mathfrak{p} \in \text{Spec}(A)} A/\mathfrak{p}$$

sending $\mathfrak{p}$ to the class of f in the quotient ring $A/\mathfrak{p}$. For $f \in A$ and any subset X of $\text{Spec}(A)$, we may form the restriction $f|_X$ of f to X. For the sake of illustration, note that $f|_{\text{Spec}(A)} = 0$ (i.e., $f|_{\text{Spec}(A)}$ maps each $\mathfrak{p}$ to the zero class in $A/\mathfrak{p}$) if and only if f belongs to the nilradical of A.

For example, we have seen (using the Nullstellensatz) that if $A = \mathbb{C}[X_1, \ldots, X_n]/I$ for some ideal $I \subseteq \mathbb{C}[X_1, \ldots, X_n]$, then the set $\text{Specm}(A)$ of maximal ideals in A is in natural bijection with $V := \{(x_1, \ldots, x_n) \in \mathbb{C}^n : f(x_1, \ldots, x_n) = 0 \text{ for all } f \in I\}$. For each such maximal ideal $\mathfrak{m}$ we may identify $A/\mathfrak{m}$ with $\mathbb{C}$. For $f \in A$, the function $f|_{\text{Specm}(A)}$ then identifies with the obvious map $V \ni (x_1, \ldots, x_n) \mapsto f(x_1, \ldots, x_n) \in \mathbb{C}$.

For a subset S of A, we set

$$V(S) := \{\mathfrak{p} \in \text{Spec}(A) : \mathfrak{p} \supseteq S\} = \{\mathfrak{p} \in \text{Spec}(A) : f(\mathfrak{p}) = 0 \text{ for each } f \in S\}.$$

For finite sets $S = \{f_1, \ldots, f_n\}$ we write simply $V(f_1, \ldots, f_n) := V(S)$. Note that if S generates an ideal $\mathfrak{a}$, then $V(S) = V(\mathfrak{a})$. Given any subset X of $\mathrm{Spec}(A)$, we set

$$I(X) := \cap_{\mathfrak{p} \in X} \mathfrak{p} = \{f \in A : f|_X = 0\}.$$

Recall that a subset of $\mathrm{Spec}(A)$ is called *closed* if it is of the form $V(S)$ for some S; this defines a topology on $\mathrm{Spec}(A)$. Recall that an ideal $\mathfrak{a}$ is *radical* if $\mathrm{rad}(\mathfrak{a}) = \mathfrak{a}$.

Lemma 3.

(i) For each ideal $\mathfrak{a}$ of A, we have $I(V(\mathfrak{a})) = \mathrm{rad}(\mathfrak{a})$.

(ii) For each subset X of $\mathrm{Spec}(A)$, we have $V(I(X)) = \overline{X}$ (the closure of X).

(iii) The maps V and I define mutually-inverse inclusion-reversing bijections between the set of radical ideals of A and the set of closed subsets of $\mathrm{Spec}(A)$.

Proof. The maps I and V are readily seen to be inclusion-reversing (cf. Exercise Sheet #1).

(i) By definition, $I(V(\mathfrak{a})) = \cap_{\mathfrak{p} \in V(\mathfrak{a})} \mathfrak{p} = \cap_{\mathfrak{p} \supseteq \mathfrak{a}} \mathfrak{p} = \mathrm{rad}(\mathfrak{a})$.

(ii) The set $V(I(X))$ is closed and contains X, so it will suffice to verify for each closed set $V(\mathfrak{a})$ containing X that $V(\mathfrak{a}) \supseteq V(I(X))$. From $V(\mathfrak{a}) \supseteq X$ we see that $f|_X = 0$ for all $f \in \mathfrak{a}$, thus $\mathfrak{a} \subseteq I(X)$. Applying the inclusion-reversing map V, we obtain $V(\mathfrak{a}) \supseteq V(I(X))$, as required.

(iii) Immediate by the above.

□

Lemma 4. *Let X be a closed subset of $\mathrm{Spec}(A)$. The following are equivalent:*

(i) $X = V(\mathfrak{p})$ for some prime ideal $\mathfrak{p}$ of A.

(ii) $I(X)$ is a prime ideal of A.

(iii) X is nonempty and may not be written as $X = X_1 \cup X_2$ for closed subsets X_1, X_2 of $\mathrm{Spec}(A)$ except in the trivial case that either $X \subseteq X_1$ or $X \subseteq X_2$.

We say that a closed subset X of $\mathrm{Spec}(A)$ is *irreducible* if it satisfies the equivalent conditions of the preceeding lemma. The irreducible closed subsets of $\mathrm{Spec}(A)$ correspond bijectively to the prime ideals of A.

We note that for any ideal $\mathfrak{a}$, we may identify

$$V(\mathfrak{a}) = \mathrm{Spec}(A/\mathfrak{a}).$$

We note also that if $\mathfrak{p}$ is a prime of A, then the primes of the localization $A_\mathfrak{p}$ correspond to the primes of A contained in $\mathfrak{p}$, hence the spectrum of $A_\mathfrak{p}$ identifies with the set of closed irreducible subsets of $\mathrm{Spec}(A)$ that *contain* $\mathfrak{p}$:

$$\mathrm{Spec}(A_\mathfrak{p}) = \{\mathfrak{q} \in \mathrm{Spec}(A) : \mathfrak{q} \subseteq \mathfrak{p}\} = \{\mathfrak{q} \in \mathrm{Spec}(A) : \mathfrak{p} \in V(\mathfrak{q})\}.$$

By an *irreducible component* of a closed subset X of $\mathrm{Spec}(A)$, we shall mean a maximal closed irreducible subset of X, i.e., a closed irreducible subset $Z \subseteq X$ with the property that if $Z' \subseteq X$ is any closed irreducible subset with $Z' \supseteq Z$, then $Z' = Z$. Using the inclusion-reversing bijections noted above, we verify readily that for any ideal $\mathfrak{a}$, the irreducible components of $X = V(\mathfrak{a})$ correspond bijectively to the set (denoted $\mathrm{Ass}'(\mathfrak{a})$ in lecture) of minimal prime ideals $\mathfrak{p} \supseteq \mathfrak{a}$.

We assume henceforth that A is Noetherian. Then the set of minimal primes of any ideal is finite, and any prime containing an ideal contains a minimal prime of that ideal. It follows that the set of irreducible components of any closed subset X of $\mathrm{Spec}(A)$ is a finite set $\{Z_1, \ldots, Z_n\}$ for which $X = Z_1 \cup \cdots \cup Z_n$.

We define the *dimension* of a closed subset X of $\mathrm{Spec}(A)$ to be

$$\dim(X) = \sup\{n \geq 0 : \exists \text{ closed irreducible subsets } Z_n \subsetneq \cdots \subsetneq Z_0 \subseteq X\}$$

and the *codimension* in the special case that Z is closed irreducible to be

$$\mathrm{codim}(Z) := \sup\{n \geq 0 : \exists \text{ closed irreducible subsets } Z_0 \supsetneq \cdots \supsetneq Z_n \supset Z\}$$

and then in general by

$$\mathrm{codim}(X) := \inf_{Z \subseteq X : \text{closed irreducible}} \mathrm{codim}(Z).$$

Equivalently, $\mathrm{codim}(X)$ is the smallest codimension of any irreducible component of X. We note also that $\dim(X)$ coincides with the largest dimension of any irreducible component of X. We might write $\mathrm{codim}(X)$ as $\mathrm{codim}_{\mathrm{Spec}(A)}(X)$ when we wish to emphasize the reference space $\mathrm{Spec}(A)$.

Using the inclusion-reversing bijections noted above, we see that

$$\dim \mathrm{Spec}\, A = \dim A$$

and more generally that

$$\dim V(\mathfrak{a}) = \mathrm{coheight}\, \mathfrak{a} = \dim A/\mathfrak{a}, \quad \dim X = \mathrm{coheight}\, I(X) = \dim A/I(X),$$

$$\mathrm{codim}\, V(\mathfrak{a}) = \mathrm{height}\, \mathfrak{a}, \quad \mathrm{codim}\, X = \mathrm{height}\, I(X)$$

for any ideal $\mathfrak{a}$ and any closed $X \subseteq \mathrm{Spec}(A)$. Lemma 1 says that $\dim X + \mathrm{codim}\, X \leq \dim \mathrm{Spec}\, A$.

4 Prime avoidance lemma

Lemma 5. *Let A be a ring, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be prime ideals, and let $\mathfrak{a}$ be an ideal contained in the union $\cup \mathfrak{p}_j$. Then there exists an index j for which $\mathfrak{a} \subseteq \mathfrak{p}_j$. Equivalently, if $\mathfrak{a} \not\subseteq \mathfrak{p}_j$ for each j, then $\mathfrak{a} \not\subseteq \cup \mathfrak{p}_j$.*

In "geometric" terms, let $Z_1, \ldots, Z_n \subseteq \mathrm{Spec}(A)$ be closed irreducible subsets, and let $X = V(\mathfrak{a})$ be a closed irreducible subset of $\mathrm{Spec}(A)$, defined by an ideal $\mathfrak{a}$, with the property that $X \not\supseteq Z_j$ for all j. Then there exists $f \in \mathfrak{a}$ with $f|_{Z_j} \neq 0$ for all j. In particular, we may find $f \in A$ with $f|_X = 0$ but $f|_{Z_j} \neq 0$ for all j.

Proof. We verify that if $\mathfrak{a}$ is not contained in any of the $\mathfrak{p}_j$, then it is not contained in their union. For this we may induct on n. The case $n = 1$ is trivial, so suppose $n > 2$. By our inductive hypothesis, we may find for each $i = 1..n$ an element $a_i \in \mathfrak{a}$ with $a_i \notin \mathfrak{p}_j$ whenever $j \neq i$. If moreover $a_i \notin \mathfrak{p}_i$ for some i, then we are done, so suppose otherwise that $a_i \in \mathfrak{p}_i$ for all i. Set $b_i := \prod_{j:j\neq i} a_j$. Then $b_i \notin \mathfrak{p}_i$ (using that $\mathfrak{p}_i$ is prime) but $b_i \in \mathfrak{p}_j$ for all $j \neq i$. It follows that $x := b_1 + \cdots + b_n$ belongs to $\mathfrak{a}$ but not to $\mathfrak{p}_i$ for any i, hence $\mathfrak{a}$ is not contained in the union of the $\mathfrak{p}_i$. □

5 Artin rings

Theorem 6. *Let A be a ring. The following are equivalent:*

(i) A is an Artin ring.

(ii) A is a Noetherian ring of dimension zero.

6 Krull intersection theorem

Theorem 7. *Let $\mathfrak{a}$ be an ideal contained in the Jacobson radical* $\mathrm{Jac}(A)$ *of a Noetherian ring A. Then*

$$\cap_{n\geq 0}\mathfrak{a}^n = 0.$$

Corollary 8. *With $A, \mathfrak{a}$ as before, let M be a finitely-generated module. Then $\cap_{n\geq 0}\mathfrak{a}^n M = 0$.*

Corollary 9. *Let $(A, \mathfrak{m})$ be a Noetherian local ring. Then $\cap_{n\geq 0}\mathfrak{m}^n = 0$.*

For the proof of Theorem 7, the fact that $\mathfrak{a}$ is contained in the Jacobson radical suggests an application of Nakayama's lemma to the ideal $M' := \cap_{n\geq 0}\mathfrak{a}^n$, for which it is clear that $\mathfrak{a}M' \subseteq M'$ and plausible but non-obvious that $\mathfrak{a}M' = M'$. The key tool in establishing the latter is the following:

Lemma 10 (Artin–Rees lemma). *Let A be Noetherian, let $\mathfrak{a}$ be an ideal, let M be a finitely-generated module, and let $M' \leq M$ be a submodule. There exists $n \geq 0$ so that for all $k \geq 0$,*

$$\mathfrak{a}^k(\mathfrak{a}^n M \cap M') = \mathfrak{a}^{n+k}M \cap M'.$$

Taking $M := A, M' := \cap_{n\geq 0}\mathfrak{a}^n$, $k := 1$ in the Artin–Rees lemma gives $\mathfrak{a}^n M \cap M' = \mathfrak{a}^{n+k}M \cap M' = M'$ and hence $\mathfrak{a}M' = M'$; we then conclude the proof of Theorem 7 by Nakayama, as indicated above.

The proof of Artin–Rees reduces formally to the case $k = 1$, and the containment

$$\mathfrak{a}(\mathfrak{a}^n M \cap M') \subseteq \mathfrak{a}^{n+1}M \cap M'$$

is clear. The proof of the trickier reverse containment is expressed most transparently using the graded ring

$$\tilde{A} := \boxplus_{i\geq 0}A_i = \{a = (a_i)_{i\geq 0} : a_i \in A_i\}, \quad A_i := \mathfrak{a}^i,$$

where the multiplication law extends the bilinear maps $\mathfrak{a}^i \times \mathfrak{a}^j \to \mathfrak{a}^{i+j}$:

$$(a \cdot b)_k = \sum_{i+j=k} a_i b_j.$$

This graded ring acts by the rule $(a \cdot m)_k := \sum_{i+j=k} a_i m_j$ on the graded module

$$\tilde{M} := \boxplus_{i \geq 0} M_i, \quad M_i := \mathfrak{a}^i M,$$

and its graded submodule

$$\tilde{M'} := \boxplus_{i \geq 0} M'_i, \quad M'_i := \mathfrak{a}^i M \cap M'.$$

Since $\mathfrak{a}$ is finitely-generated as a module over A, $\tilde{A}$ is finitely-generated as an algebra over $A_0 = A$; by the Hilbert basis theorem, it follows that $\tilde{A}$ is Noetherian. The module M is finitely-generated over A, from which it follows readily that the graded module $\tilde{M}$ is finitely-generated over $\tilde{A}$; since the ring $\tilde{A}$ is Noetherian, so is the module $\tilde{M}$, hence its submodule $\tilde{M'}$ is finitely-generated. Choose n large enough that the module $\tilde{M'}$ is generated by $\boxplus_{0 \leq i \leq n} M'_i$, thus

$$\tilde{M'} = \tilde{A} \boxplus_{0 \leq i \leq n} M'_i.$$

By taking the degree $n+1$ homogeneous component of this identity, we see that

$$\begin{aligned} \mathfrak{a}^{n+1} M \cap M' = M'_{n+1} &= \sum_{0 \leq i \leq n} A_{n+1-i} M'_i = \sum_{0 \leq i \leq n} \mathfrak{a}^{n+1-i} (\mathfrak{a}^i M \cap M') \\ &\subseteq \sum_{0 \leq i \leq n} \mathfrak{a}(\mathfrak{a}^n M \cap \mathfrak{a}^{n-i} M') \subseteq \mathfrak{a}(\mathfrak{a}^n M \cap M'), \end{aligned}$$

giving the required reverse containment. The proof of Artin–Rees and hence of the Krull intersection theorem is then complete.

7 Kernel of localization with respect to a prime

Let $\mathfrak{p}$ be a prime ideal in a Noetherian ring A. Let $\mathfrak{p}^{(n)}$ denote the nth symbolic power; it is the $\mathfrak{p}$-primary ideal given by $A \cap \mathfrak{p}^n A_{\mathfrak{p}} := \iota^*((\iota_* \mathfrak{p})^n)$, where $\iota : A \to A_{\mathfrak{p}}$ denotes the localization map.

Theorem 11. $\ker(\iota) = \cap_{n \geq 0} \mathfrak{p}^{(n)}$.

Proof. Set $\mathfrak{m} := \iota_* \mathfrak{p}$. We have $\ker(\iota) = \iota^{(-1)}(0)$ and $\iota^{-1}(\cap_{n \geq 0} \mathfrak{m}^n) = \cap_{n \geq 0} \mathfrak{p}^{(n)}$, so it suffices to show that $\cap_{n \geq 0} \mathfrak{m}^n = 0$, which is the content of Corollary 9 of the Krull intersection theorem applied to the Noetherian local ring $(A_{\mathfrak{p}}, \mathfrak{m})$. □

8 Krull's theorems on heights and dimensions

8.1 Principal ideal theorem

We start with the special case to which the general one will eventually be reduced:

Lemma 12. *Let $(A, \mathfrak{m})$ be a local Noetherian integral domain. Suppose that $\mathfrak{m}$ is a minimal prime of some principal ideal (f), with $f \in \mathfrak{m}$. Then $\mathfrak{m}$ and (0) are the only primes of A.*

In "geometric" terms: suppose that $\{\mathfrak{m}\} = V(f)$ for some $f \in \mathfrak{m}$. Then $\mathrm{Spec}(A) = \{\mathfrak{m}, (0)\}$.

Proof. Let $\mathfrak{p}$ be any prime in A other than $\mathfrak{m}$. Necessarily $\mathfrak{p} \subsetneq \mathfrak{m}$; our task is to show that $\mathfrak{p} = (0)$. Since A is a domain, it will suffice to show for some n that $\mathfrak{p}^n = (0)$. Recall that $\mathfrak{p}^{(n)}$ denotes the nth symbolic power of $\mathfrak{p}$, given here with respect to the injective localization map $A \hookrightarrow A_{\mathfrak{p}}$ by $\mathfrak{p}^{(n)} = A \cap \mathfrak{p}^n A_{\mathfrak{p}}$; it is a $\mathfrak{p}$-primary ideal which contains $\mathfrak{p}^n$. It will then suffice to verify that $\mathfrak{p}^{(n)} = (0)$ for some n. By §7, we have $\cap_{n \geq 0} \mathfrak{p}^{(n)} = \ker(A \to A_{\mathfrak{p}}) = (0)$, so it will suffice to verify that the chain of ideals $\mathfrak{p}^{(n)}$ stabilizes, i.e., that $\mathfrak{p}^{(n)} = \mathfrak{p}^{(n+1)}$ for large n.

Set $\overline{A} := A/(f)$, $\overline{\mathfrak{m}} := \mathfrak{m}/(f)$. Our hypotheses imply that $\overline{\mathfrak{m}}$ is the only prime ideal of $\overline{A}$. Thus $\overline{A}$ is a Noetherian ring of dimension 0. By Theorem 6, it follows that $\overline{A}$ is an Artin ring. Thus the descending chain of ideals $\mathfrak{p}^{(n)} + (f)$ must stabilize; in particular,

$$\mathfrak{p}^{(n)} \subseteq \mathfrak{p}^{(n+1)} + (f)$$

for large n. This says that any $x \in \mathfrak{p}^{(n)}$ may be written $x = y + zf$ for some $y \in \mathfrak{p}^{(n+1)}$ and $z \in A$. In that case, $x - y \in \mathfrak{p}^{(n)}$, and so $z \in (\mathfrak{p}^{(n)} : f)$. Since $\mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary and $f \notin \mathfrak{p}$, we have $(\mathfrak{p}^{(n)} : f) = \mathfrak{p}^{(n)}$, and so in fact $z \in \mathfrak{p}^{(n)}$. Thus

$$\mathfrak{p}^{(n)} \subseteq \mathfrak{p}^{(n+1)} + \mathfrak{p}^{(n)} f,$$

and in fact equality holds, with the reverse containment being clear. This says that $fM = M$ for the finitely-generated module $M := \mathfrak{p}^{(n)}/\mathfrak{p}^{(n+1)}$. Since $f \in \mathfrak{m} = \mathrm{Jac}(A)$, it follows from Nakayama's lemma that $M = 0$. Thus $\mathfrak{p}^{(n)} = \mathfrak{p}^{(n+1)}$ for large n, as was to be shown. □

Theorem 13. *Let A be a Noetherian ring, and let $f \in A$.*

(i) Every minimal prime $\mathfrak{p}$ of (f) satisfies $\mathrm{height}(\mathfrak{p}) \leq 1$.

(ii) If f is a non-zerodivisor, then every minimal prime $\mathfrak{p}$ of (f) satisfies $\mathrm{height}(\mathfrak{p}) = 1$.

In "geometric" terms, $\mathrm{codim}(Z) \leq 1$ *for each irreducible component Z of $V(f) \subseteq \mathrm{Spec}(A)$; if f is a non-zerodivisor, then* $\mathrm{codim}(Z) = 1$ *for each such Z. (This "generalizes" the fact from linear algebra that the kernel of a linear functional has codimension ≤ 1, with equality whenever the functional is nonzero.)*

Proof. To deduce (ii) from (i), suppose that some minimal prime $\mathfrak{p}$ of (f) has $\mathrm{height}(\mathfrak{p}) = 0$. Then $\mathfrak{p}$ is a minimal prime of (0), hence consists of zero-divisors, and so f is a zerodivisor.

Our main task is thus to establish (i). We must verify that if $\mathfrak{p}_2$ is a minimal prime of (f) and if $\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2$ are inclusions of prime ideals, then $\mathfrak{p}_0 = \mathfrak{p}_1$. After replacing A by its quotient $A/\mathfrak{p}_0$, we may reduce to the case that $\mathfrak{p}_0 = (0)$;

in particular, A is a local Noetherian domain. After then replacing A by its localization $A_{\mathfrak{p}_2}$, we reduce further to the case that A is a local Noetherian domain whose maximal ideal $\mathfrak{p}_2$ is a minimal prime of (f). We now appeal to the previous lemma. □

We will often apply the above result in a local context:

Corollary 14. *Let $(A, \mathfrak{m})$ be a Noetherian local ring. Suppose there exists $f \in A$ for which $\mathfrak{m}$ is the unique prime containing f, thus $V(f) = \{\mathfrak{m}\}$. Then* $\dim(A) = \text{height}(\mathfrak{m}) \leq 1$.

Proof. Given that $\mathfrak{m}$ is maximal, our assumption is equivalent to requiring that $\mathfrak{m}$ be a minimal prime of (f). □

For the sake of illustration, let's reformulate Theorem 13 in the contrapositive. Let A be a Noetherian ring. Let $\mathfrak{p}_0 \subsetneq \mathfrak{p}_2$ be an inclusion of primes in A. By an *intermediary prime* we will mean a prime $\mathfrak{p}_1$ for which $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2$.

Corollary 15. *The following are equivalent:*

(i) There exists an intermediary prime.

(ii) For each $f \in \mathfrak{p}_2$ there exists an intermediary prime containing f.

In "geometric" terms, let $Y_2 \subsetneq Y_0$ be irreducible closed subsets of $\text{Spec}(A)$. *Then either there are no irreducible closed subsets Y_1 contained strictly between Y_2 and Y_0, or for each $f \in I(Y_2)$ there exists an irreducible closed subset $Y_2 \subsetneq Y_1 \subsetneq Y_0$ with $Y_1 \subseteq Z(f)$.*

Proof. We need only show that (i) implies (ii). If (ii) fails, then we may find $f \in \mathfrak{p}_2$ not contained in any intermediary primes. In other words, after replacing A with $A/\mathfrak{p}_0$ as necessary to reduce to the case that $\mathfrak{p}_0$ is a minimal prime of A, we are given that $\mathfrak{p}_2$ is a minimal prime of (f). By Krull's principal ideal theorem, it follows that $\text{height}(\mathfrak{p}_2) \leq 1$; thus there exist no intermediary primes, and so (i) fails. □

8.2 Dimension theorem

Theorem 16. *Let A be a Noetherian ring, and let $f_1, \ldots, f_n \in A$. Then each minimal prime $\mathfrak{p}$ of $(f_1, \ldots, f_r)$ satisfies* $\text{height}(\mathfrak{p}) \leq r$. *In particular,* $\text{height}(f_1, \ldots, f_r) \leq r$.

In "geometric" terms, $\text{codim}(Z) \leq r$ *for each irreducible component Z of $V(f_1, \ldots, f_r) \subseteq \text{Spec}(A)$. (This "generalizes" the fact from linear algebra that the solution set to a system of r linear equations has codimension $\leq r$.)*

Here's a lemma that I think clarifies the key step in the proof.

Lemma 17. Let $(A, \mathfrak{m})$ be a Noetherian local ring, and let $f_1, \ldots, f_r \in \mathfrak{m}$ with $V(f_1, \ldots, f_r) = \{\mathfrak{m}\}$. Let $\mathfrak{p} \subsetneq \mathfrak{m}$ be a prime with no prime strictly contained between $\mathfrak{p}$ and $\mathfrak{m}$. Then there exist $g_1, \ldots, g_r \in \mathfrak{m}$ for which

1. $V(g_1, \ldots, g_r) = \{\mathfrak{m}\}$ *and*

2. $\mathfrak{p}$ *contains and is a minimal prime of* $(g_1, \ldots, g_{r-1})$.

In "geometric" terms, let Z be a closed irreducible subset of $\mathrm{Spec}(A)$ *that is minimal among the closed irreducible sets that properly contain* $\{\mathfrak{m}\}$. *Then we may find $g_1, \ldots, g_r$ for which $V(g_1, \ldots, g_r) = \{\mathfrak{m}\}$ and for which Z is an irreducible component of $V(g_1, \ldots, g_{r-1})$.*

Proof. Since $\mathfrak{m}$ is the unique prime ideal containing $(f_1, \ldots, f_r)$, we may assume after reindexing $f_1, \ldots, f_r$ as necessary that $f_r \notin \mathfrak{p}$. Then the ideal $\mathfrak{p} + (f_r)$ strictly contains $\mathfrak{p}$ and is contained in $\mathfrak{m}$; our hypotheses on $\mathfrak{p}$ imply that $\mathfrak{m}$ is the only prime ideal containing $\mathfrak{p} + (f_r)$, i.e., that $V(\mathfrak{p} + (f_r)) = \{\mathfrak{m}\}$, or that $\mathrm{rad}(\mathfrak{p} + (f_r)) = \mathfrak{m}$. In particular, for each $1 \leq i \leq r-1$ we may find n_i for which $f_i^{n_i} \in \mathfrak{p} + (f_r)$, say

$$f_i^{n_i} = g_i + z_i f_r \text{ with } g_i \in \mathfrak{p}, z_i \in A.$$

We claim that the conclusion of the lemma is now satisfied with $g_1, \ldots, g_{r-1}$ as above and $g_r := f_r$:

1. The above equation shows that any prime $\mathfrak{q}$ that contains $g_1, \ldots, g_{r-1}, f_r$ also contains $f_i^{n_i}$ and hence f_i for $1 \leq i \leq r$, hence $\mathfrak{q} = \mathfrak{m}$. Thus $V(g_1, \ldots, g_r) = \{\mathfrak{m}\}$.

2. It's clear by construction that $\mathfrak{p}$ contains $(g_1, \ldots, g_{r-1})$. There is thus a minimal prime $\mathfrak{p}'$ of $(g_1, \ldots, g_{r-1})$ contained in $\mathfrak{p}$; we must verify that $\mathfrak{p} = \mathfrak{p}'$. (Geometrically, $\mathfrak{p}'$ corresponds to an irreducible component Z' of $V(g_1, \ldots, g_{r-1})$ containing Z.) To see this, consider the quotient ring $\overline{A} := A/(g_1, \ldots, g_{r-1})$. Let

$$\overline{\mathfrak{m}} \supsetneq \overline{\mathfrak{p}} \supseteq \overline{\mathfrak{p}'} \tag{1}$$

   denote the chain of primes in $\overline{A}$ given by the image of $\mathfrak{m} \supsetneq \mathfrak{p} \supseteq \mathfrak{p}' \supseteq (g_1, \ldots, g_{r-1})$. Then $(\overline{A}, \overline{\mathfrak{m}})$ is a Noetherian local ring, and our task is equivalent to showing that $\overline{\mathfrak{p}} = \overline{\mathfrak{p}'}$. Let $f \in \overline{A}$ denote the image of f_r. The primes of $\overline{A}$ containing f are in bijection with the primes of A containing $g_1, \ldots, g_{r-1}, f_r$, so $V_{\overline{A}}(f) = \{\overline{\mathfrak{m}}\}$. By Krull's principal ideal theorem (in the form of Corollary 14), it follows that $\mathrm{height}(\overline{\mathfrak{m}}) \leq 1$. From (1) we then deduce that $\overline{\mathfrak{p}} = \overline{\mathfrak{p}'}$, as required. (Intuitively, by choosing f_r not to vanish on any irreducible component of $V(f_1, \ldots, f_{r-1})$, we guarantee that appending it to the set of generators has the effect of knocking down the dimension of each such component by 1.)

□

We now deduce Theorem 16. We must show that if $\mathfrak{p}$ is a minimal prime of $(f_1, \ldots, f_r)$, then $\mathrm{height}(\mathfrak{p}) \leq r$. We may assume without loss of generality (replacing A with $A_{\mathfrak{p}}$ and $\mathfrak{p}$ with $\mathfrak{p}_{\mathfrak{p}}$, which doesn't change the height of or

minimality assumption on the latter) that $(A, \mathfrak{p})$ is a Noetherian local ring with $V(f_1, \ldots, f_r) = \{\mathfrak{p}\}$; we must show then that $\text{height}(\mathfrak{p}) \leq r$. We do this by induction on r. The case $r = 1$ is given by Krull's principal ideal theorem, so suppose $r > 1$. Let $\mathfrak{q} \subsetneq \mathfrak{p}$ be a maximal element of the set of primes strictly contained in $\mathfrak{p}$; it will suffice then to show that $\text{height}(\mathfrak{q}) \leq r - 1$. By Lemma 17, we may assume without loss of generality that $\mathfrak{q}$ is a minimal prime of $(f_1, \ldots, f_{r-1})$; the required inequality then follows from our inductive hypothesis.

Corollary 18. *Let $\mathfrak{a}$ be an ideal in a Noetherian ring A. Then* $\text{height}(\mathfrak{a}) < \infty$.

Proof. Write $\mathfrak{a} = (f_1, \ldots, f_r)$. Then $\text{height}(\mathfrak{a}) \leq r$. □

Corollary 19. *Let $(A, \mathfrak{m})$ be a Noetherian local ring. Then* $\dim(A) = \text{height}(\mathfrak{m}) < \infty$.

Proof. Use Lemma 2. □

Remark 20. Dimension theory works best for *local* Noetherian rings: there exist non-local Noetherian rings A with $\dim(A) = \infty$. On the other hand, the height of an ideal in a Noetherian ring A is always finite, regardless of whether A is local.

8.3 Converse to the dimension theorem

Theorem 21. *Let A be a Noetherian ring. Let r, s be nonnegative integers with $s \leq r$. Let $\mathfrak{a}$ be an ideal with* $\text{height}(\mathfrak{a}) \geq r$, *and let $f_1, \ldots, f_s \in \mathfrak{a}$ satisfy* $\text{height}(f_1, \ldots, f_s) = s$. *Then there exist $f_{s+1}, \ldots, f_r \in \mathfrak{a}$ so that* $\text{height}(f_1, \ldots, f_i) = i$ *for all $s \leq i \leq r$.*

Proof. It suffices (after finitely many iterations) to consider the case $s = r - 1$. For each minimal prime $\mathfrak{q}$ of $(f_1, \ldots, f_{r-1})$, we have $\text{height}(\mathfrak{q}) = r - 1$ (here the inequality "$\geq$" follows from our assumption $\text{height}(f_1, \ldots, f_{r-1}) = r - 1$, while "$\leq$" follows from the Krull dimension theorem); it follows from this and the inequality $\text{height}(\mathfrak{a}) \geq r$ that $\mathfrak{a} \not\subseteq \mathfrak{q}$. By the prime avoidance lemma (§4), we may find an element $f_r \in \mathfrak{a}$ not contained in any minimal prime of $(f_1, \ldots, f_{r-1})$. We claim then that $\text{height}(f_1, \ldots, f_r) = r$. Consider any minimal prime $\mathfrak{q}$ of $(f_1, \ldots, f_r)$; we must verify that $\text{height}(\mathfrak{q}) = r$. The upper bound "$\leq$" follows as before from the Krull dimension theorem. For the lower bound, note that $\mathfrak{q}$ contains $(f_1, \ldots, f_{r-1})$, and so contains some minimal prime $\mathfrak{q}'$ of $(f_1, \ldots, f_{r-1})$. By construction, we have $f_r \in \mathfrak{q}$ but $f_r \notin \mathfrak{q}'$, hence $\mathfrak{q} \supsetneq \mathfrak{q}'$, and so $\text{height}(\mathfrak{q}) > \text{height}(\mathfrak{q}') = r - 1$. This forces $\text{height}(\mathfrak{q}) = r$, as required. □

Remark 22. It may be instructive to recast in geometric terms some parts of the proof given above. Our hypothesis is that each irreducible component of $V(f_1, \ldots, f_{r-1})$ has codimension $r - 1$, while each irreducible component of $V(\mathfrak{a})$ has codimension $\geq r$. It follows readily that $V(\mathfrak{a})$ contains no irreducible component of $V(f_1, \ldots, f_{r-1})$. By the prime avoidance lemma, we may thus

find an element $f_r \in \mathfrak{a}$ which does not vanish on any irreducible component of $V(f_1, \ldots, f_{r-1})$. Now, each irreducible component Z of $V(f_1, \ldots, f_r)$ is contained in some irreducible component Z' of $V(f_1, \ldots, f_{r-1})$. Since $f|_{Z'} \neq 0$, this containment must be strict: $Z \subsetneq Z'$. Therefore $\operatorname{codim}(Z) \geq r$; Krull then gives $\operatorname{codim}(Z) \leq r$, hence $\operatorname{codim}(Z) = r$, hence $\operatorname{codim}(V(f_1, \ldots, f_r)) = r$, as required.

Corollary 23. *Let $\mathfrak{p}$ be a prime ideal of height r in a Noetherian ring A. Then there exist $f_1, \ldots, f_r \in \mathfrak{p}$ so that $\mathfrak{p}$ is a minimal prime of $(f_1, \ldots, f_r)$.*

In "geometric" terms, every closed irreducible subset Z of $\operatorname{Spec}(A)$ with $\operatorname{codim}(Z) = r$ arises as an irreducible component of $V(f_1, \ldots, f_r) \subseteq \operatorname{Spec}(A)$ for some $f_1, \ldots, f_r \in A$.

Proof. We apply the previous result with $s = 0$. □

Here's a slightly sharper variant:

Theorem 24. *Let $\mathfrak{p}$ be a prime ideal in a Noetherian ring with $\operatorname{height}(\mathfrak{p}) = r$. Let $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r = \mathfrak{p}$ be a chain of primes realizing the height of $\mathfrak{p}$. (Note that this forces $\operatorname{height}(\mathfrak{p}_i) = i$ for all i.) There exist $f_1, \ldots, f_r$ so that for each $0 \leq i \leq r$,*

- *$\operatorname{height}(f_1, \ldots, f_i) = i$, and*
- *$\mathfrak{p}_i$ is a minimal prime of $(f_1, \ldots, f_i)$ for each $0 \leq i \leq r$.*

In "geometric" terms, let $Z_0 \supsetneq \cdots \supsetneq Z_r$ be closed irreducible subsets of $\operatorname{Spec}(A)$ with $\operatorname{codim}(Z_r) = r$. (Note that this forces $\operatorname{codim}(Z_i) = i$ for all i.) Then we may find $f_1, \ldots, f_r \in A$ so that for each $0 \leq i \leq r$,

- *every irreducible component of $V(f_1, \ldots, f_i)$ has codimension i, and*
- *Z_i is an irreducible component of $V(f_1, \ldots, f_i)$.*

Proof. We argue by induction as above, choosing f_{i+1} to belong to $\mathfrak{p}_{i+1}$ but not to any minimal prime of $(f_1, \ldots, f_i)$. □

9 Systems of parameters

9.1 A characterization of dimension

Lemma 25. *Let $(A, \mathfrak{m})$ be a Noetherian local ring and $x_1, \ldots, x_n \in \mathfrak{m}$. The following conditions are equivalent:*

(i) $\mathfrak{m}$ is the only prime containing $(x_1, \ldots, x_n)$, i.e.:

$$V((x_1, \ldots, x_n)) = \{\mathfrak{m}\}.$$

(ii) $\mathfrak{m}$ is a minimal prime of $(x_1, \ldots, x_n)$.

(iii) $\operatorname{rad}((x_1, \ldots, x_n)) = \mathfrak{m}$.

(iv) The ideal $(x_1, \ldots, x_n)$ *is* $\mathfrak{m}$*-primary.*

Proof. The equivalence of (i),(ii) and (iii) follows from the assumption that $\mathfrak{m}$ is maximal. The equivalence of (iii) and (iv) follows from the fact that an ideal is primary whenever its radical is a maximal ideal. □

Theorem 26. *Let* $(A, \mathfrak{m})$ *be a Noetherian local ring. Then* $\dim(A)$ *is the smallest integer* n *for which the equivalent conditions of Lemma 25 are satisfied, i.e.,*

$$\dim(A) = \min\{n \geq 0 : \exists x_1, \ldots, x_n \in \mathfrak{m} \text{ with } V((x_1, \ldots, x_n)) = \{\mathfrak{m}\}\}.$$

Proof. If there exist $x_1, \ldots, x_n$ with $V((x_1, \ldots, x_n)) = \{\mathfrak{m}\}$ then Krull's dimension theorem implies that $\dim(A) = \operatorname{height}(\mathfrak{m}) \leq n$. If $n = \dim(A)$, then the "converse to Krull" (Corollary 23) implies that there exist $x_1, \ldots, x_n$ with $V((x_1, \ldots, x_n)) = \{\mathfrak{m}\}$. □

Theorem 26 will be very useful as a tool for giving *upper bounds* on the dimension of a Noetherian local ring $(A, \mathfrak{m})$: to show that $\dim(A) \leq n$, it suffices to construct elements $x_1, \ldots, x_n$ with $V((x_1, \ldots, x_n)) = \mathfrak{m}$.

9.2 Definition

Definition 27. Let $(A, \mathfrak{m})$ be a Noetherian local ring. We say that $x_1, \ldots, x_n \in \mathfrak{m}$ form a *system of parameters* for $\mathfrak{m}$ if

(i) $n = \dim(A) = \operatorname{height}(\mathfrak{m})$, and

(ii) the equivalent conditions of Lemma 25 are satisfied, e.g., if $V((x_1, \ldots, x_n)) = \{\mathfrak{m}\}$.

Theorem 26 implies that systems of parameters exist.

9.3 Extensions of partial systems of parameters

Let $(A, \mathfrak{m})$ be a Noetherian local ring. Given a collection of $x_1, \ldots, x_r \in \mathfrak{m}$ of elements of its maximal ideal, we aim to understand when this collection may be extended to a system of parameters. To that end, define the quotient ring $\overline{A} := A/(x_1, \ldots, x_r)$; it is a Noetherian local ring with maximal ideal $\overline{\mathfrak{m}}$ given by the image of $\mathfrak{m}$, and satisfies the following general dimension lower-bound:

Lemma 28. $\dim(\overline{A}) \geq \dim(A) - r$.

Proof. Write $s = \dim(\overline{A})$. Choose elements $y_1, \ldots, y_s \in A$ whose images $\overline{y_1}, \ldots, \overline{y_s} \in \overline{A}$ form a system of parameters for $\overline{\mathfrak{m}}$. In particular, $\overline{\mathfrak{m}}$ is the only prime containing $(\overline{y_1}, \ldots, \overline{y_s})$. It follows that $\mathfrak{m}$ is the only prime containing $(x_1, \ldots, x_r, y_1, \ldots, y_s)$. From this we deduce the upper bound $\dim(A) \leq r + s$, which rearranges to the required inequality. □

Theorem 29. *Among the following assertions, (i) implies (ii) and (iii), while (ii) and (iii) are equivalent.*

(i) $\operatorname{height}((x_1, \ldots, x_r)) = r$.

(ii) *We may extend* $\{x_1, \ldots, x_r\}$ *to a system of parameters for* $\mathfrak{m}$.

(iii) $\dim(\overline{A}) = \dim(A) - r$.

Proof.

- (i) implies (ii): Set $n := \operatorname{height}(\mathfrak{m}) = \dim(A)$. Then every prime in A has height $\leq n$, so $r \leq n$. By Theorem 21, we may find $x_{r+1}, \ldots, x_n$ for which $\operatorname{height}((x_1, \ldots, x_n)) = n$, i.e., so that n is the minimal height among primes containing $(x_1, \ldots, x_n)$. Since $\mathfrak{m}$ is the unique prime in A of height n, we deduce that it is the only prime containing $(x_1, \ldots, x_n)$. Thus $x_1, \ldots, x_n$ is a system of parameters.
- (i) implies (iii): we combine Lemma 28 with the easy inequality $\dim(A) \geq \dim(\overline{A}) + \operatorname{height}((x_1, \ldots, x_r))$ (cf. Lemma 1). (This implication has been included redundantly for the sake of illustration.)
- (ii) implies (iii): Suppose we can extend $x_1, \ldots, x_r$ to a system of parameters $x_1, \ldots, x_r, y_1, \ldots, y_s$ for $\mathfrak{m}$. Then $r+s = \dim(A)$ and $V((\overline{y_1}, \ldots, \overline{y_s})) = \overline{\mathfrak{m}}$, whence $s \geq \dim(\overline{A})$; by Lemma 28, we deduce that $s \geq \dim(\overline{A}) \geq \dim(A) - r = s$, so equality holds and $\dim(\overline{A}) = s$, as required.
- (iii) implies (ii): Suppose that $s := \dim(\overline{A}) = \dim(A) - r$. Let $y_1, \ldots, y_s \in \mathfrak{m}$ be such that their images $\overline{y_1}, \ldots, \overline{y_s}$ form a system of parameters for $\overline{\mathfrak{m}}$. Then $V((x_1, \ldots, x_r, y_1, \ldots, y_s)) = \{\mathfrak{m}\}$ and $r + s = \dim(A)$, so $x_1, \ldots, x_r, y_1, \ldots, y_s$ gives the required extension of $x_1, \ldots, x_r$ to a system of parameters for $\mathfrak{m}$.

□

Corollary 30. *Let* $(A, \mathfrak{m})$ *be a Noetherian local ring, and let* $f \in \mathfrak{m}$ *be a non-zerodivisor. Then*

$$\dim(A/(f)) = \dim(A) - 1.$$

Proof. Since f is a non-zerodivisor, Krull's principal ideal theorem implies that $\operatorname{height}((f)) = 1$. Theorem 29 applies with $r := 1$ and $x_1 := f$ to produce an extension of $\{f\}$ to a system of parameters $f, y_1, \ldots, y_s$ for A, with $s := \dim(A/(f))$. In particular, $\dim(A) = s + 1$, as required. □

10 Dimensions of polynomial rings

Theorem 31. *Let* A *be a Noetherian ring, and* $n \in \mathbb{Z}_{\geq 0}$. *Then*

$$\dim A[X_1, \ldots, X_n] = \dim A + n.$$

Proof. By iterating, it suffices to consider the case $n = 1$. Set $r := \dim(A)$. We must verify that $\dim A[X] = r + 1$. Let $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ be a chain of primes in A of length realizing the dimension of A. Then

$$\mathfrak{p}_0 A[x] \subsetneq \cdots \subsetneq \mathfrak{p}_r A[X] \subsetneq \mathfrak{p}_r A[X] + XA[X]$$

is readily seen to give a chain of primes in $A[X]$ of length $r+1$, hence $\dim A[X] \geq r+1$. The upper bound is trickier. It will suffice to show for each maximal ideal $\mathfrak{m} \subseteq A[X]$ that $\text{height}(\mathfrak{m}) \leq r + 1$. Set $\mathfrak{p} := \mathfrak{m} \cap A$; it is a prime ideal. We may replace A with its localization $A_\mathfrak{p}$ and $A[X]$ with $(A[X])_\mathfrak{p} = A_\mathfrak{p}[X]$ to reduce to the case that $(A, \mathfrak{p})$ is a Noetherian local ring. The quotient $A/\mathfrak{p}$ is then a field and so the ring $A[X]/\mathfrak{p}A[X] = A/\mathfrak{p}[X]$ is then a PID. The image of $\mathfrak{m}$ in the latter ring is thus principal. We may thus write $\mathfrak{m} = \mathfrak{p}A[X] + fA[X]$ for some $f \in A[X]$. Let $x_1, \ldots, x_r \in \mathfrak{p}$ be a system of parameters for $\mathfrak{p}$. Then $\mathfrak{m}$ is the only prime containing $(x_1, \ldots, x_r, f)$: any such prime $\mathfrak{q}$ contains $x_1, \ldots, x_r$ and hence contains $\mathfrak{p}$, and so identifies with a prime ideal in the quotient $A/\mathfrak{p}[X]$ that contains the image of f, whence $\mathfrak{q} = \mathfrak{m}$. It follows from Theorem 26 that $\dim(A) = \text{height}(\mathfrak{m}) \leq r + 1$, as required. □

For example:

Proposition 32. *Let $A := \mathbb{C}[X_1, \ldots, X_n]$, and let $\mathfrak{m}$ be a maximal ideal, thus $\mathfrak{m} = (X_1 - x_1, \ldots, X_n - x_n)$ for some $(x_1, \ldots, x_n) \in \mathbb{C}^n$. Then* $\text{height}(\mathfrak{m}) = n$. *The localization $A_\mathfrak{m}$ is a local ring of dimension n, whose maximal ideal is generated by a system of parameters.*

Proof. The ideals $\mathfrak{p}_i := (X_1 - x_1, \ldots, X_i - x_i)$ $(i = 0..n)$ are prime, distinct and increasing to $\mathfrak{p}_n = \mathfrak{m}$, so $\text{height}(\mathfrak{m}) \geq n$. Conversely, it's clear that $\text{height}(\mathfrak{m}) \leq \dim(A) = n$. Therefore $\text{height}(\mathfrak{m}) = n$. The assertion concerning $A_\mathfrak{m}$ then follows from the identity $\dim(A_\mathfrak{m}) = \text{height}(\mathfrak{m})$ and the fact that $\mathfrak{m}$ is generated by $X_1 - x_1, \ldots, X_n - x_n$. □

11 Preliminaries on regular local rings

Let $(A, \mathfrak{m})$ be a Noetherian local ring of dimension $d := \dim(A) = \text{height}(\mathfrak{m})$. Denote by $k := A/\mathfrak{m}$ the residue field. For any module M, the quotient $M/\mathfrak{m}M$ is then naturally a k-vector space. This consideration applies in particular when $M = \mathfrak{m}$, so that $M/\mathfrak{m}M = \mathfrak{m}/\mathfrak{m}^2$.

Lemma 33. *In general,* $\dim_k \mathfrak{m}/\mathfrak{m}^2 \geq d$. *The following are equivalent:*

(i) $\mathfrak{m}$ *is generated by d elements, necessarily a system of parameters.*

(ii) $\dim_k \mathfrak{m}/\mathfrak{m}^2 = d$.

Proof. Set $r := \dim_k \mathfrak{m}/\mathfrak{m}^2$.

For the first inequality, suppose $x_1, \ldots, x_r \in \mathfrak{m}$ have the property that their images give a k-basis of $\mathfrak{m}/\mathfrak{m}^2$. By Nakayama's lemma, it follows that $x_1, \ldots, x_r$

generate $\mathfrak{m}$. By Krull's dimension theorem, it follows that $d = \text{height}(\mathfrak{m}) \leq r$, as required.

(i) implies (ii): If $x_1, \ldots, x_d$ generate $\mathfrak{m}$, then their images span $\mathfrak{m}/\mathfrak{m}^2$, whence $d \geq r$. Comparing with the reverse inequality which holds in general, we deduce that $d = r$.

(ii) implies (i): Assuming (ii), we may find $x_1, \ldots, x_d \in \mathfrak{m}$ which generate $\mathfrak{m}/\mathfrak{m}^2$, hence (by Nakayama) generate $\mathfrak{m}$, giving (i). □

12 Basics on integral extensions

Let $A \subseteq B$ be rings. The discussion that follows applies with minor modifications to any A-algebra $\phi : A \to B$, by replacing A with $\phi(A)$.

We say that $x \in B$ is *integral over* A if it is a root of a monic polynomial with coefficients in a, i.e., if there exist $a_1, \ldots, a_n \in A$ so that

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0.$$

We say that B is *integral over* A if each $x \in B$ is integral over A.

For example, if $K \subset L$ are fields, then $x \in L$ (resp. L itself) is integral over K precisely when it is algebraic over K.

We say that the extension $A \subseteq B$ is *finite* if B is a finite A-module. (We might also say more generally that a morphism $\phi : A \to B$ is finite if $\phi(A) \subseteq B$ is finite.)

The key point is the following:

Theorem 34. *Let $x \in B$. The following are equivalent:*

(i) x is integral over A.

(ii) The subring $A[x] \subseteq B$ generated by x and $\phi(A)$ is a finitely-generated A-module.

(iii) $A[x]$ is contained in a subring C of B which is finitely-generated as an A-module.

(iv) There is a faithful $A[x]$-module M which is finitely-generated over A.

Proof of Theorem 34. (i) implies (ii): If x is integral over A, say $x^n = \cdots$, then the subring $A[x]$ is generated as an A-module by $1, x, \ldots, x^{n-1}$.

(ii) implies (iii): take $C := A[x]$.

(iii) implies (iv): take $M := C$, and note $C \ni 1$.

(iv) implies (i): Write $M = \sum_{i=1}^n Ae_i$, then $xM \subseteq M$ gives equations $xe_i = \sum_{j=1}^n a_{ij} e_j$, which we may rewrite in the form $\Delta e = 0$, where $\Delta_{ij} := \delta_{ij} x - a_{ij} \in A[x]$ and e is the column vector with jth entry $e_j \in A$. By Cramer's rule, we have $\Delta^{\text{ad}} \Delta = \det(\Delta) 1_n$ for some matrix Δ^{ad} with entries in $A[x]$, whose (i,j) entry may be expressed as $(-1)^{i+j} \det(\Delta^{i,j})$, where $\Delta^{i,j}$ denotes the matrix obtained by striking out from Δ the ith row and jth column. Thus $\det(\Delta) e_j = 0$ for all j. Since M is faithful, it follows that $\det(\Delta) = 0$, which gives a monic polynomial equation for x over A. □

Lemma 35. *Let $A \subseteq B \subseteq C$ be rings. Let $x \in C$ be integral over A. Then x is integral over B.*

Proof. Clear: a monic equation satisfied by x with coefficients in A also has coefficients in B. □

Lemma 36. *Let $A \subseteq B \subseteq C$ be rings, with B finite over A and C finite over B. Then C is finite over A.*

Proof. By hypothesis, we have $B = \sum_i Ax_i$ and $C = \sum_j By_j$ for some finite collections $\{x_i\} \subseteq B$, $\{y_j\} \subseteq C$. Then

$$C = \sum_j (\sum_i Ax_i)y_j = \sum_{i,j} Ax_i y_j.$$

□

Lemma 37. *Let $x_1, \ldots, x_n \in B$ be integral over A. Then $A[x_1, \ldots, x_n]$ is a finite over A.*

Proof. We induct on n. The case $n = 1$ follows from the theorem. For $n > 1$, we see that $A[x_1, \ldots, x_n]$ is integral and hence finite over $A[x_1, \ldots, x_{n-1}]$, which is in turn finite over A; we then conclude by the previous lemma. □

Corollary 38. *The following are equivalent for an extension of rings $A \subset B$:*

1. *B is finite over A.*
2. *B is integral and finitely-generated over A.*

Proof. If B is finite over A, then the equivalence "(iii) implies (i)" proved above shows that it is integral over A; on the other hand, it is clearly finitely-generated. The converse is given by the preceeding lemma. □

Corollary 39. *The set of elements $x \in B$ that are integral over A forms an A-subalgebra of B.*

Proof. If $x, y \in B$ are integral over A, then the previous results show that $A[x, y]$ is finite over A, hence integral over A. In particular, $a_1 x + a_2 y$ (for $a_1, a_2 \in A$) and xy are integral over A. □

Definition 40. Let $A \subseteq B$ be rings. The *integral closure $\overline{A}$ of A in B* is the set of all $x \in B$ that are integral over A. By the previous result, $\overline{A}$ is an A-subalgebra of B. We say that A is *integrally closed in B* if $A = \overline{A}$, i.e., if every element of B that is integral over A already belongs to A.

Lemma 41. *Let $A \subset B \subset C$ be rings. If B is integral over A and C is integral over B, then C is integral over A.*

Proof. Let $x \in C$; we must check that x is integral over A. Since C is integral over B, we have

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0$$

for some $b_1, \ldots, b_n \in B$. Since each b_i is integral over A, the ring $B_0 := A[b_1, \ldots, b_n]$ is finite over A. The element x is integral over B_0, and so $B_0[x] = A[b_1, \ldots, b_n, x]$ is finite over B_0. Thus $A[b_1, \ldots, b_n, x]$ is finite over A. By Theorem 34, we conclude that x is integral over A. □

Corollary 42. *Let $\overline{A}$ denote the integral closure of $A \subset B$. Then $\overline{A}$ is integrally closed in B.*

Lemma 43. *Let $A \subset B$ be an integral extension of rings.*

1. *Let $\mathfrak{b} \subset B$ be an ideal, and set $\mathfrak{a} := A/\mathfrak{a}$. Then the extension of rings $A/\mathfrak{a} \subset B/\mathfrak{b}$ is integral.*
2. *Let $S \subset A$ be a multiplicative subset. Then $S^{-1}A \subset S^{-1}B$ is integral.*

Proof. Just do it. □

Definition 44. We say that an integral domain A is *normal* if it is integrally closed in its field of fractions $K := \mathrm{Frac}(A)$.

Lemma 45. *Let A be a UFD. Then A is normal.*

Proof. Suppose $r/s \in K := \mathrm{Frac}(A)$ is integral over A, where $r, s \in A$ are coprime. Then $(r/s)^n + a_1(r/s)^{n-1} + \cdots + a_n = 0$ for some $a_1, \ldots, a_n \in A$. Thus

$$-r^n = a_1 r^{n-1} s + a_2 r^{n-2} s^2 + \cdots + a_n s^n.$$

The RHS and hence the LHS is then divisible by s, so s divides r^n; since r, s are coprime, we must have $s \in A^\times$, and so $r/s \in A$. □

Example 46. In particular, $\mathbb{Z}$ and $k[x]$ (for a field k) are both normal. On the other hand, the ring $A := k[x^2, x^3]$ is not integrally closed in its field of fractions $K := k(x)$ (because $x \in K - A$ is integral over A), hence is not normal.

The integral closure of $\mathbb{Z}$ in $\mathbb{C}$ is the ring of *algebraic integers*. Given a finite field extension $K/\mathbb{Q}$, the integral closure $\mathcal{O}_K$ of $\mathbb{Z}$ in K is called the *ring of integers* of K. These rings are all normal. One can show that if $K = \mathbb{Q}(\sqrt{-3})$, then $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, which properly contains the subring $\mathbb{Z}[\sqrt{-3}]$, which is thus *not* a normal ring.

More generally, if A is a normal domain with field of fractions K, if L/K is a field extension, and if B denotes the integral closure of A in L, then B is normal. This situation arises often both in algebraic number theory (where $K = \mathbb{Q}$, for instance) and in the study of curves in algebraic geometry (where, e.g., $K = k[t]$ for some field k).

The *normalization* A^{norm} of an integral domain A is the integral closure of A inside $\mathrm{Frac}(A)$. The preceeding result shows that A^{norm} is normal.

Lemma 47. *Normality is a local property, i.e., the following are equivalent for an integral domain A:*

1. *A is normal.*
2. *$S^{-1}A$ is normal for each multiplicative subset $S \subset A$.*
3. *$A_{\mathfrak{m}}$ is normal for each maximal ideal $\mathfrak{m}$ of A.*

Proof. (i) implies (ii): Welp, let $x \in K$ be integral over $S^{-1}A$. Write down a monic equation. Clearing denominators, we deduce that sx is integral over A for some $s \in S$. Since A is normal, we have $sx = a$ for some $a \in A$, hence $x = a/s \in S^{-1}A$.

(ii) implies (iii): immediate.

(iii) implies (i): Let $x \in K$ be integral over A. For each $\mathfrak{m}$, we may then find some $b_{\mathfrak{m}} \in \mathfrak{m}$ so that $b_{\mathfrak{m}}x$ is integral over A. The ideal generated by the $b_{\mathfrak{m}}$ is not contained in any maximal ideal, hence equals the unit ideal, so we may write $1 = \sum a_{\mathfrak{m}} b_{\mathfrak{m}}$ as a finite sum with $a_{\mathfrak{m}} \in A$, almost all zero. Then $x = \sum a_{\mathfrak{m}} b_{\mathfrak{m}} x$ is integral over A. □

13 Lying over

Lemma 48. *Let $A \subseteq B$ be an integral extension of integral domains. Then A is a field if and only if B is a field. Equivalently, if $A \subseteq B$ is an integral extension of rings and $\mathfrak{q} \subset B$ is prime, then $\mathfrak{p} := \mathfrak{q} \cap A$ is maximal if and only if $\mathfrak{q}$ is maximal.*

Proof. Suppose A is a field. Let $x \in B$ is nonzero. Write $x^n + a_1 x^{n-1} + \cdots + a_n = 0$, with n minimal. Since B is a domain, we then have $a_n \neq 0$, and so $x^{-1} = -(x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1})/a_n$. Thus B is a field.

Conversely, suppose B is a field Let $x \in A$ be nonzero. Then $1/x \in B$. Write $(1/x)^n + a_1(1/x)^{n-1} + \cdots + a_n = 0$. Then

$$1/x = -(a_1 + a_2 x + \cdots + a_n x^{n-1}) \in A.$$

□

Corollary 49. *Let $(A, \mathfrak{p})$ be a local ring and $A \subset B$ an integral extension. Then*

$$\{\textit{maximal ideals } \mathfrak{m} \subset B\} = \{\textit{primes } \mathfrak{q} \subset B : \mathfrak{q} \cap A = \mathfrak{p}\}.$$

Proof. We apply the lemma, taking into account that $\mathfrak{p}$ is the only maximal ideal of A. □

Theorem 50. *Let $A \subseteq B$ be integral. Then the natural map* $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ *is surjective, and its fibers have no inclusion relations, i.e.:*

1. *We say that a prime $\mathfrak{q}$ of B* lies over *a prime $\mathfrak{p}$ of A if $\mathfrak{q} \cap A = \mathfrak{p}$. Then each prime $\mathfrak{p}$ of A has some prime $\mathfrak{q}$ of B lying over it.*

2. *If $\mathfrak{q}, \mathfrak{q}'$ are primes of B that lie over the same prime of A, then $\mathfrak{q} \subseteq \mathfrak{q}' \implies \mathfrak{q} = \mathfrak{q}'$.*

Proof. The extension $A_\mathfrak{p} \subset B_\mathfrak{p}$ remains integral. The primes of B lying over $\mathfrak{p}$ correspond (in inclusion-preserving manner) to the primes of $B_\mathfrak{p}$ lying over $\mathfrak{m} := \mathfrak{p}A_\mathfrak{p}$ hence (by the previous lemma) to the maximal ideals of $B_\mathfrak{p}$. We have $B_\mathfrak{p} \neq 0$, so maximal ideals exist, and it is clear that no inclusion relations exist between maximal ideals. □

14 Going up

We say that an extension of rings $A \subseteq B$ satisfies *going up* if whenever $\mathfrak{p} \subset \mathfrak{p}' \subset A$ and $\mathfrak{q} \subset B$ are primes with $\mathfrak{q}$ lying over $\mathfrak{p}$, there exists a prime $\mathfrak{q}' \supseteq \mathfrak{q}$ lying over $\mathfrak{p}'$.

Equivalently, given $m < n$ and chain of primes $\mathfrak{p}_0 \supset \cdots \subset \mathfrak{p}_n \subset A$ and $\mathfrak{q}_0 \supset \cdots \subset \mathfrak{q}_m \subset A$ with $\mathfrak{q}_i$ lying over $\mathfrak{p}_i$ for $i \leq m$, we can extend the latter chain to $\mathfrak{q}_0 \supset \cdots \subset \mathfrak{q}_n \subset A$ with $\mathfrak{q}_i$ lying over $\mathfrak{p}_i$ for $i \leq n$.

Theorem 51. *Any integral extension $A \subset B$ satisfies "going up".*

Proof. Apply "lying over" to the prime $\mathfrak{p}'/\mathfrak{p}$ of $A/\mathfrak{p}$ inside $B/\mathfrak{q}$. □

As an application:

Proposition 52. *Let $A \subseteq B$ be an integral ring extension. Let $\mathfrak{b} \subset B$ be an ideal, and $\mathfrak{a} := \mathfrak{b} \cap A$. Then*

(i) $\dim(A) = \dim(B)$.

(ii) $\dim(A/\mathfrak{a}) = \dim(B/\mathfrak{b})$.

(iii) $\text{height}(\mathfrak{b}) \leq \text{height}(\mathfrak{a})$.

Proof. (i): A chain of primes in B lies over a chain of primes in A. The constituents of the latter are distinct by the "non-inclusions" theorem. Thus $\dim(A) \geq \dim(B)$.

Conversely, a chain of primes in A lifts to a chain in B, by the "going up" theorem. Thus $\dim(A) \leq \dim(B)$.

(ii) is a consequence of (i).

(iii): Let $\mathfrak{p}$ be a minimal prime of $\mathfrak{a}$. By applying "lying over" to $A/\mathfrak{a} \subseteq B/\mathfrak{b}$, there is a minimal $\mathfrak{q}$ of $\mathfrak{b}$ lying over $\mathfrak{p}$. A chain of primes ending at $\mathfrak{q}$ lies over a chain of primes ending at $\mathfrak{p}$. Thus $\text{height}(\mathfrak{b}) \leq \text{height}(\mathfrak{q}) \leq \text{height}(\mathfrak{p})$; since $\mathfrak{p}$ was arbitrary, we conclude upon taking infima that $\text{height}(\mathfrak{b}) \leq \text{height}(\mathfrak{a})$. □

15 Galois action on primes

Lemma 53. *Let A be a normal integral domain. Let $K := \text{Frac}(A)$, and let L/K be a normal extension. Let B denote the integral closure in L of A. Then*

1. *each $\sigma \in G := \mathrm{Aut}(L/K)$ induces a ring automorphism of B that fixes A;*

2. *G acts on the set of primes of B lying above a given prime $\mathfrak{p}$ of A, i.e.: if $\mathfrak{q} \subset B$ is prime, then so is $\sigma(\mathfrak{q}) \subset B$, and one has $\mathfrak{q} \cap A = \sigma(\mathfrak{q}) \cap A$.*

3. *This action is transitive: given primes $\mathfrak{q}, \mathfrak{q}'$ of B lying over the same prime $\mathfrak{p}$ of A, one can find $\sigma \in G$ for which $\sigma(\mathfrak{q}) = \mathfrak{q}'$.*

We treat first the case of a finite extension. We reduce in that case, using prime avoidance and the absence of inclusions among fibers of $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$, to showing that

$$\mathfrak{q}' \subset \cup_{\sigma \in G} \sigma(\mathfrak{q}).$$

Recall that for L/K normal, one has L/L^G Galois with $\mathrm{Gal}(L/L^G) = G$ and L^G/K purely inseparable: for each $x \in L^G$ the exists $n \geq 1$ (a prime power) with $x^n \in K$. Let $x \in \mathfrak{q}'$. Since L/K is finite, we may set $y := \prod_{\sigma \in G} \sigma(x)$. Then $y \in L^G \cap B$, so some $y^n \in K \cap B$. Since A is normal and B is integral over A, we have $K \cap B = A$, thus $y^n \in \mathfrak{q}' \cap A = \mathfrak{p} \subseteq \mathfrak{q}$. Thus there exists σ with $\sigma(x) \in \mathfrak{q}$, so $\sigma^{-1}(y) \in \mathfrak{q}'$.

In general, let

Then it takes a bit of Zorn's lemma to finish it all off. TODO: write that down.

Give the example of a Galois extension of number fields.

16 Going down

For "going down" theorem, you use a bit of Galois theory. Hard to beat Eisenbud or Matsumura's treatment; Bosch is also fine.

It says that if $A \subseteq B$ is an integral extension of integral domains, with A normal, then the "going down" property holds: for a prime $\mathfrak{q} \subset B$ lying over $\mathfrak{p} \subset A$ and another prime $\mathfrak{p}' \subset \mathfrak{p}$, we can find a prime $\mathfrak{q}' \subset \mathfrak{q}$ lying over $\mathfrak{p}'$.

This is somehow equivalent to: Let $\mathfrak{p} \subset A$ be prime. Then any minimal prime of $\mathfrak{p}B$ lies over $\mathfrak{p}$.

- Suppose $\mathfrak{p}$ satisfies what we called "going down" above. Let $\mathfrak{q}'$ be a minimal prime of $\mathfrak{p}B$. Set $\mathfrak{p}' := \mathfrak{q} \cap A$. Then $\mathfrak{p} \subset \mathfrak{p}'$, so by going down, we can find a prime $\mathfrak{q} \subset \mathfrak{q}'$ lying over $\mathfrak{p}$. But then $\mathfrak{q} \supset \mathfrak{p}B$, so $\mathfrak{q} = \mathfrak{q}'$ by minimality. But this contradicts the fact that there are no inclusion relations in the fibers of $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ for integral extensions $A \subset B$.

- Suppose any minimal prime of $\mathfrak{p}B$ lies over $\mathfrak{p}$, for all primes $\mathfrak{p}$ of A, and let the inclusion $\mathfrak{p} \subset \mathfrak{p}'$ of primes be given, together with a prime $\mathfrak{q}'$ over $\mathfrak{p}'$. Then $\mathfrak{q}' \supset \mathfrak{p}B$. I think we can just use Zorn's lemma to produce a minimal prime $\mathfrak{q}' \supset \mathfrak{q} \supset \mathfrak{p}B$.

It'd be nice to give an example showing how this can fail.

The proof is fairly easy, using the Galois trick.

17 Applications of theorems on integral ring extensions to dimension

If $A \subseteq B$ is integral, $\mathfrak{b} \subseteq B$ is an ideal, and $A := \mathfrak{b} \cap A$, then

1. $\dim(A) = \dim(B)$,
2. $\text{height}(\mathfrak{b}) \leq \text{height}(\mathfrak{a})$, with equality if A, B are integral domains with A normal (or more generally, if "going down" holds), and
3. $\text{coheight}(\mathfrak{a}) = \text{coheight}(\mathfrak{b})$.

18 Noether normalization?

Let k be a field. The following result is very useful:

Theorem 54 (Noether normalization)**.** *Let A be a finitely-generated k-algebra. There exist $x_1, \ldots, x_n \in A$ with the following properties.*

1. *$x_1, \ldots, x_n$ are algebraically independent, i.e., the map*

$$k[X_1, \ldots, X_n] \to A$$

$$X_j \mapsto x_j$$

   is injective.

2. *A is integral, hence finite, over the subring $k[x_1, \ldots, x_n]$.*

Since integral extensions preserve dimension, the conclusion implies in particular that $\dim(A) = n$, and also that if A is a domain, then $\dim(A) = n = \text{trdeg}_k(\text{Frac}(A))$ (noting that $\text{Frac}(A)$ is an algebraic extension of $k(x_1, \ldots, x_n)$).

The key lemma for the proof is the following.

Lemma 55. *Let A be a k-algebra and $x_1, \ldots, x_n \in A$. Let f be a nonzero element of the polynomial ring $k[X_1, \ldots, X_n]$. Set $w := f(x_1, \ldots, x_n) \in A$. Then there exist $z_1, \ldots, z_{n-1} \in k[x_1, \ldots, x_n]$ such that $k[x_1, \ldots, x_n]$ is integral over $k[w, z_1, \ldots, z_{n-1}]$.*

To deduce Noether normalization from this, suppose that the finitely-generated \$k\$-algebra A is generated by elements $x_1, \ldots, x_n$. If these elements are algebraically independent, then we are done. Otherwise we may find a nonzero element f of the polynomial ring $k[X_1, \ldots, X_n]$ for which $0 = f(x_1, \ldots, x_n)$. The key lemma (applied with $w = 0$) produces elements $z_1, \ldots, z_{n-1} \in A$ for which $k[x_1, \ldots, x_n]$ is integral over $k[z_1, \ldots, z_{n-1}]$. By iterating this procedure finitely many times, we conclude.

We note that "finite" and "integral" are the same in these contexts, because everything is finitely-generated.

For the proof of the key lemma, we warm up by considering rings of the form $A := k[X, Y]/(f)$ for some nonzero $f \in k[X, Y]$. We denote by $x, y \in A$

the images of X, Y. Thus A has two generators x, y satisfying the relation $f(x, y) = 0$. We aim to produce an element $z \in A$ so that A is integral over $k[z]$. This is a special case of the key lemma that illustrates the basic idea.

Let's start with the example $f = XY - 1$. Then we may think $A \cong k[x, 1/x] \subseteq k(x) = \mathrm{Frac}(A)$. Observe in this case that A is *not* integral over $k[x]$ or $k[y]$. For instance, $k[x]$ is a UFD, hence normal (i.e., integrally closed in $k(x)$), hence $1/x \in A \notin k[x]$ is not integral over $k[x]$.

On the other hand, A is integral over $k[z]$ if $z = y - ax$ with $a \neq 0$: We have $A = k[x, z]$, so it suffices to show that x is integral over $k[z]$. We have $zx = xy - ax^2 = 1 - ax^2$, so $ax^2 + zx - 1 = 0$; we may divide by a to get the required monic equation for x over $k[z]$.

This suggests a fairly general strategy. Write $f = f_n + \cdots + f_0$, where f_j denotes the homogeneous component of degree j (thus f_j is a linear combination of terms $x^i y^{j-i}$). We may assume that $f_n \neq 0$.

Lemma 56. *Suppose Y does not divide f_n. Then A is integral over $k[y]$.*

Proof. Our hypothesis implies that $f = aX^n + \cdots$, where $a \neq 0$ and $\cdots$ consists of lower order terms in X, with coefficients in $k[Y]$. This relation taken in the quotient ring A shows that x is integral over y. □

Corollary 57. *Let $a \in k$. Suppose $Y - aX$ does not divide f_n. Then A is integral over $k[y - ax]$.*

Proof. Apply the lemma with modified coordinates $X' := X, Y' := Y - aX$. □

Corollary 58. *Suppose the field k is infinite. Then there exists $a \in k$ so that A is integral over $k[y - ax]$.*

Proof. Over an algebraic closure $\overline{k}$, we may factor $f_n = \prod_{i=1..n}(a_i x - b_i y)$ for some $a_i, b_i \in \overline{k}$ with $(a_i, b_i) \neq (0, 0)$. We then choose $a \in k$ not equal to any of the ratios b_i/a_i and apply the previous corollary. □

This completes the proof of Noether normalization for $A = k[X, Y]/(f)$ in the special case that k is infinite. What if k is finite? Consider for instance the case that $k = \mathbb{F}_2$ and $f = Y(Y + X) - 1$, so that $y(y + x) = 1$. Thus $A = k[y, y - y^{-1}] \subseteq k(y)$. The above proof obviously doesn't work, and in fact A is not integral over $k[y]$ or $k[y - 1]$. So we need another trick to address this special case. We might try, instead of $y - ax$, something like $z := y - x^2$. Then $y = x^2 + z$. We expand out:

$$0 = f(x, y) = f(x, x^2 + z) = (x^2 + z)(x^2 + z + x) - 1 = x^4 + \cdots,$$

where $\cdots$ denotes terms of lower order in x with coefficients in $k[z]$. Thus x is integral over $k[z]$; since $A = k[x, z]$, we conclude that A is integral over $k[z]$. There's nothing special about the number 2: we could have just as well taken $z := y - x^s$ for any $s \geq 2$ and then expanded out $0 = f(x, x^s + z)$. The same trick obviously works for any polynomial f: if s is large enough, the same argument will give a monic relation satisfied by x over $k[z]$.

Lemma 59. *Let $s \in \mathbb{Z}_{\geq 1}$ be sufficiently large in terms of $0 \neq f \in k[X,Y]$, and take $A = k[X,Y]/(f) \ni x, y$ as above. Then A is integral over $k[z]$ with $z := y - x^s$.*

Proof. (Not clear whether there's any point in writing this all out; might already be clear enough.) We expand out $0 = f(x,y) = f(x, x^s + z)$ as above. Say $f(X,Y) = \sum_{\alpha \in I} c_\alpha X^{\alpha_1} Y^{\alpha_2}$, where $I \subseteq \mathbb{Z}^2_{\geq 0}$ is finite and $c_\alpha \in k^\times$. We have

$$x^{\alpha_1} y^{\alpha_2} = x^{\alpha_1}(x^s + z)^{\alpha_2} = x^{\alpha_1 + s\alpha_2} + \cdots,$$

where $\cdots$ denotes terms of lower order in X with coefficients in $k[z]$. We may choose s so that for all $\alpha, \beta \in I$, we have

$$\alpha \neq \beta \implies \alpha_1 + s\alpha_2 \neq \beta_1 + s\beta_2.$$

(Just take s larger than the maximum of α_j over all $\alpha \in I$ and $j = 1, 2$.) Take $\alpha \in I$ with $\alpha_1 + s\alpha_2$ maximal. Then

$$0 = f(x, x^s + z) = c_\alpha x^{\alpha_1 + s\alpha_2} + \cdots,$$

with $\cdots$ as above. Thus x is integral over $k[z]$. □

More generally, let's suppose now that we have a ring A of dimension d with n generators $x_1, \ldots, x_n$. As indicated above, we may assume that $n > d$ and that there is some nontrivial polynomial relation f satisfied by the x_i, i.e., $0 \notin f \in k[X_1, \ldots, X_n]$ with $f(x_1, \ldots, x_n) = 0$. We choose integers s_j and introduce the variables $z_j := x_j - x_n^{s_j}$ for $1 \leq j < n$. Then

$$0 = f(x_1, \ldots, x_n) = f(x_n^{s_1} + z_1, \ldots x_n^{s_{n-1}} + z_{n-1}, x_n).$$

By choosing the s_j suitably as in the case $n = 2$ (e.g., $s_j := s^j$ for s large enough), we may arrange that this proves that x_n is integral over $A_0 := k[z_1, \ldots, z_{n-1}]$. But then clearly A is integral over A_0. We can now apply our induction hypothesis to A_0 to conclude.

Actually, you like Bosch's treatment much better. He shows that if $A = k[x_1, \ldots, x_n]$ is a finitely-generated \$k\$-algebra and $f = \sum c_\alpha x^\alpha$ with some $c_\alpha \neq 0$, then there exist $z_1, \ldots, z_{n-1}$ so that $k[x_1, \ldots, x_n]$ is finite over $k[f, z_1, \ldots, z_{n-1}]$. We can then deduce Noether normalization by recursively applying this step with $f = 0$ until we arrive at the case that the x_i are algebraically independent. That's much less clunky than what you had done.

How about the refined version?

After this, you can re-prove Nullstellensatz. You can then give applications to heights of primes in \$k\$-domains.

Here we follow Matsumura's treatment (p89) of Nagata's approach.

Theorem 60. *Let k be a field, let A be a finitely-generated k-algebra with $\dim(A) = n$, and let $\mathfrak{a} \subseteq A$ be an ideal with $\dim(A/\mathfrak{a}) = n - r$. There exist $y_1, \ldots, y_n \in k[x]$ so that*

1. *A is finite over the subring $k[y] := k[y_1, \ldots, y_n]$, and*

2. *$\mathfrak{a} \cap k[y] = (y_1, \ldots, y_r)$.*

Proof. We induct on r.
If $r = 0$, then $A/\mathfrak{a}$ □

<++>
For Noether normalization, I think 13.1 in Eisenbud looks like a pretty good treatment. It also leads readily to the dimension formulas you're after. 11.2.4 in Vakil is also a nice exposition of Nagata's proof. Maybe try to combine that w/ what Eisenbud does, and also read Matsumura?

Theorem 61 (Noether normalization)**.** *Let A be an integral domain that is finitely-generated over a subfield k. Set $d = \dim(A)$. Then there is a finite injective map $k[X_1, \ldots, X_d] \hookrightarrow A$. (Okay, need to know that finite implies integral for the application below.)*

Proof. We write $A = k[Y_1, \ldots, Y_n]/\mathfrak{p}$, and induct on n. Then $d \leq n$. If $d = n$, then $\mathfrak{p} = (0)$, so we're done. We assume now that $n > d$ and induct on n. We try to find elements $Z_1, \ldots, Z_{n-1} \in k[Y_1, \ldots, Y_n]$ so that A is finite over $k[Z_1, \ldots, Z_{n-1}]/\mathfrak{q}$, where $\mathfrak{q} := k[Z_1, \ldots, Z_{n-1}] \cap \mathfrak{p}$. Then $\dim k[Z]/\mathfrak{q} = d$, so by our inductive hypothesis, $k[Z]/\mathfrak{q}$ is finite over some $k[X_1, \ldots, X_d]$.

To find the required elements, we choose $0 \neq f \in \mathfrak{p}$. We then choose a large natural number e and introduce the variables $Z_j := Y_j - Y_n^{e^j}$ for $j = 1..n-1$, so that $Y_j = Z_j + Y_n^{e^j}$ and thus if $f = \sum c_\alpha Y^\alpha$, then

$$f = \sum c_\alpha Y^\alpha = \sum c_\alpha (Z_1 + Y_n^e)^{\alpha_1} \cdots (Z_{n-1} + Y_n^{e^{n-1}})^{\alpha_{n-1}} Y_n^{\alpha_n}.$$

Define the weight of α to be $\sum_{j=1..n} e^j \alpha_j$. We choose $e > \sup\{\alpha_j : c_\alpha \neq 0, j \in \{1..n\}\}$. Then each monomial occurring in the expansion of f has a different weight. Let β be the multi-index of highest weight for which $c_\beta \neq 0$, and set $\ell := \sum_{j=1..n} e^j \beta_j$. Then we may write

$$f = Y_n^\ell + a_1(Z_1, \ldots, Z_{n-1}) Y_n^{\ell-1} + \cdots + a_\ell(Z_1, \ldots, Z_{n-1})$$

for some $a_j \in k[Z_1, \ldots, Z_{n-1}]$. This shows that Y_n is integral over $k[f, Z_1, \ldots, Z_{n-1}]$. Reducing this equation modulo $\mathfrak{p}$, we deduce that the image $y_n \in A$ of Y_n is integral over $k[z_1, \ldots, z_{n-1}]$.

Maybe it's cleaner to start by saying that you'll induct on the number of generators of A. If A admits d generators, then it's a polynomial ring, so you're done. Then you can avoid some futzing. □

19 Dimension vs. transcendence degree

Theorem 62. *Let k be a field, and let A be an integral domain that is a finitely-generated k-algebra. Then* $\dim(A) = \mathrm{trdeg}_k(\mathrm{Frac}(A))$.

Proof. Consider first the case that $A = k[X_1, \ldots, X_n]$ is a polynomial ring in n indeterminates. We've seen then that $\dim(A) = n$, while it's clear that $\mathrm{trdeg}_k(\mathrm{Frac}(A)) = n$, so the required identity holds.

We now reduce the general case to this one. By Noether normalization, there is a finite map $k[X_1, \ldots, X_d] \hookrightarrow A$ for some d. Now Now we should have seen by now that integral ring morphisms preserve dimensions/heights/coheights (this is an application of lying over and going up/down theorems). Thus $\dim(A) = d$. Moreover, the field extension $\mathrm{Frac}(A)/\mathrm{Frac}(k[X_1, \ldots, X_d])$ is algebraic, so the two fields have the same transcendence degree. □

Theorem 63. *Let A be as above. Then* $\mathrm{height}(\mathfrak{p}) + \dim(A/\mathfrak{p}) = \dim(A)$ *for every prime $\mathfrak{p}$. In particular,* $\mathrm{height}(\mathfrak{m}) = \dim(A)$ *for every maximal ideal $\mathfrak{m}$.*

Proof. DFD □

20 Valuation rings

Let K be a field, and let $(G, +, 0, \leq)$ be a totally ordered abelian group written additively (e.g., $G = \mathbb{Z}$); thus for $x, y, z \in G$ with $x \leq y$, we have $x + z \leq y + z$.

A *valuation* of K with values in G is a map $v : K^\times \to G$ such that for all $x, y \in K^\times$, we have

1. $v(xy) = v(x) + v(y)$, and
2. $v(x + y) \geq \min(v(x), v(y))$ (called the *ultrametric inequality*).

In that case, the set $A := \{x \in K^\times : v(x) \geq 0\} \cup \{0\}$ is a subring of K, called the *valuation ring* of v. We note that by replacing G with its image, we may assume that v is surjective; this will often be convenient.

Lemma 64. *The subset $\mathfrak{m} := \{x \in K^\times : v(x) > 0\} \cup \{0\}$ is an ideal, and $(A, \mathfrak{m})$ is a local ring with unit group $A^\times = \{x \in K^\times : v(x) = 0\}$.*

Proof.

- $\mathfrak{m}$ is an abelian group: if $v(x) > 0$ and $v(y) > 0$, then $v(x + y) \geq \min(v(x), v(y)) > 0$.
- $\mathfrak{m}$ is closed under multiplication by A: if $v(x) \geq 0$ and $v(y) > 0$, then $v(xy) = v(x) + v(y) > 0$.
- If $x \in A - \mathfrak{m}$, then $v(x) = 0$, hence $v(1/x) = -v(x) = 0$, hence $1/x \in A$, and so $x \in A^\times$. Conversely, if $x \in A^\times$, then $v(x), v(1/x) \geq 0$, so $v(x) = 0$ and $x \in A - \mathfrak{m}$. Thus $(A, \mathfrak{m})$ is local and $A^\times$ is as described.

□

It is customary extend such a valuation to a map $v : K \to G \cup \{\infty\}$, where $n \leq \infty$ for all $n \in G$, by setting $v(0) := 0$, so that these identities read more concisely as

$$A = \{x \in K : v(x) \geq 0\}, \quad \mathfrak{m} = \{x \in K : v(x) > 0\}, \quad A^\times = \{x \in K : v(x) = 0\}.$$

Definition 65. Let A be an integral domain with field of fractions $K := \mathrm{Frac}(A)$. We say that A is a *valuation ring* (or VR for short) if it is the valuation ring of some valuation v of K.

A valuation v is *discrete* if its value group G is isomorphic to $\mathbb{Z}$ and if v is nontrivial; the corresponding valuation ring is then called a *discrete valuation ring* (or DVR for short). Identifying G with $\mathbb{Z}$, the image of v is then a nontrivial subgroup of $\mathbb{Z}$, hence of the form $n\mathbb{Z}$; replacing v with v/n, we may thus assume without loss of generality that $v : K^\times \to \mathbb{Z}$ is surjective. If $\mathfrak{a}$ is a nonzero ideal in A, then there exists a smallest integer $n \geq 0$ for which $v(x) = n$ for some $x \in \mathfrak{a}$; then $\mathfrak{a}$ contains and hence equals $\{x \in K : v(x) \geq n\}$, so all ideals are of the latter form. It follows easily that A is regular Noetherian local PID in which every ideal is a power of the maximal ideal.

Example 66. The ring $k[[X]]$ of formal power series in a variable X is a DVR: take $v(\sum_i c_i X^i) := \inf\{i : c_i \neq 0\} \in \mathbb{Z} \cup \{\infty\}$. For example, $v(X + X^2) = 1$, $v(X^{-3} + X^{10}) = -3$, $v(1) = 0$, $v(0) = \infty$.

The ring $\cup_{n \geq 1} k[[X^{1/n}]]$ of formal power series with rational exponents is a valuation ring with value group $\mathbb{Q}$. (We will see below that it is *not* a DVR.)

If $K = \mathbb{Q}$ and p is a prime number, then we may write any $x \in \mathbb{Q}^\times$ as $p^n u/v$ with u, v coprime to p. We then set $v(x) := n$. This defines a discrete valuation on $\mathbb{Q}$ with valuation ring $\mathbb{Z}_{(p)}$.

Lemma 67. *Let A be an integral domain, $K := \mathrm{Frac}(A)$. The following are equivalent:*

1. *A is a valuation ring.*
2. *For each $x \in K^\times$, one has $x \in A$ or $x^{-1} \in A$ (or both).*

Proof. (i) implies (ii): Suppose $v : K \to G \cup \{\infty\}$ is a valuation with valuation ring A, so that $A = \{x \in K : v(x) \geq 0\}$, and let $x \in K^\times$, so that $v(x) \in G$. If $v(x) \geq 0$, then $x \in A$. If $v(x) \leq 0$, then $v(x^{-1}) \geq 0$, and so $x^{-1} \in A$.

(ii) implies (i): Let $G := K^\times / A^\times$; it is an abelian group. Let $v : K^\times \to G$ denote the natural quotient map. We denote the group law on G by $+$, and write $0 := v(1)$ for its identity element. Clearly $v(xy) = v(x) + v(y)$.

We equip G with a partial order $\leq$ given by A-divisibility: $xA^\times \leq yA^\times$ iff $y \in Ax$. We check that this defines a total order: if $x, y \in K^\times$, then either $x/y \in A$ (in which case $yK^\times \leq xK^\times$) or $y/x \in A$ (in which case $xK^\times \leq yK^\times$).

We check the ultrametric inequality, that $v(x + y) \geq \min(v(x), v(y))$. Suppose for instance that $v(x) \leq v(y)$, so that $y \in Ax$. Then $x + y \in Ax$, so $v(x) \leq v(x + y)$, as required.

Thus v is a valuation. We have $v(x) \geq 0$ iff $x \in A \cdot 1$, so A is the valuation ring of v. □

Example 68. $A := k[x^2, x^3] \subseteq K = k(x)$ is not a valuation ring: the element $x \in K^\times$ satisfies $x \notin A, x^{-1} \notin A$.

The ultrametric inequality can be strengthened to an equality if $v(x) \neq v(y)$:

Lemma 69. *If $v(x) \neq v(y)$, then $v(x+y) = \min(v(x), v(y))$. More generally, if $v(x_1) < v(x_2) \leq v(x_3) \leq \cdots \leq v(x_n)$, then $v(x_1 + \cdots + x_n) = v(x_1)$.*

Proof. Suppose for instance that $v(x) < v(y)$. Then $y/x \in \mathfrak{m}$, hence $1 + y/x \in A^\times$, hence $v(1+y/x) = 0$, hence $v(x+y) = v(x)v(1+y/x) = v(x)$. The second assertion follows by induction. □

Lemma 70. *Valuation rings are normal.*

Proof. Let $v : K^\times \to G$ be a valuation with valuation ring A. Let $x \in K$ be integral over A, thus

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

for some $a_i \in A$. Suppose that $v(x) < 0$. Then for $i = 1..n$, we have $v(a_i) \geq 0$, hence $v(x^n) < v(x^i) \leq v(a_i x^i)$. By the strengthened ultrametric inequality, it follows that

$$\infty = v(0) = v(x^n + \cdots + a_n) = v(x^n) < 0,$$

a contradiction. □

Theorem 71. *Let A be an integral domain with field of fractions K and integral closure $\overline{A} \subseteq K$. Then $\overline{A}$ is the intersection of all valuation rings B of K containing A.*

Proof. If $x \in K$ is integral over A, then it is also integral over each valuation ring B of K containing A; by the previous lemma, it follows that x belongs to B. This gives the "easy" inclusion. Conversely, we must verify that if $x \in K$ is *not* integral over A (so that in particular, $x \neq 0$), then there *exists* a valuation ring B of K containing A for which $x \notin B$:

Observe first that x is not integral over $A[1/x]$: if it were, then we could clear denominators to get a monic equation for x over A, contrary to hypothesis. In particular, $x \notin A[1/x]$. Thus $1/x$ does not belong to the unit group of $A[1/x]$, and there is a prime (or even maximal) ideal $\mathfrak{p}$ of $A[1/x]$ for which $1/x \in \mathfrak{p}$.

Observe that if $(B_i)_{i \in I}$ are subrings of K containing $A[1/x]$ for which

1. $i \leq j \implies B_i \subseteq B_j$, and
2. $\mathfrak{p}B_i \neq B_i$,

then the (increasing) union $B := \cup_{i \in I} B_i$ also has the property that $\mathfrak{p}B \neq B$, for else we may write $1 = p_1 b_1 + \cdots + p_n b_n$ with $p_1, \ldots, p_n \in \mathfrak{p}$ and $b_1, \ldots, b_n \in B_i$ for some i, contrary to hypothesis.

By Zorn's lemma, there is thus a subring B of K containing $A[1/x]$ and maximal with respect to the property that $\mathfrak{p}B \neq B$. *We claim that B is a valuation ring.* Assume the claim for the moment. Let v be a defining valuation

for B, and let $\mathfrak{m} = \{x \in B : v(x) > 0\} \subseteq B$ denote the maximal ideal of B. Then $1/x \in \mathfrak{p} \subseteq \mathfrak{p}B \subseteq \mathfrak{m}$, so $v(x) = -v(1/x) < 0$, so $x \notin B$. We have thus produced the required valuation ring of K, containing A, which does not contain x. It remains only to establish the claim.

To that end, we verify first that B *is local*. Choose any maximal ideal $\mathfrak{m}$ of B containing $\mathfrak{p}B \neq B$. Then $B_{\mathfrak{m}} \neq 0$, so $\mathfrak{m}B_{\mathfrak{m}} \neq B_{\mathfrak{m}}$. In particular, $\mathfrak{p}B_{\mathfrak{m}} \neq B_{\mathfrak{m}}$. By the maximality of B, it follows that $B = B_{\mathfrak{m}}$. Thus $(B, \mathfrak{m})$ is local.

We verify next that B *is normal*. Suppose otherwise $y \in K$ is integral over B, but that $y \notin B$. Then $B \subsetneq B[y]$ is an integral extension, so $B[y]$ contains a prime $\mathfrak{n}$ lying over $\mathfrak{m}$. (Here we use lying over!) In particular, $\mathfrak{p}B[y] \subseteq \mathfrak{n} \subsetneq B[y]$. But this contradicts the maximality of B.

We verify next that $B \subseteq A_{\mathfrak{p}}$. We must verify that if $y \in A - \mathfrak{p}$, then $y \in B^{\times}$, i.e., that $y \notin \mathfrak{m}$. In the contrapositive, we must verify that $\mathfrak{m} \cap A \subseteq \mathfrak{p}$. TODO. You forget how to finish this off; the important thing is just that you need, at the very least, the lying over property, and so this lecture will have to come a bit later.

Okay, but even then, why is B a valuation ring? If $y \in K - B$ then you need to show that $B[y] = B$, for instance, by verifying that $\mathfrak{p}B[y] \neq B[y]$. Why should that be? □

The key step is that if $\mathfrak{p}$ is a prime in A and B is a subring of K that is maximal with respect to the property $\mathfrak{p}B \neq B$, then B is local, normal, contains $A_{\mathfrak{p}}$, and satisfies $\mathfrak{m}_B \cap A = \mathfrak{p}$.

1. Local: let $\mathfrak{m} \supseteq \mathfrak{p}B$. Then $\mathfrak{p}B_{\mathfrak{m}} \neq B_{\mathfrak{m}}$.
2. Normal: if $x \in K$ is integral over B, then $B[x]$ contains a prime lying over the maximal ideal of B.
3. $B \supseteq A_{\mathfrak{p}}$: invert
4. $\mathfrak{m}_B \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$, etc.

I guess the point here is to give some insight regarding normal rings, and also to introduce DVR's and to prove that awesome theorem characterizing them.

TODO: determine what facts from above are really needed for this discussion. Do you need the "lying over" and "going down" theorems, for instance? If not, it might be worth introducing this stuff a bit earlier, so as to give more examples to play with.

21 Dedekind domains

Let $(A, \mathfrak{p})$ be a one-dimensional Noetherian local domain. Let K denote the fraction field of A.

Lemma 72. *For each $x \in K$ there exists $n \geq 0$ so that $x\mathfrak{p}^n \subseteq A$.*

Proof. It suffices to show for each $0 \neq y \in A$ that one has $\mathfrak{p}^n \subseteq (y)$ for some n. This follows from the fact that $A/(y)$ is an Artin local ring with maximal ideal $\mathfrak{p}/(y)$, which is thus its nilradical. □

Lemma 73. *Suppose $y \in K$ satisfies $\mathfrak{p}y \subseteq A$. Then either*

1. *$1/y \in \mathfrak{p}$, or*
2. *y is integral over A.*

Proof. If $\mathfrak{p}y = A$, then we can write $ty = 1$ for some $t \in \mathfrak{p}$. Otherwise $\mathfrak{p}y \subseteq \mathfrak{p}$; since $\mathfrak{p}$ is a finitely-generated A-module, it follows that y is integral over A. □

In other words, every element of $\mathfrak{p}^{-1}$ is either (..)

Theorem 74. *If A is normal, then A is a DVR.*

Proof. Let $(B, \mathfrak{m})$ be a valuation ring in K that contains A and for which $\mathfrak{m}$ lies over $\mathfrak{p}$. Let v be a defining valuation for B. Then $v(A) \geq 0$ and $v(\mathfrak{p}) > 0$. We aim to show that $A = B$. (Then we're done, since a Noetherian VR is a DVR.)

Let $x \in B$. Thus $x \in K$ and $v(x) \geq 0$. We have seen that $\mathfrak{p}^n x \subseteq A$ for some n. (This used the one-dimensionality of A.) Choose n minimal with this property. If $n = 0$, then we're done: $Ax \subseteq A$, so $x \in A$. Suppose otherwise that $n \geq 1$, so that $\mathfrak{p}^{n-1}x \not\subseteq A$. Choose $y \in \mathfrak{p}^{n-1}x$ with $y \notin A$. Then $v(y) \geq v(x) \geq 0$ and $\mathfrak{p}y \subseteq \mathfrak{p}^n x \subseteq A$. We have $v(1/y) \leq 0$, so $1/y \notin \mathfrak{p}$. By the lemma, we deduce that y is integral over A, whence by the normality of A that $y \in A$, contradiction. □

22 The future

22.1 Some exercises

22.1.1

Let A be a ring, not necessarily Noetherian. We are asked to show that

$$\dim A + 1 \leq \dim A[X] \leq 2 \dim A + 1.$$

We may establish the first inequality as in the Noetherian case. For the second, it suffices to verify that for any prime chain $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subseteq A[X]$ with $\mathfrak{p}_1 \cap A = \mathfrak{p}_2 \cap A =: \mathfrak{p}$, one has $\mathfrak{p}_1 = \mathfrak{p}A[X]$, I think we just reduce to case in which $(A, \mathfrak{p})$ is local, and then use that $\dim(A/\mathfrak{p})[X] = 1$.

22.1.2

Let $A = k[X, Y]$ for a field k. Let $f \in A$ be non-constant. We want to show that $\dim A/(f) = 1$. Well, A is Noetherian, and $\dim(A) = 2$, and f is non-constant, hence a non-unit. It suffices to show for each maximal ideal $\mathfrak{m}$ containing (f) that $\dim A_{\mathfrak{m}}/(f) = 1$. For this we can reduce to the local case? We need to know that f is not a zero-divisor. Everything in sight is an integral domain, so there's no issue there.

22.1.3

Let $(A, \mathfrak{m})$ be a regular Noetherian local ring with residue field $k = A/\mathfrak{m}$.

Suppose first that $\dim(A) = 0$. We are asked then to verify that A is a field. We are given that $\dim(A) = 0 = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$. Thus $\mathfrak{m} = \mathfrak{m}^2$. By Nakayama, it follows that $\mathfrak{m} = (0)$. Thus A is a field.

Suppose next that $\dim(A) = 1$. We are asked to verify that A is a local principal ideal domain. Welp, let $f \in \mathfrak{m} - \mathfrak{m}^2$, so that the image of f spans $\mathfrak{m}/\mathfrak{m}^2$. By Nakayama, f generates $\mathfrak{m}$. So $\mathfrak{m} = (f)$ is a principal ideal. Now consider any ideal $\mathfrak{a} \subseteq A$. We must verify that $\mathfrak{a}$ is principal. We may suppose that $\mathfrak{a}$ is nonzero. We have $\mathfrak{m} \supseteq \mathfrak{a}$. Since $\mathfrak{a}$ is nonzero and $\cap \mathfrak{m}^n = 0$, there exists $n \geq 1$ so that $\mathfrak{m}^n \supseteq \mathfrak{a}$ but $\mathfrak{m}^{n+1} \not\supseteq \mathfrak{a}$. Thus $\mathfrak{a}$ is contained in (f^n), but $\mathfrak{a}$ is not contained in (f^{n+1}). Choose $x \in \mathfrak{a}$ with $x \notin (f^{n+1})$. We may write $x = f^n y$. If $y \in \mathfrak{m}$, then $x \in (f^{n+1})$, contradiction. Thus y is a unit. Thus $(x) = (f^n)$. Thus $\mathfrak{a}$ contains $\mathfrak{m}^n$. Thus $\mathfrak{a} = \mathfrak{m}^n$, as required.

22.1.4

Let $(A, \mathfrak{m})$ be a regular Noetherian local ring of dimension d with residue field $k := A/\mathfrak{m}$. This means, we recall, that $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = \dim(A)$, or equivalently, that $\mathfrak{m}$ is generated by a system of parameters.

Let $f_1, \ldots, f_r \in \mathfrak{m}$. We are asked to verify that the following are equivalent:

1. The quotient $\overline{A} := A/(f_1, \ldots, f_r)$ is regular of dimension $d - r$.
2. The residue classes $\overline{f_1}, \ldots, \overline{f_r} \in \mathfrak{m}/\mathfrak{m}^2$ are linearly independent over $k := A/\mathfrak{m}$.

Well, assume (i), i.e., that the quotient is regular of dimension $d - r$. Then what? Well, the dimensional equality implies (by an earlier result) that we may extend $f_1, \ldots, f_r$ to a system of parameters $f_1, \ldots, f_d$ of $\mathfrak{m}$. Now, we are given that $\dim_k(\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2) = d - r$.

Now, hmm. It's surely not the case that *any* system of parameters generates $\mathfrak{m}/\mathfrak{m}^2$; after all, we can take the squares of the elements of a given system to obtain a new system that is contained in $\mathfrak{m}^2$.

A simple example by which to understand what's going on might be when A is a DVR, $\mathfrak{m} = (f)$, and we take $f_1 := f^2$. Then (ii) fails, and indeed, $A/(f^2)$ is not regular. But why not, exactly? Okay, well, we can compute pretty easily the dimension of $\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2$, perhaps? I think it should be $d - \dim \operatorname{span}\{\overline{f_1}, \ldots, \overline{f_r}\}$.

22.1.5