Commutative Algebra
Fall 2020

Notes by Patrick Lei

Lectures by Eric Urban

Columbia University

Disclaimer

These notes were taken during lecture using the `vimtex` package of the editor `neovim`. Any errors are mine and not the instructor's. In addition, my notes are picture-free (but will include commutative diagrams) and are a mix of my mathematical style and that of the instructor. If you find any errors, please contact me at `plei@math.columbia.edu`.

Contents

1

Basic Notions

The references we will use in this course are Matsumura's *Commutative Algebra* and Serre's *Algèbre Locale, Multiplicités*. There is an English translation of Serre. We will begin with general results on rings and modules. We will assume all rings are commutative and unital. Recall that and ideal I of a ring A is prime if and only if A/I is a domain, and I is maximal if and only if A/I is a field.

1.1 Basics of Ideals

Definition 1.1.1. Let $I \subset A$ be an ideal. Then the *radical* $\sqrt{I}$ of I is the set

$$\sqrt{I} := \{x \in A \mid x^a \in I \text{ for some } a \in \mathbb{N}\}.$$

Definition 1.1.2. An ideal $I \subset A$ is *primary* if $I \neq A$ and the zero divisors in A/I are nilpotent. Thus if $xy \in I$ and $x \notin I$, then $y^n \in I$ for some n.

Proposition 1.1.3. *If $Q \subset A$ is primary, then $\sqrt{Q}$ is a prime ideal.*

Proof. If $xy \in \sqrt{Q}$, then $x^n y^n \in Q$. If $x^n \notin Q$, then $y \in \sqrt{q}$ because $(y^n)^a \in Q$. □

Remark 1.1.4. The converse to Proposition 1.1.3 is false in general.

Definition 1.1.5. Let A be a ring. Then the *spectrum* $\operatorname{Spec} A$ of A as a set is the set of prime ideals of A. We may place the Zariski topology on this set, where the basis of open sets is given by $D_f = \operatorname{Spec} A \setminus V_f$, where V_f is the set of prime ideals containing f.

If $\varphi : A \to B$ is a morphism of rings, the morphism $\varphi^* : \operatorname{Spec} B \to \operatorname{Spec} A$ is continuous in the Zariski topology.

Exercise 1.1.6. In particular, if $\pi : A \to A/I$, then π^* is an embedding.

Exercise 1.1.7. Let $I \subset A$ be an ideal. Then let $P_1, \ldots, P_r$ be ideals of A that are all prime except possibly two of them. Show that if $I \not\subset P_i$ for all i, then $I \not\subset \bigcup_i P_i$.

Exercise 1.1.8. Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ be ideals of A such that $\mathfrak{a}_i + \mathfrak{a}_j = A$. Then

1. $\bigcap_i \mathfrak{a}_i = \mathfrak{a}_1 \cdots \mathfrak{a}_r$
2. There is an isomorphism of rings $A/\bigcap_i \mathfrak{a}_i \cong \prod_i A/\mathfrak{a}_i$.

1.2 Localization

Let $S \subset A$ be a multiplicative subset. The main examples are $S_f = \{1, f, f^2, \ldots\}$ and $S_\mathfrak{p} = A \setminus \mathfrak{p}$ for a prime ideal $\mathfrak{p}$. Then if $0 \notin S$, there is at least one ideal $\mathfrak{a}$ such that $\mathfrak{a} \cap S = \emptyset$. Denote the set of such $\mathfrak{a}$ by $\mathcal{M}_S$. Then any maximal element of $\mathcal{M}_S$ is a prime ideal in A. Existence of a maximal element is seen using Zorn's lemma.

To see that maximal elements of $\mathcal{M}_S$ are prime ideals, note that $(x) + P$ is not in $\mathcal{M}_S$, so if $x, y \notin P$, there exist $a, b \in A$ and $s, s' \in S$ such that $ax \equiv s \mod P$ and $by \equiv s' \mod P$. Therefore $abxy \notin P$, so xy is not in P

Lemma 1.2.1. *Let* nil A *be the set of all nilpotent elements. Then*

$$\operatorname{nil} A = \bigcap_{\substack{P \subset A \\ P \text{ prime}}} P.$$

Proof. One direction is easy, so let x be contained in all prime ideals. Then consider the set S_x. If $0 \notin S_x$, then $\mathcal{M}_{S_x}$ is nonempty, so it has a maximal element. This is a prime ideal, which implies x is not contained in some prime. □

Corollary 1.2.2. *Let Q be an ideal of A. Then $\sqrt{Q}$ is the intersection of all prime ideals containing Q.*

Now fix a multiplicative subset S. Then we will define an equivalence relation on $A \times S$. We write

$$(a, s) \sim (b, r)$$

if there exists $t \in S$ such that $t(ar - bs) = 0$. If A is a domain, then this says that $\frac{a}{s} = \frac{b}{r}$. Now we will define the *localization* $S^{-1}A$ to be the set of equivalence classes for this relation. Note there is a natural morphism $A \to S^{-1}A$ that sends $a \mapsto \frac{a}{1}$.

Note that the localization has a universal property: If $\varphi : A \to B$ is a morphism such that $\varphi(S) \subset B^\times$, then φ factors uniquely through $S^{-1}A$.

Localization gives a map $\operatorname{Spec} S^{-1}A \to \operatorname{Spec} A$, and in particular, if $S = \{1, f, f^2, \ldots\}$, we recover the set $D_f = \operatorname{Spec} A_f$.

1.3 Modules

Let A be a ring. Then an A-module M is an abelian group with an action of A. If M is an A-module and $S \subset A$ is a multiplicative set, then $S^{-1}M$ is the set of equivalence classes for $(m, s) \sim (m', s')$ if there exists $t \in S$ such that $t(s'm - sm') = 0$. This is an $S^{-1}A$-module.

Lemma 1.3.1. *Let M be an A-module. Then the map*

$$M \to \prod_{\substack{\mathfrak{p} \subset A \\ \mathfrak{p} \text{ maximal}}} M_\mathfrak{p}$$

is injective.

Proof. Let $x \in M$ be nonzero. Then the annihilator of x is a proper ideal of A, so it is contained in a maximal ideal. This implies that $x_p \in M_p$ is nonzero. □

Corollary 1.3.2. *Let A be a domain. Then $A = \bigcap_\mathfrak{p} A_\mathfrak{p}$, where this intersection makes sense inside the fraction field of A.*

Proof. Apply the previous lemma to $M = K/A$. $\square$

Definition 1.3.3. Let M be an A-module and $x \in A$. Then x is *M-regular* if the morphism $m \mapsto xm$ is injective. Additionally, if x is A-regular, then it is called *regular*.

The set S_0 of all regular elements in A is multiplicative, and the ring $S_0^{-1}A$ is called the *total ring of fractions*. If A is a domain, then $S_0 = A \setminus \{0\}$, and $S_0^{-1}A$ is the field of fractions.

Definition 1.3.4. A ring A is a *local ring* if A has only one maximal ideal. In this case, all elements not in the maximal ideal are units.

Remark 1.3.5. If $I \subset A$ is an ideal such that $A \setminus I = A^\times$, then A is a local ring and I its maximal ideal.

Example 1.3.6. Now let A be a general ring and $\mathfrak{p} \in \operatorname{Spec} A$. Then $A_\mathfrak{p}$ is a local ring with maximal ideal $\mathfrak{p}A_\mathfrak{p}$.

Definition 1.3.7. Now suppose A, B are local rings. Then a morphism $\varphi : A \to B$ of rings is *local* if $\varphi(\mathfrak{m}_A) \subset \mathfrak{m}_B$. This means we have a commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \downarrow & & \downarrow \\ k_A & \longrightarrow & k_B \end{array} \tag{1.1}$$

where $k_A = A/\mathfrak{m}_A$ is the residue field of A.

Recall that the nilradical is the set of all nilpotent elements, or equivalently the intersection of all prime ideals. Then the *Jacobson radical* $\operatorname{rad} A$ is defined to be the intersection of all maximal ideals.

Proposition 1.3.8. *Let $x \in A$. Then $x \in \operatorname{rad} A$ if and only if $1 + xa$ is a unit for any $a \in A$.*

Proof. If $(1 + x)A \neq A$, then $1 + x$ is contained in some maximal ideal mfm, which implies $1 \in \mathfrak{m}$. In the other direction, suppose there exists some maximal ideal $\mathfrak{m}$ such that $x \notin \mathfrak{m}$. Then x is nonzero in $A/\mathfrak{M}$. Thus there exists b such that $1 - xb \in m$, which contradicts the assumption that $1 + xa$ is a unit for any a. $\square$

Lemma 1.3.9 (Nakayama's Lemma)**.** *Let M be a finitely generated A-module. Then let I be an ideal such that $IM = M$. Then there exists $x \in I$ such that $(1 + x)M = 0$. In particular, if $I \subseteq \operatorname{rad} A$, then $M = 0$.*

Proof. We will induct on the number of generators. If $M = A.m$, then $m = xm$ for some $x \in I$, and thus $(1 - x)m = 0$. Now suppose $M = Am_1 + \cdots + Am_r$. Let $M' = M/Am_r$. By the inductive hypothesis, $(1 + x)M' = 0$ for some $x \in I$. Therefore $(1 + x)M \subset Am_r$, so $(1 + x)IM = (1 + x)M \subset Im_r$. Therefore $(1 + x)m_r = ym_r$ for some $y \in I$, and thus $(1 + x - y)m_r = 0$. Thus $(1 + x)(1 + x - y)M \subset (1 + x - y)Am_r = 0$. $\square$

Corollary 1.3.10. *Let $N, N' \subset M$ and $I \subset A$ such that $M = N + IN'$. Then if either*

1. *I is nilpotent;*
2. *$I \subset \operatorname{rad} A$ and N' is finitely generated,*

then $M = N$.

Proof. 1. Suppose I is nilpotent. Then

$$\begin{aligned} M &= N + IN' = N + IM \\ &= N + I(N + IM) \\ &= N + I^2 M \\ &\vdots \\ &= N + I^n M \\ &= N \end{aligned}$$

because I is nilpotent.

2. Let $I \subseteq \operatorname{rad} A$ and N' be finitely generated. Then set $M_0 = M/N = IN_0'$, where N_0' is the image of N' inside M_0. Because N_0' is finitely generated, so is M_0. Therefore $M_0 = IM_0 = 0$, so $M = N$.

□

Remark 1.3.11. Most of the time, we apply this result when A is local and I is the maximal ideal of A. In this case, $M/\mathfrak{m}M$ is a finite-dimensional vector space over $A/\mathfrak{m}$.

1.4 Artinian and Noetherian Rings

Definition 1.4.1. We say that an A-module M satisfies the *ascending chain condition* if any ascending chain of submodules of M becomes stationary. Similarly, M satisfies the *descending chain condition* if any descending chain of submodules becomes stationary. If M satisfies the ascending chain condition, it is called *Noetherian*, and if M satisfies the descending chain condition, it is *Artinian*.

Proposition 1.4.2. *Assume we have a short exact sequence of A modules*

$$0 \longrightarrow N \longrightarrow M \longrightarrow P \longrightarrow 0. \tag{1.2}$$

Then M is Noetherian (resp. Artinian) if and only if N and P are.

Proof. Proving that if M is Noetherian, then N and P are is left to the reader. Now consider a chain

$$M_1 \subset M_2 \subset \cdots M_n \subset \cdots$$

Then let P_i be the image of the M_i in P and $N_i = N \cap M_i$. Then we have an exact sequence

$$0 \to N_i \to M_i \to P_i \to 0.$$

Because (N_i) and (P_i) stabilize, so must M_i from the exact sequence. □

Corollary 1.4.3. *If A is Noetherian (resp. Artinian), then any finitely generated A-module is Noetherian (resp. Artinian).*

Corollary 1.4.4. *Assume A is Noetherian. Then any finitely generated A-module M has a projective resolution by finite free A-modules. In other worse, there exists an exact sequence*

$$\cdots \to F_n \to F_{n-1} \to \cdots \to F_1 \to F_0 \to M \to 0$$

such that each $F_i = A^{m_i}$.

Proof. Suppose M is finitely generated. Then $M = Am_1 + \cdots + Am_r$, so we have a sequence

$$A^r \xrightarrow{\varphi_0} M \to 0.$$

Then $\ker \varphi_0 = N_0$ and $F_0 = A^r$. Then we repeat this process with N_0 taking the role of M. $\square$

Proposition 1.4.5. *An A-module M is noetherian if and only if any submodule of M is finitely generated.*

Proof. Let $N \subseteq M$. Then choose $n_1 \in N$. Then if $An_1 \neq N$, choose $n_2 \in N \setminus An_1$. This process will stop because M is Noetherian, so N is finitely generated.

Now suppose any submodule is finitely generated. Given a chain

$$M_1 \subset M_2 \subset \cdots \subset M_n \subset \cdots,$$

set $N = \bigcup_i M_i$. This is finitely generated and is also equal to the first M_i that contains all of the generators. $\square$

This means that a ring A is noetherian if and only if all ideals of A are finitely generated. In particular, fields and principal ideal domains are Noetherian.

Proposition 1.4.6. *Let M be Noetherian and suppose S is a multiplicative subset of A. Then $S^{-1}M$ is Noetherian.*

Proof. Consider the morphism $M \to S^{-1}M$. Then let N_i be a chain of $S^{-1}A$-modules in $S^{-1}M$. Their preimages M_i form a chain, and they are stationary, so N_i is also stationary. $\square$

Theorem 1.4.7. *Let A be a Noetherian ring. Then $A[X]$ is Noetherian.*

Proof. Let $I \subset A[X]$. Then $\mathfrak{A}_n \subset A$ be generated by the dominant coefficients of polynomials in I of degree at most n. Then we can write $a \in \mathfrak{A}_n$ as $a = \sum \alpha_i \beta_i$ where $\alpha_i \in A$ and β_i a dominant coefficient of a polynomial of degree at most n in I. Thus the $\mathfrak{A}_n$ form a chain of ideals of A that stabilizer for $n \geq N$. Then $\mathfrak{A}_N = (\beta_1, \ldots, \beta_r)$. Set $Q_i = \beta_i X^N + \cdots \in I$. If $P \in I$, then there exists S such that $P = QS + R$ such that $Q \in AQ_1 + \cdots + AQ_r$ and $\deg R < N$.

Therefore $P \in (Q_1, \ldots, Q_r) + A[X]_{N-1} \cap I$, so $I \subset (Q_1, \ldots, Q_r) + A[X]_{N-1} \cap I$ and is thus finitely generated. $\square$

Corollary 1.4.8. *Let B be a finitely-generated A-algebra. Then if A is Noetherian, B is also Noetherian.*

Corollary 1.4.9. *Any finitely generated algebra over a field is Noetherian.*

Remark 1.4.10. Suppose A is Noetherian and M an A-module. If M is finitely generated, then M is Noetherian, but submodules are not necessarily Noetherian. However, they are finitely generated.

Suppose $A \subset B$ is an inclusion of rings. Then we say that $x \in B$ is *integral over A* if there exists a monic polynomial $Q \in A[t]$ such that $Q(x) = 0$.

Proposition 1.4.11. *The following are equivalent:*

1. *$x \in B$ is integral over A;*
2. *$A[x]$ is a finitely-generated A-module;*
3. *There exists $A[x] \subset C \subset B$ such that C is a finitely-generated A-module.*
4. *There exists a faithful $A[x]$-module M which is finitely generated over A.*

Proof. **1 implies 2** Note that $A[x]$ is generated by $1, x, x^2, \dots, x^m$, where Q has degree m.

2 implies 3 Set $C = A[x]$.

3 implies 4 Choose $M = C$.

4 implies 1 Write $M = Am_1 + \cdots + Am_r$. M is an $A[x]$-module, so we can consider $x.M \subset M$. Then for all i, we have $xm_i = \sum a_{ij} m_j$, so if we write consider the matrix $T = (a_{ij})$, then this matrix represents the map given by multiplication by x. Therefore we have

$$\det(T - xI_r) \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = 0,$$

so set $Q = \det(T - xI_r)$. This is monic and $Q(x).m_i = 0$ for all i, and therefore $Q(x)$ acts by 0 on M. Because M is a faithful $A[x]$-module, we have $Q(x) = 0$.

□

Exercise 1.4.12. Let $x, y \in B \supset A$. Show that if x and y are integral over A then so are $x + y, xy$.

Proposition 1.4.13. *Let $A \subset B \subset C$. Assume that A is Noetherian and that C is a finitely-generated A-algebra. If C is a finitely-generated B-module, then B is a finitely-generated A-algebra.*

Proof. Write $C = Bc_1 + \cdots + Bc_r$. Also, we can write $C = A[x_1, \dots, x_m]$ for some $x_i \in C$. Then we can write $x_i = \sum b_{ij} c_j$ and $c_i c_j = \sum b_{ijk} c_k$ for $b_{ij}, b_{ijk} \in B$. Then $B_0 = A[b_{ij}, b_{ijk}]$ is a finitely-generated A-algebra. Any element of C is a polynomial in the x_i with coefficients in A, so C is a finitely-generated B_0-module. In particular, B_0 is Noetherian. Because $B \subset C$, this implies that B is a finitely generated B_0-module, so it is a finitely-generated A-algebra. □

Corollary 1.4.14. *Let k be a field and E a finitely-generated k-algebra. If E is a field, then E is a finite extension of k.*

Proof. Let E be a finitely-generated k-algebra. Then there exist $x_1, \dots, x_r \in E$ that are algebraically independent over k. Then E is algebraic over $k(x_1, \dots, x_r)$, which is the field of fractions of $k[x_1, \dots, x_r]$. However, this gives an inclusion $k \subset F \subset E$, where E is a finitely-generated k-algebra and E is algebraic over F.

By the proposition, F is a finitely-generated k-algebra. Therefore, we can write $F = h[y_1, \dots, y_s]$, where $y_i = \frac{f_i}{g_i}$. Because $k[x_1, \dots, x_n]$ is a UFD, then we can write

$$h = \prod_{i=1}^{s} g_i + 1 \in k[x_1, \dots, x_n].$$

h is repatively prime to all of the g_i, so $\frac{1}{h} \notin k[y_!, \dots, y_s]$. This gives a contradiction, so E must be algebraic over k. □

1.4.1 Primary Decomposition in Noetherian Rings

Definition 1.4.15. An ideal $\mathfrak{a} \subset A$ is *irreducible* if for any decomposition $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$, then either $\mathfrak{a} = \mathfrak{b}$ or $\mathfrak{a} = \mathrm{c}$.

Example 1.4.16. If $\mathfrak{a}$ is a prime ideal, then $\mathfrak{a}$ is irreducible. To see this, if $\mathfrak{a} \mid \mathfrak{b}\mathfrak{c}$, then $\mathfrak{a}$ contains one of $\mathfrak{b}, \mathfrak{c}$, and so either $\mathfrak{a} = \mathfrak{b}$ or $\mathfrak{a} = \mathfrak{c}$.

Remark 1.4.17. Suppose $\mathfrak{m} \subset A$ is a maximal ideal. Then any power $\mathfrak{m}^n$ of $\mathfrak{m}$ is primary.

Proof. We want to prove that the zero divisors of $A/\mathfrak{m}^n$ are nilpotent. Because $\mathfrak{m}$ is maximal, then $A/\mathfrak{m}^n$ is a local ring with maximal ideal $\mathfrak{m}/m^n$. But then $A/\mathfrak{m}^n \setminus \mathfrak{m}/\mathfrak{m}^n$ are all units, so everything in $\mathfrak{m}$ is nilpotent. □

Lemma 1.4.18. *If A is Noetherian, then every irreducible ideal is primary.*

Proof. Let $\mathfrak{a} \subset A$ be irreducible. Then we can pass to the quotient, so we may asusme $\mathfrak{a} = 0$. Let x, y be nonzero with $xy = 0$. We want to show that x is nilpotent.

Because A is Noetherian, then there exists n such that $\operatorname{Ann} x^n = \operatorname{Ann} x^{n+1}$. We want to show that $(x^n) \cap (y) = 0$, so choose $z = ax^n = by$. Then $zx = ax^{n+1} = byx = 0$, so $a \in \operatorname{Ann} x^{n+1} = \operatorname{Ann} x^n$. However, this means $z = 0$. Because 0 is irreducible, then $(x^n) = 0$, so $x^n = 0$. □

Corollary 1.4.19. *If A is Noetherian, then every ideal of A has a primary decomposition. In other words, we can write $I = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r$, where each $\mathfrak{a}_i$ is primary.*

Proof. Let S be the set of ideals with no primary decomposition. If S is nonempty, then S has a maximal element I. To see this, we can use the fact that A is Noetherian, so any chain of ideals in S eventually stabilizes. We know that I is not irreducible, we can write $I = \mathfrak{a} \cap \mathfrak{b}$ such that $I \neq \mathfrak{a}, \mathfrak{b}$. In addition, $\mathfrak{a}, \mathfrak{b} \notin S$, so they have a primary decomposition. This implies that $\mathfrak{a} \cap \mathfrak{b} = I$ has a primary decomposition. □

Remark 1.4.20. This decomposition is not unique. For example, consider $I = \langle x^2, xy \rangle \subset k[x, y]$. Then $I = \langle x \rangle \cap \langle x^2, xy, y^n \rangle$ for all $n > 0$.

1.4.2 Artinian Rings

Proposition 1.4.21. *Assume that A is Artinian.*

1. *Every prime ideal of A is maximal.*
2. *A has finitely many maximal ideals.*
3. *The Jacobson radical of A is nilpotent.*

Proof.

1. Fix a prime ideal $\mathfrak{p}$ and consider the domain $B = A/\mathfrak{p}$. Choose $B \ni x \neq 0$ and consider the decreasing chain (x^n) of ideals. This stabilizes, so there exists $(x^n) = (x^{n+1})$, so we can write $x^n = x^{n+1}y$ for some $y \in B$, and therefore $1 = xy$ because B is a domain. Therefore x has an inverse, so B is a field. Thus $\mathfrak{p}$ is maximal.
2. Suppose we have infinitely many maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n, \ldots$ that are pairwise distinct. Then we form a chain
$$\mathfrak{p}_1 \supset \mathfrak{p}_1\mathfrak{p}_2 \supset \cdots$$
which becomes stationary. Therefore $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset \mathfrak{p}_{n+1}$, so $\mathfrak{p}_{n+1}$ contains some $\mathfrak{p}_i$. Because these ideals are maximal, this is a contradiction.
3. Consider $I = \operatorname{rad}(A) = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$. Then the chain $I \supset I^2 \supset \cdots$ stabilizes, so $I^n = I^{n+1}$ for some n. Let $J = ((0) : I^n)$.[1] We will show that $J = A$. If not, let $J' \supsetneq J$ such that J' is minimal for this property. Such a J' exists because A is Artinian.

   Let $x \in J' \setminus J$ and consider the ideal $Ax + J$ By minimality of J', we see that $Ix + J \subsetneq J'$ (otherwise $J = J'$ by Nakayama's lemma). Therefore $Ix + J = J$, so $Ix \subset J$ and thus $x \in (J : I)$. Therefore, $I^{n+1}x \subset I^n J = (0)$. This implies $I^n x = 0$, so $x \in J$ and thus $J' = J$. □

[1] Here, $(\mathfrak{a} : \mathfrak{b}) = \{x \in A \mid x\mathfrak{b} \in \mathfrak{a}\}$.

Definition 1.4.22. An A-module M is called *irreducible* if 0 and M are the only submodules of M.

Definition 1.4.23. An A-module M is said to be *of finite length* if there exists a (finite) decreasing sequence of submodules
$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_{n+1} = 0$$
such that M_i/M_{i+1} is irreducible for $i = 0, \ldots, n$. In this case, n is actually unique and depends only on M. We will call n the *length* of M.

Proposition 1.4.24. *Let A be a ring. Then A is Artinian if and only if A is of finite length as an A-module.*

Proof. If A is of finite length, then we have a sequence $A = M_0 \supsetneq \cdots \supsetneq M_{n+1} = 0$ where M_i/M_{i+1} is irreducible. If $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots$ is a decreasing chain of ideals, so $\mathfrak{a}_i \cap M_n$ is a decreasing chain of ideals. However, each is either M_n or 0, so this chain stabilizes. Similarly, the chain $(M_j \cap \mathfrak{a}_i)/(M_{j+1} \cap \mathfrak{a}_i)$ also stabilizes for all j. Therefore, there exists N such that for all $i > N$, $M_j \cap \mathfrak{a}_i/(M_{j+1} \cap \mathfrak{a}_i)$ is constant for all j, so $\mathfrak{a}_i$ is constant for all $i > N$.

Now suppose that A is Artinian. Choose $I = \operatorname{rad}(A) = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_m$, where the $\mathfrak{m}_i$ are the maximal ideals of A. Then I is nilpotent, so there exists $n > 0$ such that
$$0 = I^n = \mathfrak{m}_1^n \cdots \mathfrak{m}_m^n.$$
Then $A = A/I^n = \prod A/\mathfrak{m}_j^n$ by the Chinese remainder theorem, so $A/\mathfrak{m}_j^n$ is clearly a local ring and is of finite length as an A-module. Note that the $A/\mathfrak{m}_j$-vector space $\mathfrak{m}_j^i/\mathfrak{m}_j^{i+1}$ is finite-dimensional because A is Artinian. Therefore $\mathfrak{m}_j^i/\mathfrak{m}_j^{i+1}$ is of finite length. $\square$

Exercise 1.4.25. If there is an exact sequence $0 \to N \to M \to P \to 0$ of A-modules, then M is of finite length if and only if N and P are of finite length. Moreover, $\ell(M) = \ell(P) + \ell(N)$.

Theorem 1.4.26. *A is Artinian if and only if A is Noetherian and* $\dim A = 0$*.*

Proof. If A is Artinian, we have already proved that $\dim A = 0$. By the previous proposition, because A is of finite length, A is Noetherian. To see this, for a chain $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$, note that $\mathfrak{a}_m \cap M_i/\mathfrak{a}_m \cap M_{i+1}$ stabilizes. We can do this for each i, so any increasing chain stabilizes.

Now assume A is Noetherian and has dimension 0. We know that (0) has a primary decomposition, so we can write $(0) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$, where each $\mathfrak{q}_i$ is primary. Then $\mathfrak{m}_i = \sqrt{\mathfrak{q}_i}$ is a prime ideal, so it is maximal because $\dim A = 0$. Because A is Noetherian and for all $x \in \mathfrak{m}_i$, $x^n \in \mathfrak{q}_i$ for $n \gg 0$, so there exists N such that $\mathfrak{m}_i^N \subset \mathfrak{q}_i$ for each i. Therefore
$$\mathfrak{m}_1^N \cdots \mathfrak{m}_r^N \subset \mathfrak{q}_1 \cdots \mathfrak{q}_r \subset \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r = 0,$$
so $\mathfrak{m}_1^N \cdots \mathfrak{m}_1^N = 0$. Therefore, $A \cong A/\mathfrak{m}_1^N \times \cdots \times A/\mathfrak{m}_r^N$. Each $A/\mathfrak{m}_i^N$ is of finite length (because each $\mathfrak{m}_i^j/\mathfrak{m}_i^{j+1}$ is a finite-dimensional vector space), so A is of finite length. $\square$

Proposition 1.4.27. *Let A be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Then one of the following holds:*

(a) Either $\mathfrak{m}^n \supsetneq \mathfrak{m}^{n+1}$ for all n, or;

(b) $\mathfrak{m}^n = 0$ for $n \gg 0$ and in this case, A is Artininian.

Proof. If $\mathfrak{m}^n = \mathfrak{m}^{n+1}$, then $\mathfrak{m}^n = 0$ by Nakayama's lemma. This implies that $A = A/\mathfrak{m}^n$ is of finite length. Then if $\mathfrak{p}$ is prime, then $\mathfrak{m}^n = (0) \subset \mathfrak{p}$, so $\mathfrak{m} \subset \mathfrak{p}$. Because $\mathfrak{m}$ is maximal, $\mathfrak{m} = \mathfrak{p}$, so $\dim A = 0$. $\square$

Theorem 1.4.28 (Structure Theorem for Artinian Rings)**.** *An Artinian ring is uniquely up to isomorphism a finite product of Artinian local rings.*

Proof. Previously, we proved that $A = \prod A/\mathfrak{m}_i^N$. Each of these is a local Artinian ring. $\square$

2

Linear Algebra of Modules

Proposition 2.0.1. *Assume M, N, P are A-modules.*

1. *The sequence $N \to M \to P \to 0$ is exact if and only if for all A-modules Q, the sequence*
$$0 \to \mathrm{Hom}(P, Q) \to \mathrm{Hom}(M, Q) \to \mathrm{Hom}(N, Q)$$
is exact.
2. *The sequence $0 \to N \to M \to P$ is exact if and only if for all A-modules Q, the sequence*
$$0 \to \mathrm{Hom}(Q, N) \to \mathrm{Hom}(Q, M) \to \mathrm{Hom}(Q, P)$$
is exact.

Proof. This is left as an exercise. □

Remark 2.0.2. In general, if $0 \to M \to N \to P \to 0$ is exact, then

$$0 \to \mathrm{Hom}(P, Q) \to \mathrm{Hom}(N, Q) \to \mathrm{Hom}(M, Q) 0 \to \mathrm{Hom}(Q, M) \to \mathrm{Hom}(Q, N) \to \mathrm{Hom}(Q, P)$$

are exact but the last morphism is not necessarily surjective.

Definition 2.0.3. A module Q is *projective* if the functor $\mathrm{Hom}(Q, -)$ is exact. Here, exact means that short exact sequences are preserved. Similarly, a module I is *injective* if the functor $\mathrm{Hom}(-, I)$ is exact.

Proposition 2.0.4. *A module Q is projective if and only if Q is a direct factor of a free module. In other words, there exists a free module F and A-module Q' such that $F = Q \oplus Q'$.*

Proof. Suppose Q is projective. Then there is a surjection $\pi : A^{(S)} \to Q \to 0$. Because Q is projective, there exists a map θ such that $\pi \circ \theta = \mathrm{id}$. Therefore $A^{(S)} \cong Q \oplus Q'$, where Q' is the kernel of π.

On the other hand, if $A^{(S)} = Q \oplus Q'$, then for any diagram of the form

$$\begin{tikzcd} M \arrow[r] & P \arrow[r] & 0 \\ & Q \arrow[u] & \end{tikzcd} \tag{2.1}$$

we can embed Q in $A^{(S)}$ and then use projectivity of free modules (because $\mathrm{Hom}(A, M) = M$). □

Remark 2.0.5. If M is projective and finitely generated, then it is a direct factor of a finite free module.

Definition 2.0.6. A *projective resolution* of an A-module M is a right bounded complex

$$\cdots \to P_{n+1} \to P_n \to \cdots \to P_0 \to 0$$

of projective modules such that there exists $P_0 \to M$ such that

$$\cdots P_{n+1} \to P_n \to \cdots \to P_0 \to M \to 0$$

is exact.

Exercise 2.0.7. Show that any module has a projective resolution (**Hint:** construct a free resolution). In addition, any two projective resolutions are homotopic.

Definition 2.0.8. $k_q : M_q \to N_{q+1}$ such that $\phi_q = d^N \circ k_q + k_{q-1} \circ d^M$.

2.1 Tor and Ext Functors

Note that for a complex, we can compute the *homology* $H_q(M_\bullet) := \ker d_q / \operatorname{Im} d_{q+1}$. This measures the defect of the complex from being exact. For functors that are not exact, we can construct *derived functors* that measure the defect of exactness. Let $F : A\text{-Mod} \to A\text{-Mod}$ be right exact. Then for any M, we can consider a projective resolution $P_\bullet \to M \to 0$. Applying F to $P_.$, then the *left derived functor* $L_\bullet F(M)$ is defined by $L_\bullet F(M) = H_\bullet(F(P_\bullet))$.

Proposition 2.1.1. *If* $0 \to M \to N \to P \to 0$ *is exact, then we have a long exact sequence*

$$\cdot \to L_1 F(M) \to L_q F(N) \to L_q F(P) \to L_{q-1} F(M) \to \cdots \to L_0 F(M) \to L_0 F(N) \to L_0 F(P) \to 0.$$

Recall that the tensor product $M \otimes N$ of two modules M, N is an A-module with a bilinear map $M \times N \to M \otimes N$ such that all bilinear maps $M \times N \to P$ factor through $M \otimes N$.

Proposition 2.1.2. *The functors* $- \otimes N, \operatorname{Hom}(N, -)$ *are an adjoint pair.*

Corollary 2.1.3. *If* $N \to M \to P \to 0$ *is exact, then*

$$N \otimes Q \to M \otimes Q \to P \otimes Q \to 0$$

is exact.

Definition 2.1.4. A module Q is *flat* if $- \otimes Q$ is exact.

We can defined the left derived functors $\operatorname{Tor}_q(Q, M)$ of the tensor product.

Proposition 2.1.5. *Any projective module is flat.*

Proof. Clearly free modules are flat, so write $Q \oplus Q' = A^{(S)}$ and then note that the tensor product distributes over the sum. □

Proposition 2.1.6. *The following are equivalent:*

1. *M is flat over A.*
2. *If $N' \hookrightarrow N$, then $M \otimes N' \hookrightarrow M \otimes N$.*

3. *For all finitely generated ideals $I \subset A$, $I \otimes M \hookrightarrow M$.*
4. *For any finitely generated ideals $I \subset A$, $\mathrm{Tor}_1(M, A/I) = 0$.*
5. *For any finitely generated module N, we have $\mathrm{Tor}(M, N) = 0$.*
6. *For all $a_i \in A$ and $x_i \in M$ such that $\sum a_i x_i = 0$ there exist $y_1, \ldots, y_s \in M$ and b_{ij} such that $x_i = \sum b_{ij} y_j$.*

Proof. It is clear that 1 is equivalent to 2 implies 3 implies 4 implies 5. The directions 3 implies 2 and 4 implies 3 are left to the reader.

1 implies 6 Choose $a_i \in A, x_i \in M$ such that $\sum_{i=1}^r a_i x_i = 0$. Then define a map $A^r \xrightarrow{f} A$ by

$$f(b_1, \ldots, b_r) = \sum_{i=1}^r a_i b_i$$

and define $K = \ker f$. Because M is A-flat, we have an exact sequence

$$0 \to K \otimes M \to M^r \to M.$$

Then $(x_1, \ldots, x_r) \in \ker f \otimes \mathrm{id}_M$. Therefore there exists $b_1, \ldots, b_s \in K$ and $y_1, \ldots, y_s \in M$ such that

$$(x_1, \ldots, x_r) = \sum_{j=1}^s b_j \otimes y_j.$$

Writing $b_j = (b_{1j}, \ldots, b_{rj})$, we obtain the identity

$$\sum_{i=1}^r b_{ij} a_i = 0$$

and thus $x_i = \sum b_{ji} y_j$.

6 implies 3 Choose an ideal $I \subset A$. Consider the map $0 \to I \otimes M \to M$. Then for any element in the kernel, we can write

$$\sum_i a_i \otimes x_i \mapsto \sum a_i x_i = 0.$$

Then we can write $x_i = \sum b_{ij} y_j$ and so

$$\sum a_i \otimes x_i = \sum \sum a_i \otimes b_{ij} y_j = \sum \left(\sum a_i b_{ij} \right) \otimes y_j = 0$$

and thus $I \otimes M \to M$ is injective. □

Let $\phi : A \to B$ be a map of rings and let M be a B-module. Define ϕ to be *flat* if B is flat as an A-module.

Proposition 2.1.7. *If $\phi : A \to B$ is flat and M is a flat B-module, then M is also flat as an A-module.*

Proof. Let S be an A-module. Then $S \otimes_A M = S \otimes_A (B \otimes_B M) = (S \otimes_A B) \otimes_B M$. If $0 \to N_1 \to N_2$ is an exact sequence of A-module, by flatness of B as an A-module, then

$$0 \to N_1 \otimes_A B \to N_2 \otimes_A B$$

is exact. Because M is flat over B, we see that

$$0 \to (N_1 \otimes_A B) \otimes_B M \to (N_2 \otimes_A B) \otimes_B M$$

is exact, as desired. □

Now let M be an A-module. Then for any map $A \xrightarrow{\phi} B$, we can consider the B-module $M_{(B)} \coloneqq M \otimes_A B$.

Proposition 2.1.8. *If M is A-flat, then $M_{(B)}$ is B-flat.*

Proof. For a B-module S, write

$$\begin{aligned} S \otimes_B M_{(B)} &= S \otimes_B (M \otimes_A B) \\ &\cong S \otimes_B (B \otimes_A M) \\ &\cong (S \otimes_B B) \otimes_A M \\ &\cong S \otimes_A M. \end{aligned}$$

Thus if $0 \to S_1 \to S_2$ is exact, then $0 \to S_1 \otimes_A M \to S_2 \otimes_A M$ is exact because M is A-flat, as desired. $\square$

Proposition 2.1.9. *Let $S \subset A$ be a multiplicative subset of A. Then the morphism of rings $A \to S^{-1}A$ is flat.*

The proof is left to the reader. This can be reformulated as $M \otimes_A S^{-1}A \cong S^{-1}M$.

Now we will give some remarks about the Ext functors. For any left exact functor, we may define the right derived functors $R^\bullet F$ by

$$R^i F(M) = H^i(F(I^\bullet))$$

where $M \to I^\bullet$ is an injective resolution. Then we will define the right derived functors of $\mathrm{Hom}_A(N, -)$ by $\mathrm{Ext}^i_A(N, -)$.

Proposition 2.1.10. *If M is injective, then $\mathrm{Ext}^i_A(N, M) = 0$ for all $i > 0$. Similarly, if N is projective, then $\mathrm{Ext}^i_A(N, M) = 0$ for all $I > 0$.*

Remark 2.1.11. We can compute $Ext^i(N, M)$ using a projective resolution of N.

Proposition 2.1.12. *Let $A \to B$ be a morphism of rings and let M, N be A-modules. Then let $M_{(B)}, N_{(B)}$ be their base changes to B. Then we have*

$$\mathrm{Ext}^i_B(M_{(B)}, N_{(B)}) = \mathrm{Ext}^i_A(M, N)_{(B)}$$

and

$$\mathrm{Tor}^B_i(M_{(A)}, N_{(B)}) = \mathrm{Tor}^A_i(M, N)_{(B)}$$

if B is A-flat.

Proof. This follows from the definition of $\mathrm{Ext}, \mathrm{Tor}$ using projective resolutions using the following facts.

1. If M is A-projective, then $M_{(B)}$ is B-projective.

2. Since B is A-flat, for any complex $X^\bullet$ of A-modules, then $H^\bullet(X^\bullet_{(B)}) = H^\bullet(X^\bullet)_{(B)}$.

$\square$

2.2 Flatness

Proposition 2.2.1. *Let A be a local ring. Then any finitely generated flat A-module is free. In particular, free, projective, and flat are equivalent for A-modules.*

Proof. We know that free implies projective implies flat. Therefore we will show that if M is flat, then it is free. Assume that M is finitely generated and A-flat. Let $k = A/\mathfrak{m}$ be the residue field of A. Define $\overline{M} = M \otimes_A k$, which is a vector space of finite dimension over k. Then there exists $x_1, \dots, x_r \in M$ that descend to a basis of $\mathfrak{M}$.

Then the map $A^r \to M, (a_i) \mapsto \sum a_i x_i$ is surjective by Nakayama's lemma. We will prove that this map is injective by induction. If $r = 1$, then suppose $ax_1 = 0$. Then there exist $y_1, \dots, y_s, b_{11}, \dots, b_{1s}$ such that

$$x_1 = \sum_{j=1}^{s} b_{ij} y_j$$

where $ab_{ij} = 0$ for all $j = 1, \dots, s$. Because $\overline{x}_1 \neq 0$, there exists j such that $\overline{b}_{1j} \neq 0$ so b_{1j} is invertible in A. Thus $a = 0$.

Now suppose $a_1 x_1 + \cdots + a_r x_r = 0$. Then there exist $y_1, \dots, y_s$ and b_{ij} such that

$$x_i = \sum b_{ij} y_j$$

and

$$\sum a_i \begin{pmatrix} b_{i1} \\ \vdots \\ b_{ij} \end{pmatrix} = 0.$$

Because $\overline{x}_r \neq 0$, we see that $\overline{b}_{rj} \neq 0$ for some j and thus b_{ij} is a unit. Then $a_1 b_{1j} + \cdots + a_r b_{rj} = 0$, so we can write

$$\sum a_i (x_i - c_i x_r) = 0.$$

We know that $\overline{x}_1 - c_1 \overline{x}_r, \dots, \overline{x}_{r-1} - c_{r-1} \overline{x}_r$ are linearly independent over k, so from the induction $a_1 = \cdots = a_r = 0$ and thus $a_r = 0$. $\square$

Remark 2.2.2. If M is not finitely generated, the proposition is false. An example is given by taking the field of fractions of a local domain.

When proving the proposition, we in fact proved that

Lemma 2.2.3. *If $x_1, \dots, x_r \in M$ with M a flat A-module for A a local ring and $\overline{x}_1, \dots, \mathfrak{x}_r$ are linearly independent in $M \otimes_A k$, then $x_1, \dots, x_r$ are linearly independent in M.*

Proposition 2.2.4. *Suppose that $A \to B$ is flat and I_1, I_2 are ideals of A. Then*

1. *$(I_1 \cap I_2)B = I_1 B \cap I_2 B$;*
2. *If I_2 is finitely generated, then $(I_1 : I_2)B = (I_1 B : I_2 B)$.*

Proof. The proof is a formal consequence of flatness.

1. Consider the exact sequence $0 \to I_1 \cap I_2 \to A \to A/I_1 \times A/I_2$. Tensoring with B, we obtain an exact sequence
$$0 \to (I_1 \cap I_2) \otimes B \to B \to B/I_1 B \times B/I_2 B.$$
But then $(I_1 \cap I_2) \otimes B = (I_1 \cap I_2)B$, but the kernel of the last map is clearly $I_1 B \cap I_2 B$.

2. Set $I_2 = (x_1, \dots, x_r)$. Then because

$$(I_1 : I_2) = \bigcap_{i=1}^{r} (I_1 : x_i A),$$

it suffices to prove the result for I_2 a principal ideal. We have an exact sequence

$$0 \to (I_1 : xA) \to A \xrightarrow{\times x} A/I_1.$$

Tensoring by B, we obtain

$$0 \to (I_1 : xA) \otimes B \to B \to B/I_1 B,$$

and by analysing the kernel, we see that $(I_1 : xA)B = (I_1 B : xB)$. By repeated application of the previous part, the desired result follows. $\square$

Example 2.2.5. We will give an example where the previous proposition is not true in general. Let $A = k[x,y]$ and $B = A/xA = k[y]$. Then choose $I_1 = (x+y), I_2 = (y)$, so $I_1 \cap I_2 = I_1 I_2 = ((x+y)y)$. But then we have $(I_1 \cap I_2)B = y^2 B$, but $I_1 B \cap I_2 B = yB$.

Another example is $A = k[x,y], B = k[x,y,z]/(xz-y) \cong k[x,z], I_1 = xA, I_2 = yA$. Here we can check that $(I_1 \cap I_2) = (xy)$, that $(I_1 \cap I_2)B = x^2 zB$, but $I_1 B \cap I_2 B = xzB$. Viewing this geometrically as $\operatorname{Spec} B \to \operatorname{Spec} A$, we can check the fiber over $(0,0)$ and see that the map is not flat.

Proposition 2.2.6. *Let $A \xrightarrow{\varphi} B$ be a ring homomorphism. The following are equivalent:*

1. *B is flat over A;*
2. *$B_{\mathfrak{P}}$ is flat over $A_{\mathfrak{p}}$ for all $\mathfrak{P} \in \operatorname{Spec} B$ and $\mathfrak{p} = \varphi^{-1}(\mathfrak{P})$.*
3. *$B_{\mathfrak{P}}$ is flat over $A_{\mathfrak{p}}$ for any $\mathfrak{P}$ maximal.*

Proof. **1 implies 2:** We know that $B_{\mathfrak{p}}$ is flat over $A_{\mathfrak{p}}$. But then $B_{\mathfrak{P}}$ is flat over $B_{\mathfrak{p}}$ because it is a localization. By transitivity of flatness, $B_{\mathfrak{P}}$ is flat over $A_{\mathfrak{p}}$.

2 implies 3: This is obvious.

3 implies 1: Note that for all $\mathfrak{P}$ maximal, $\operatorname{Tor}_i^A(B,N)_{\mathfrak{P}} = 0$ for $i > 0$. This implies that $\operatorname{Tor}_i^!(B,N) = 0$, and thus B is flat over A. To get that the first Tor is zero we need to use the lemma belos. $\square$

Lemma 2.2.7. *Let $\varphi : A \to B$ be a morphism of rings and choose $\mathfrak{P} \in \operatorname{Spec} B$. Then let $\mathfrak{p} = \varphi^{-1}(\mathfrak{P})$ and N an A-module. Then $\operatorname{Tor}_i^A(B,N)$ is a B-module and $\operatorname{Tor}_i^A(B,N)_{\mathfrak{P}} = \operatorname{Tor}_i^{A_{\mathfrak{p}}}(B_{\mathfrak{P}}, N_{\mathfrak{p}})$.*

Proof. Let $X_\bullet \to N$ be a projective resolution. Then Tor is computed by the homology of the complex $B \otimes_A X_\bullet$. When we localize, we localize the homology at the B term. However, $B_{\mathfrak{p}} \otimes_A X_\bullet = B_{\mathfrak{P}} \otimes_{A_{\mathfrak{p}}} (X_\bullet)_{\mathfrak{p}}$, so because X_i is A-projective, then $X_{\mathfrak{p}}$ is $A_{\mathfrak{p}}$-projective, and thus $(X_\bullet)_{\mathfrak{p}}$ is a projective resolution of $N_{\mathfrak{p}}$. Thus the complex $B_{\mathfrak{P}} \otimes_{A_{\mathfrak{p}}} (X_\bullet)_{\mathfrak{p}}$ computes the Tor as desired. $\square$

Definition 2.2.8. An A-module N is said to be *faithfully flat* if

1. N is A-flat;
2. For any sequence $P \to Q \to R$ of A-modules, if $P \otimes N \to Q \otimes N \to R \otimes N$ is exact, then $P \to Q \to R$ is exact.

Theorem 2.2.9. *Let M be an A-module. Then the following are equivalent:*

1. *M is faithfully flat over A;*
2. *M is flat and for any nonzero N, $M \otimes N \neq 0$;*
3. *M is flat and for all maximal ideals $\mathfrak{m} \subset A$, $\mathfrak{m}.M \neq M$.*

Proof. **1 implies 2:** Choose the sequence $0 \to N \to 0$. Then tensor with M. If $N \otimes M = 0$, the sequence is now exact, then the original sequence is exact, and thus $N = 0$.

2 implies 3: Consider $N = A/\mathfrak{m}$. Then $N \otimes M = M/\mathfrak{m}M \neq 0$, so $M \neq \mathfrak{m}M$.

3 implies 2: Choose $0 \neq x \in N$ and set $I = \mathrm{Ann}(x) \subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Then $Ax = A/I$, so $Ax \otimes M \cong M/IM \neq 0$. Because Ax injects into N, $Ax \otimes M$ injects into $N \otimes M$, which must be nonzero.

2 implies 1: Consider the sequence $P \xrightarrow{f} Q \xrightarrow{g} R$. Then because M is flat, $\ker(g \otimes \mathrm{id}_M) = \ker(g) \otimes M$ and $\mathrm{Im}(f \otimes \mathrm{id}_M) = \mathrm{Im}(f) \otimes M$. If $g \circ f = 0$, then $\mathrm{Im}(g \circ f) = 0$, which happens iff $\mathrm{Im}(g \circ f) \otimes M = 0$. Then $\mathrm{Im}((g \otimes \mathrm{id}_M) \circ (f \otimes \mathrm{id}_M)) = 0$.

If $P \otimes M \to Q \otimes M \to R \otimes M$ is exact, then $P \to Q \to R$ is a complex. Finally, we need that $\ker g = \mathrm{Im}\, f$. By flatness of M, we can tensor to find that $\ker g / \mathrm{Im}\, f \otimes M = 0$ and then we see that $\ker g / \mathrm{Im}\, f = 0$. ☐

Corollary 2.2.10. *Let $A \to B$ be a local homomorphism and let M be a finitely-generated B=module. Then M if flat over A if and only if M is faithfully flat over A.*

Proof. Clearly faithfully flat implies flat. Then we need to show that $M \neq \mathfrak{m}_A.M$. By Nakayama's lemma, we know that $M \otimes k_B \neq 0$, so $\mathfrak{m}_{\mathfrak{B}} M \neq M$. In particular, $\mathfrak{m}_A M \neq M$. In particular, this implies that item 3 of the previous theorem holds. Thus M is faithfully flat over A. ☐

Remark 2.2.11. This also shows that flat and faithfully flat are equivalent over local rings. Alternatively, we can use the equivalence of flat and free.

Remark 2.2.12. Faithful flatness is transitive. In addition, if $A \to B$ is a morphism of rings, and M is faithfully flat over A, then $M \otimes_A B$ is faithfully flat over B.

Proposition 2.2.13. *Let M be a faithfully flat B-module which is faithfully flat over A. Then B is faithfully flat over A.*

Proof. Let N be an A-module. Then $(B \otimes_A N) \otimes_B M = M \otimes_A N \neq 0$ if $N \neq 0$. This implies that $B \otimes_A N$ is nonzero. Now it suffices to show that B is flat over A.

Let (S) be an exact sequence of A-modules. Then if we consider $((S) \otimes_A M) = (S) \otimes_A M$, this is exact by flatness of M over A. By faithful flatness of M over B, this implies that $(S) \otimes_A B$ is exact. ☐

Proposition 2.2.14. *Let $A \to B$ be faithfully flat. Then*

1. *For any A-module N, the map $N \to N \otimes_A B$ is injective;*
2. *If $I \subset A$ is an ideal, then $IB \cap A = I$;*
3. *The map $\operatorname{Spec} B \to \operatorname{Spec} A$ is surjective.*

Proof. 1. Let $0 \neq x \in N$. Then $Ax \otimes B \hookrightarrow N \otimes B$. Because B is faithfully flat, $Ax \otimes B \neq 0$.

2. Recall that $B/IB = B \otimes A/I$. Then the map $A/I \to B/IB$ is injective. Therefore we have a map $A \to B/IB$ which has kernel $I = IB \cap A$.

3. Choose $\mathfrak{p} \in \operatorname{Spec} A$. Then $B_\mathfrak{p} = B \otimes_A A_\mathfrak{p}$ and $A_\mathfrak{p} \to B_\mathfrak{p}$ is faithfully flat by base change. This means that $\mathfrak{p}B_\mathfrak{p} \subsetneq B_\mathfrak{p}$. Thus if we choose $\mathfrak{m}$ to be a maximal ideal of $B_\mathfrak{p}$ containing $\mathfrak{p}B_\mathfrak{p}$, we see that $\mathfrak{m} \cap A_\mathfrak{p} \supset \mathfrak{p}A_\mathfrak{p}$ and thus they are equal by maximality of $\mathfrak{p}A_\mathfrak{p}$. Then if we choose $\mathfrak{P} = \mathfrak{m} \cap B$, we see that
$$\begin{aligned}\mathfrak{P} \cap A &= \mathfrak{m} \cap A \\ &= \mathfrak{m} \cap A_\mathfrak{p} \cap A \\ &= \mathfrak{p}A_\mathfrak{p} \cap A \\ &= \mathfrak{p}.\end{aligned}$$
Thus the image of $\mathfrak{P}$ is $\mathfrak{p}$. □

Theorem 2.2.15. *Let $\varphi : A \to B$ be a map of rings. The following are equivalent:*

1. *The map φ is faithfully flat.*
2. *The map φ is flat and* $\operatorname{Spec} B \to \operatorname{Spec} A$ *is surjective.*
3. *The map φ is flat and for all maximal ideals $\mathfrak{m}$ of A, there exists some maximal ideal $\mathfrak{m}'$ of B such that $\varphi^{-1}(\mathfrak{m}') = \mathfrak{m}$.*

Proof. **1 implies 2:** This is the previous proposition.

2 implies 3: Choose a maximal ideal $\mathfrak{m} \subset A$. Then there exists $\mathfrak{P} \in \operatorname{Spec} B$ such that $\varphi^{-1}(\mathfrak{P}) = \mathfrak{m}$. But then if $\mathfrak{m}'$ is any maximal ideal containing $\mathfrak{P}$, we see that $\varphi^{-1}(\mathfrak{m}') = \varphi^{-1}(\mathfrak{P}) = \mathfrak{m}$ by maximality of $\mathfrak{m}$.

3 implies 1: We want to prove that $B \neq \mathfrak{m}B$ for any maximal ideal $\mathfrak{m}$ of A. Then there exists $\mathfrak{m}'$ such that $\varphi^{-1}(\mathfrak{m}') = \mathfrak{m}$. But then $B \supsetneq \mathfrak{m}' \supset \mathfrak{m}B$. □

Proposition 2.2.16 (Descent)**.** *Let $A \to B$ be faithfully flat and M be an A-module. Then*

1. *M is flat (resp. faithfully flat) if and only if $M \otimes_A B$ is B-flat (resp. B-faithfully flat).*
2. *Assume A is a local ring and M is finitely-generated. Then M is free if and only if $M \otimes_A B$ is B-free.*

Proof. 1. Let (S) be an exact sequence. Then $(S) \otimes_A B$ is exact, so $S \otimes_A B \otimes M \otimes_A B = (S \otimes_A M) \otimes_A B$ is exact. By faithful flatness of B, $(S) \otimes_A M$ is exact. Now if $N \neq 0$ is another A-module, we know that $M_{(B)} \otimes N_{(B)} \neq 0$, but this is the same as $(M \otimes_A N)_{(B)}$, so $M \otimes_A N$ is nonzero.

2. Assume that A is local. Then suppose $M \otimes_A B$ is free. Therefore $M \otimes_A B$ is faithfully flat. But then, M is faithfully flat over A, which means that M is free because M is finitely generated. □

Exercise 2.2.17. Let $A \subset B$ be integral domains. Assume that A and B have the same field of fractions. Prove that $A \hookrightarrow B$ is faithfully flat if and only if $A = B$.

2.3 More on Integral Dependence

Recall Proposition **1.4.11**.

Corollary 2.3.1. *Let $x_1, \ldots, x_n \in B$. If each x_i is integral over A, then $A[x_1, \ldots, x_n]$ is a finitely-generated A-module.*

Corollary 2.3.2. *Let $C \subset B$ be the set of integral elements over A. Then C is a subring of B.*

Proof. Note that $x + y, xy \in A[x][y] \in A[x, y]$, which is a finitely-generated A module. Therefore they are integral over A. □

Remark 2.3.3. The ring C is not necessarily finitely-generated over A. For an example, choose $\mathbb{Z}\overline{\mathbb{Z}} \subset \overline{\mathbb{Q}}$.

Definition 2.3.4. Let $A \subset B$. Then we say that B is *integral over* A if all elements of B are integral over A.

Corollary 2.3.5. *Let $A \subset B \subset C$ be extensions of rings. Then if B is integral over A and C is integral over B, then C is integral over A.*

Proof of this is left to the reader.

Definition 2.3.6. Let A be an integral domain. We say that A is *integrally closed* if for all $x \in K = \operatorname{Frac} A$, then x is integral over A if and only if $x \in A$.

Definition 2.3.7. Assume that $A \subset B$ is an inclusion of rings. Then the *integral closure of A inside B* is the set of all elements of B that are integral over A.

Example 2.3.8. A typical example of this situation is when A is a domain, K is its fraction field, and L/K is a field extension. Then we can consider the integral closure B of A inside L. In number theory, if K is a number field, we define its *ring of integers* $\mathcal{O}_K$ to be the integral closure of $\mathbb{Z}$ in K.

Exercise 2.3.9. If $K = \mathbb{Q}(\zeta_p)$, prove that $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.

Exercise 2.3.10. Let B be an integral domain and $A \subset B$. Prove that the integral closure of A inside B is integrally closed.

Lemma 2.3.11. *Let B be a domain that is integral over A. Then A is a field if and only if B is a field.*

Proof. Assume that A is a field. Now choose $0 \neq x \in B$. But then we know that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

for some $a_i \in A$ and $a_0 \neq 0$. But then we have

$$x^{-1} = -a_0^{-1}\left(\sum_{i=1}^{n} a_i x^i\right)$$

and so $x^{-1} \in B$.

Now assume that B is a field. Choose $0 \neq xinA$. Then $x^{-1} \in B$. This means that x^{-1} is integral over A, which means that

$$a^{-n} + a_{n-1}x^{-(n-1)} + \cdots + a_0 = 0$$

for some $a_i \in A, a_0 \neq 0$. Then if we multiply by a^{n-1}, we obtain

$$a^{-1} + a_{n-1} + a_{n-2}x + \cdots + a_0 x^{n-1} = 0,$$

which means $x^{-1} \in A$. □

Corollary 2.3.12. *Let $A \subset B$ and B be integral over A. Let $\mathfrak{P} \in \operatorname{Spec} B$ and $\mathfrak{p} = A \cap \mathfrak{P}$. Then $\mathfrak{p}$ is maximal if and only if $\mathfrak{P}$ is maximal.*

Proof. Note that $B/\mathfrak{P}$ is integral over $A/\mathfrak{p}$. Then we apply the lemma to $A/\mathfrak{p} \subset B/\mathfrak{P}$. □

We can refine this into going-up and going-down. Let $\phi : A \to B$ be a morphism of rings and let $\phi^* : \operatorname{Spec} B \to \operatorname{Spec} A$ be the induced map of spaces.

Definition 2.3.13 (Going-up)**.** A ring homomorphism ϕ satisfies the *Going-up property* if the following holds:

Let $\mathfrak{p} \subset \mathfrak{p}'$ be prime ideals of A and suppose that $\phi^*(\mathfrak{P}) = \mathfrak{p}$. Then there exists $\mathfrak{P}' \subset \mathfrak{P}$ such that $\phi^*(\mathfrak{P}') = \mathfrak{p}'$.

Definition 2.3.14 (Going-down)**.** A ring homomorphism ϕ satisfies the *Going-down property* if the following holds:

Let $\mathfrak{p} \subset \mathfrak{p}'$ be prime ideals of A. Then let $\mathfrak{P}' \in \operatorname{Spec} B$ satisfy $\phi^*(\mathfrak{P}') = \mathfrak{p}'$. Then there exists $\mathfrak{P} \subset \mathfrak{P}'$ with $\phi^*(\mathfrak{P}) = \mathfrak{p}$.

Lemma 2.3.15. *The going-down property is equivalent to the following:*

For all $\mathfrak{p} \in \operatorname{Spec} A$ and $\mathfrak{P}$ a minimal prime ideal of B containing $\mathfrak{p}B$, we have $\mathfrak{P} \cap A = \mathfrak{p}$.

Proof. First suppose that going-down holds. Then choose $\mathfrak{P}$ be a minimal prime containing $\mathfrak{p}B$. Then $\mathfrak{p}' = \phi^{-1}(\mathfrak{P}) \supset \mathfrak{p}$. If $\mathfrak{p}' \neq \mathfrak{p}$, then there exists $\mathfrak{P}_0 \subset \mathfrak{P}$ such that $\varphi^{-1}(\mathfrak{P}_0) = \mathfrak{P}$, which contradicts minimality.

Now suppose the other condition holds. Suppose $\mathfrak{P}'$ goes to $\mathfrak{p}' \supset \mathfrak{p}$. Then we know that $\mathfrak{p}B \subset \mathfrak{p}'B \subset \mathfrak{P}'$. If we fix $\mathfrak{P}_0$ to be the minimal prime containing $\mathfrak{p}B$, then we see that $\mathfrak{P}_0 \cap A = \mathfrak{p}$. □

Theorem 2.3.16. *If $\phi : A \to B$ is flat, then going-down holds.*

Proof. Fix $\mathfrak{p} \subset \mathfrak{p}'$ and let $\mathfrak{P}'$ lie over $\mathfrak{p}'$. Then we know that $B_{\mathfrak{P}'}$ is flat over $\mathfrak{A}_{\mathfrak{p}'}$. Because $A_{\mathfrak{p}'}$ is local and the map $A_{\mathfrak{p}'} \to \mathfrak{B}_{\mathfrak{P}'}$ is local, it is faithfully flat. This implies that the map $\operatorname{Spec} B_{\mathfrak{P}'} \to \operatorname{Spec} A_{\mathfrak{p}'}$ is surjective, so there exists $\mathfrak{P}_1 \in \operatorname{Spec} B_{\mathfrak{P}'}$ such that $\phi^{-1}(\mathfrak{P}_1) = \mathfrak{p}A_{\mathfrak{p}'}$.

Now set $\mathfrak{P} := \mathfrak{P}_1 \cap B$. Then we see that

$$\begin{aligned}
\phi^{-1}(\mathfrak{P}) &= \phi^{-1}(\mathfrak{P}_1 \cap B) \\
&= \phi^{-1}(\mathfrak{P}_1) \cap A \\
&= \mathfrak{p}\mathfrak{A}_{\mathfrak{p}'} \cap A \\
&= \mathfrak{p}.
\end{aligned}$$

□

We will see consequences of this result in algebraic geometry.

We will now consider integral ring extensions $A \subset B$.

Theorem 2.3.17 (Cohen-Seidenberg)**.** *Suppose $A \subset B$ is an integral extension. Then the following hold:*

1. *The map* $\operatorname{Spec} B \to \operatorname{Spec} A$ *is surjective.*
2. *There are no inclusion relations between the prime ideals of B which are above a fixed prime ideal of A.*
3. *Going-up holds for $A \subset B$.*
4. *If A is local with maximal ideal $\mathfrak{m}$, then the prime ideals of B lying over $\mathfrak{m}$ are precisely the maximal ideals of B.*

5. *Assume further that A and B are integral domains and that A is integrally closed. Then going-down holds for $A \subset B$.*

6. *If B is the integral closure of A in a normal extension of field L of $K := \operatorname{Frac} A$, then any two prime ideals of B lying over the same prime ideal of A are conjugate by an element of $\operatorname{Aut}(L/K)$.*

Proof. We prove **4**, then **1**, **2**, and **3**, then **6**, and finally **5**.

1. Let $\mathfrak{p} \in \operatorname{Spec} A$. Then $B_\mathfrak{p} = B \otimes_A A_\mathfrak{p}$ is integral over $A_\mathfrak{p}$. Applying **4**, we obtain the desired result.

2. Consider $B_\mathfrak{p}$ again. By **4**, because ideals lying over $\mathfrak{p}$ are maximal, there cannot be inclusion relations between them.

3. Let $\mathfrak{p} \subset \mathfrak{p}'$ and $\mathfrak{P} \in \operatorname{Spec} B$ lying over $\mathfrak{p}$. Then $B/\mathfrak{P}$ is integral over $A/\mathfrak{p}$. By **1**, we know that $\operatorname{Spec} B/\mathfrak{P} \to \operatorname{Spec} A/\mathfrak{p}$ is surjective. Thus there exists $\overline{\mathfrak{P}}' \in \operatorname{Spec} B/\mathfrak{P}$ lying over $\overline{\mathfrak{p}}' = \mathfrak{p}'/\mathfrak{p}$. Then we know that $\overline{\mathfrak{P}}' = \mathfrak{P}'/\mathfrak{P}$ for some prime ideal $\mathfrak{P}'$ of B, and this is the ideal we are looking for.

4. This is a consequence of Lemma 2.3.15.

5. Write $L = \operatorname{Frac} B \supset K = \operatorname{Frac} A$. Then let L_1 be the normal closure of L/K. Then let $\mathfrak{p} \subset \mathfrak{p}'$ in A and $\mathfrak{P}'$ in B lie over $\mathfrak{p}'$. Then let $\mathfrak{P}_1 \subset \mathfrak{P}_1'$ in B_1 the integral closure of A in L_1. These exist thanks to **1** and **3**.

   Let $\mathfrak{P}_1''$ in B_1 such that $\mathfrak{P}_1'' \cap B = \mathfrak{P}'$. Then there exists σ such that $\mathfrak{P}_1'' = \sigma(\mathfrak{P}_1')$ because both ideals are above $\mathfrak{p}'$. Then we can choose
   $$\mathfrak{P} := \sigma(\mathfrak{P}_1) \cap B \subset \mathfrak{P}_1'' \cap B = \mathfrak{P}'.$$
   We need to show that $\mathfrak{P} \cap A = \mathfrak{p}$. But this is simply
   $$\begin{aligned} \mathfrak{P} \cap A &= \sigma(\mathfrak{P}_1) \cap A \\ &= \sigma(\mathfrak{P}_1 \cap A) \\ &= \sigma(\mathfrak{p}) \\ &= \mathfrak{p}. \end{aligned}$$

6. We know that A is integrally closed in K. Then let L/K be a finite Galois (we can always reduce to this case) extension and B the integral closure of A in L. Then let $\mathfrak{P}, \mathfrak{P}' \in \operatorname{Spec} B$ lie above $\mathfrak{p} \in \operatorname{Spec} A$. We will show there exists $\sigma \in \operatorname{Gal}(L/K)$ such that $\sigma(\mathfrak{P}) = \mathfrak{P}'$.

   Suppose that no such σ exists. Then for all $\sigma \in \operatorname{Gal}(L/K)$, $\mathfrak{P}' \neq \sigma(\mathfrak{P})$. In particular, $\mathfrak{P}' \not\subset \sigma(\mathfrak{P})$. Then there exists $x \in \mathfrak{P}'$ which is not in any $\sigma(\mathfrak{P})$ then we see that
   $$y := \prod_{\sigma \in \operatorname{Gal}(L/K)} \sigma(x) \in K$$
   is integral over A, so $y \in A$. Also, $y \notin \mathfrak{P}$ because $x \notin \sigma(\mathfrak{P})$, so $x \in \mathfrak{P}'$ and thus $y \in \mathfrak{P}'$, so $y \in \mathfrak{p} \subset \mathfrak{P}$. This gives a contradiction. ☐

Corollary 2.3.18. *Assume that B is integral over A.*

1. *If $\mathfrak{P}_0 \subsetneq \mathfrak{P}_1 \subsetneq \cdots \subsetneq \mathfrak{P}_r$ is a chain of prime ideals of B, the the $\mathfrak{p}_i := \mathfrak{P}_i \cap A$ for a chain of prime ideals of A.*

2. *If $p_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ is a chain of prime ideals of A, then there exists a chain $\mathfrak{P}_0 \subsetneq \cdots \subsetneq \mathfrak{P}_r$ of prime ideals of B above it.*

3. *If A is integrally closed and B is a domain, then for any chain $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ and $\mathfrak{P}_r \in \operatorname{Spec} B$ above $\mathfrak{p}_r$, there exists a chain $\mathfrak{P}_0 \subsetneq \cdots \subsetneq \mathfrak{P}_r$ above the chain in A.*

Proof. The proof is clear and left to the reader. □

Definition 2.3.19. Let $\mathfrak{p} \in \operatorname{Spec} A$. Then define the *height* of $\mathfrak{p}$ by

$$\operatorname{ht}(\mathfrak{p}) = \max \{n \geq 0 \mid \exists \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}\}.$$

Then define the *dimension* of A by

$$\dim A = \max \{\operatorname{ht}(\mathfrak{p}) \mid p \in \operatorname{Spec} A\}.$$

Corollary 2.3.20. *Let $A \subset B$ be an integral extension. Then*

1. *Suppose $\mathfrak{P} \in \operatorname{Spec} B$ lies above $\mathfrak{p} \in \operatorname{Spec} A$. Then $\operatorname{ht}(\mathfrak{P}) \leq \operatorname{ht}(\mathfrak{p})$.*

2. $\dim A = \dim B$.

3. *If A is integrally closed and B is a domain, then we have $\operatorname{ht}(\mathfrak{P}) = \operatorname{ht}(\mathfrak{p})$.*

Proof. This is an immediate consequence of the previous corollary. □

2.4 Associated Primes

Let M be an A-module and $\mathfrak{p} \in \operatorname{Spec} A$.

Definition 2.4.1. We say that $\mathfrak{p}$ is an *associated prime* of M if one of the two following equivalent conditions hold.

1. There exists $x \in M$ such that $\operatorname{Ann}_A(x) = \mathfrak{p}$;

2. There is an injection $A/\mathfrak{p} \hookrightarrow M$.

We will denote the set of associated primes using the unfortunate notation $\operatorname{Ass}_A(M)$. Then the set of primes $\mathfrak{p}$ such that $M_\mathfrak{p} \neq 0$ will be denoted $\operatorname{Supp}_A(M)$.

Proposition 2.4.2. *Let $\mathfrak{p}$ be a maximal element of $\{\operatorname{Ann}(x) \mid x \in M, x \neq 0\}$. Then $\mathfrak{p} \in \operatorname{Ass}_A(M)$.*

Proof. We will show that such a maximal element is actually a prime ideal. Suppose $ab \in \mathfrak{p}$. Then $\mathfrak{p} = \operatorname{Ann}(x)$ for some nonzero x, so $b.x \neq 0$. Then $\operatorname{Ann}(x) \subset \operatorname{Ann}(bx) \neq A$. By maximality, $\operatorname{Ann}(x) = \operatorname{Ann}(bx)$. Because $abx = 0$, then $a \in \operatorname{Ann}(bx) = \mathfrak{p}$. □

Corollary 2.4.3. *Let A be Noetherian.*

1. *M is nonzero if and only if $\operatorname{Ass}_A(M)$ is nonempty.*

2. *The set of zero divisors for M is the union of the associated primes of M.*

Proof.
1. If there is some associated prime, then clearly $M \neq 0$. In the other direction, the set of annihilators has a maximal element because A is Noetherian, so there must be an associated prime.

2. Let $a \in \operatorname{Ann}(x)$ for some nonzero $x \in M$. Then $\operatorname{Ann}(x) \subset \mathfrak{p}$ is contained in some associated prime (because it is contained in some maximal element), and thus every zero divisor is contained in an associated prime. The other direction is obvious. $\square$

Lemma 2.4.4. *Let $S \subset A$ be a multiplicative set and M an A-module. Then*

$$\operatorname{Ass}_A(S^{-1})M = \varphi^*(\operatorname{Ass}_{S^{-1}A}(S^{-1}M)).$$

Proof. Let $\mathfrak{p} \in \operatorname{Ass}_A(S^{-1}M)$. Then $\mathfrak{p} = \operatorname{Ann}_A \frac{x}{1}$ for some $x \in M$, so $\mathfrak{p} \cap S$ must be empty. Next, we see that the set $\{\operatorname{Ann}_A(sx) \mid s \in S\}$ contains some maximal element $\mathfrak{m}$ because A is Noetherian. But then $\mathfrak{m} = \operatorname{Ann}_A(s_0 \cdot x) = \mathfrak{p}$.

On the other hand, if $a \in \mathfrak{p}$, then $\frac{ax}{1} = 0$, which means $asx = 0$ for some $s \in S$. Then $a \in \operatorname{Ann}_A(sx) \subset \operatorname{Ann}(s_0 sx) = \operatorname{Ann}(s_0 x)$. Thus $\mathfrak{p} \subset \operatorname{Ann}(s_0 x)$. Thus we have shown that

$$\operatorname{Ass}_A(S^{-1}M) \subset \varphi^* \operatorname{Ass}_{S^{-1}A}(S^{-1}M).$$

The other inclusion is clear. $\square$

Theorem 2.4.5. *Let A be Noetherian and M and A-module. Then $\operatorname{Ass}_A(M) \subset \operatorname{Supp}_A(M)$ and any minimal element of $\operatorname{Supp}_A(M)$ is inside $\operatorname{Ass}_A(M)$.*

Proof. Let $\mathfrak{p} \in \operatorname{Ass}_A(M)$. Then $A/\mathfrak{p}$ injects in M, so we have an injection $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \hookrightarrow M_\mathfrak{p}$. Thus $\mathfrak{p} \in \operatorname{Supp}_A(M)$.

Now choose a minimal $\mathfrak{p} \in \operatorname{Supp}_A(M)$. Thus $M_\mathfrak{p}$ is nontrivial, so there exists a prime ideal $\mathfrak{q} \subset \mathfrak{p}$ such that $\mathfrak{q}A_\mathfrak{p} \in \operatorname{Ass}_{A_\mathfrak{p}}(M_\mathfrak{p})$. Thus $M_\mathfrak{q} = (M_\mathfrak{p})_{\mathfrak{q}A_\mathfrak{p}}$ is nonzero, so $\mathfrak{q} \in \operatorname{Supp}(M)$. By minimality, $\mathfrak{q} = \mathfrak{p}$ and thus $\mathfrak{p}A_\mathfrak{p} \in \operatorname{Ass}_{A_\mathfrak{p}}(M_\mathfrak{p})$. Therefore $\mathfrak{p} \in \operatorname{Ass}_A(M)$. $\square$

Definition 2.4.6. If $\mathfrak{p} \in \operatorname{Ass}_A(M)$, then $\mathfrak{p}$ is not necessarily minimal in the support of M. Then such a prime is called an *embedded prime*.

Proposition 2.4.7. *Let A be Noetherian and M a finitely-generated A-module. Then*

1. *There exists a chain*
$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$
such that $M_i/M_{i-1} \cong A/\mathfrak{p}_i$ for $i = 1, \ldots, n$ and $\mathfrak{p}_i \in \operatorname{Supp}_A(M)$.

2. *Given such a sequence, we have $\operatorname{Ass}_A(M) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. In particular this set is finite.*

Proof.
1. Suppose $M \neq 0$ Then choose $\mathfrak{p}_1 \in \operatorname{Ass}_A(M)$ and let M_1 be the image of $A/\mathfrak{p}_1$ in M. Then if M/M_1 is nonzero, choose $\mathfrak{p}_1 \in \operatorname{Ass}_A(M/M_1)$ and M_2 defined analogously to M_1. This gives a sequence of submodules of M such that $A/\mathfrak{p}_i \cong M_i/M_{i-1}$. Because M is Noetherian, this sequence becomes stationary. Thus there exists n such that $M_n = M$.

2. This is a consequence of the next lemma.

$\square$

Remark 2.4.8. In general the support of a module is **not** finite.

Lemma 2.4.9. *Assume we have an exact sequence of modules $0 \to M' \to M \to M''$. Then $\operatorname{Ass}(M) \subset \operatorname{Ass}(M') \cup \operatorname{Ass}(M'')$.*

Proof. If $\mathfrak{p} \in \operatorname{Ass}(M)$, there exists $N \subset M$ such that $N \cong A/\mathfrak{p}$. Then if $N \cap M' = 0$, $N \hookrightarrow M''$ and $\mathfrak{p} \in \operatorname{Ass}(M'')$. If the intersection is nonzero, then there exists some nonzero $x \in N \cap M'$ such that $\operatorname{Ann}_A(x) = p$ because $A/\mathfrak{p}$ is a domain. Thus $\mathfrak{p} \in \operatorname{Ass}(M')$. $\square$

Definition 2.4.10. We say that M is *coprimary* if $\mathrm{Ass}_A(M) = \{\mathfrak{p}\}$.

Definition 2.4.11. Let $N \subset M$. Then we say that N is $\mathfrak{p}$*-primary* if $\mathrm{Ass}_A(M/N) = \{\mathfrak{p}\}$. Alternatively, we say that N *belongs to* $\mathfrak{p}$.

Lemma 2.4.12. *A module M is coprimary if and only if M is nonzero and any zero divisor for M is locally nilpotent (for all $x \in M$, there exists $n > 0$ such that $a^n.x = 0$).*

Proof. Suppose that M is coprimary. Now suppose that $a \in \mathfrak{p}$ and $x \in M$. Then $\mathrm{Ass}(Ax) = \{\mathfrak{p}\}$, so $\mathfrak{p}$ is minimal in the support of A_x, which is $V(\mathrm{Ann}(x))$. Therefore, $\mathfrak{p} = \sqrt{\mathrm{Ann}(x)}$. Thus for $a \in \mathfrak{p}$, $a^n \in \mathrm{Ann}(x)$.

In the other direction, let $\mathfrak{p}$ be the set of locally nilpotent elements with respect to M. This is clearly an ideal of A. Then let $\mathfrak{q} \in \mathrm{Ass}_A(M)$. Then $x \in M$, so $\mathfrak{q} = \mathrm{Ann}(x)$. Therefore $\mathfrak{p} \subset \mathfrak{q}$ because $\mathfrak{q}$ is a prime ideal. However, $\mathfrak{q}$ is contained in the set of zero divisors, which is precisely $\mathfrak{p}$. □

Remark 2.4.13. Let $I \subset A$ be an ideal. Then $\mathrm{Ass}_A(A/I) = \{\mathfrak{p}\}$ if and only if the zero divisors of A/I are locally nilpotent. This is equivalent to I being primary.

Lemma 2.4.14.

1. *Let $Q_1, Q_2 \subset M$ be $\mathfrak{p}$-primary submodules. Then $Q_1 \cap Q_2$ is $\mathfrak{p}$-primary.*
2. *Let $N = Q_1 \cap \cdots \cap Q_r$ be an irredundant decomposition (i.e. Q_i is $\mathfrak{p}_i$-primary) for distinct $\mathfrak{p}_i$. Then $\mathrm{Ass}_A(M/N) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.*

Proof.

1. Note that $M/Q_1 \cap Q_2$ injects in $M/Q_1 \oplus M/Q_2$. The desired result follows from the previous lemma.
2. First, note that $M/N \hookrightarrow \bigoplus M/Q_i$. Then suppose $\mathrm{Ass}(M/N) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. Then we have an injection
$$\frac{Q_2 \cap \cdots \cap Q_r}{N} \hookrightarrow M/N$$
and thus $\mathrm{Ass}((Q_1 \cap \cdots \cap Q_r)/N)$ is contained in $\mathrm{Ass}(M/N)$. By the exact sequence
$$0 \to N \to Q_2 \cap \cdots \cap Q_r \to M/Q_1,$$
we see that $\mathrm{Ass}(Q_2, \cap \cdots \cap Q_r/N) = \{\mathfrak{p}_1\}$. □

Theorem 2.4.15. *Let M be a module over a Noetherian ring A. Then for all $\mathfrak{p} \in \mathrm{Ass}(M)$, there exists a $\mathfrak{p}$-primary submodule $Q(\mathfrak{p}) \subset M$ such that*

$$\bigcap_{\mathfrak{p} \in \mathrm{Ass}(M)} Q(\mathfrak{p}) = \{0\}.$$

Proof. Fix $\mathfrak{p} \in \mathrm{Ass}(M)$. Consider the set

$$\mathcal{S}_{\mathfrak{p}} = \{N \subseteq M \mid \mathfrak{o} \notin \mathrm{Ass}(N)\}.$$

This set is nonempty because $0 \in \mathcal{S}_{\mathfrak{p}}$. Next, if $N_\lambda \in \mathcal{S}_{\mathfrak{p}}$ is a chain, then the module $N = \bigcup N_\lambda$ is a submodule of M. In addition, $\mathrm{Ass}(N) \subset \bigcup \mathrm{Ass}(N_\lambda)$. This implies that $\mathcal{S}_{\mathfrak{p}}$ contains a maximal element by Zorn's lemma. Choose such a maximal element $Q(\mathfrak{p})$.

We will show that $M/Q(\mathfrak{p})$ is coprimary. By the exact sequence

$$0 \to Q(\mathfrak{p}) \to M \to M/\mathfrak{Q}(\mathfrak{p}),$$

if $\mathfrak{p}' \in \operatorname{Ass}(M/Q(\mathfrak{p}))$, then $\mathfrak{p}' = \mathfrak{p}$ because otherwise $A/\mathfrak{p}'$ would inject in $M/Q(\mathfrak{p})$ as $Q'/Q(\mathfrak{p})$. Then $\operatorname{Ass}(Q') \subset \operatorname{Ass}(Q(\mathfrak{p})) \cup \operatorname{Ass}(Q'/Q(\mathfrak{p}))$, so $Q' \supsetneq Q(\mathfrak{p})$, contradicting minimality. Thus $\operatorname{Ass}(M/Q(\mathfrak{p})) = \{\mathfrak{p}\}$.

The second part of the claim follows immediately from the fact that $\operatorname{Ass}\left(\bigcap Q(\mathfrak{p})\right) = \bigcap \operatorname{Ass}(Q(\mathfrak{p})) = \emptyset$. □

Corollary 2.4.16. *Let M be an A-module of finite type. Then any $N \subset M$ has a primary decomposition*

$$N = Q_1 \cap \cdots \cap Q_r$$

such that

1. *The Q_i are $\mathfrak{p}_i$-primary;*
2. *No Q_i can be omitted;*
3. *This decomposition is irredundant:* $\operatorname{Ass}(M/N) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.

Proof. Apply the previous theorem to M/N. Because M/N is of finite type, $\operatorname{Ass}(M/N)$ is finite. Then use the previous lemma. □

Exercise 2.4.17. Let $A \xrightarrow{\varphi} B$ be a morphism of rings and let M be a B-module. Then prove that

$$\varphi^*(\operatorname{Ass}_B(M)) = \operatorname{Ass}_A(M)$$

where $\varphi^* \colon \operatorname{Spec} B \to \operatorname{Spec} A$ is the induced map of spaces.

3

Dimension Theory

3.1 Graded Rings and Modules

Let $A = \bigoplus_{n \geq 0} A_n$ be a graded ring. This means that $A_n \cdot A_m \subset A_{n+m}$. Then an A-module M is a graded module if

$$M = \bigoplus_{n \in \mathbb{Z}} M_n$$

such that $A_n \cdot M_m \subset M_{n+m}$. We will call M_m the homogeneous elements of degree m on M.

Now let $N \subset M$ be a submodule. We say that N is a graded submodule if $N = \bigoplus N \cap M_m$. N is also called homogeneous. A homogeneous element of M is an element of some M_m. Being a graded submodule is the same as every element being a sum of homogeneous elements.

Lemma 3.1.1. *The following are equivalent:*

1. *N is a homogeneous submodule.*
2. *N is generated by homogeneous elements.*
3. *If $x = x_r + \cdots + x_n \in N$ for $x_i \in M_i$, then for all i, $x_i \in N$.*

Moreover, if $N \subset M$ is homogeneous, then so is M/N, and

$$M/N = \bigoplus_m M_m/N_m.$$

Proof. The proof is left as an exercise to the reader. □

Example 3.1.2. Let k be any ring. Then the ring $A = k[x_1, \ldots, x_r]$ is a graded ring where the grading is by the degree of each monomial. In particular, $A_0 = k$. Then an ideal $I \subset A$ is graded if $I = \bigoplus_n I_n$ where $I_n = I \cap A_n$. In addition, A/I is a graded ring.

Proposition 3.1.3. *Let A be a Noetherian graded ring and M a graded A-module. Then*

1. *If $\mathfrak{p} \in \operatorname{Ass}(M)$, then $\mathfrak{p}$ is a graded ideal of A and there exists a homogeneous $x \in M$ such that $\mathfrak{p} = \operatorname{Ann}(x)$.*
2. *One can choose a $\mathfrak{p}$-primary graded submodule $Q(\mathfrak{p})$ such that $0 = \bigcap_{\mathfrak{p} \in \operatorname{Ass}(M)} Q(\mathfrak{p})$.*

Proof. Let $x \in M$ and set $\mathfrak{p} = \mathrm{Ann}(M)$. Then write $x = x_e + x_{e-1} + \cdots + x_0$. Then for $f \in \mathfrak{p}$, write $f = f_r + \cdots + f_s$. If $fx = 0$, then we can write

$$0 = fx + f_r x_e + (f_{r-1}x_e + f_r x_{e-1}) + \cdots$$

and deduce that $0 = f_r x_e = f_r^2 x_{e-1} = \cdots$. Then $f_r^e \in \mathfrak{p}$, so $f_r \in \mathfrak{p}$. By induction, all $f_i \in \mathfrak{o}$, so $\mathfrak{p}$ is graded.

The proof of the second part is simply the following lemma. □

Lemma 3.1.4. *Let $\mathfrak{p}$ be a graded prime ideal and $Q \subset M$ such that Q is $\mathfrak{p}$-primary. Let $Q' \subset Q$ be the submodule of Q generated by the homogeneous elements of Q. Then Q' is $\mathfrak{p}$-primary.*

Proof. This will be proved later. □

We will now discuss filtrations of rings. A *filtration* is a sequence of subgroups

$$A = J_0 \supset J_1 \supset J_2 \cdots$$

such that $J_n \cdot J_m = J_{n+m}$. If we set

$$A' = \bigoplus_{n=0}^{\infty} J_n / J_{n+1},$$

then A' is a graded ring.

The basic example is $J_m = I^m$ for some fixed ideal $I \subset A$. in this case, the filtration is called the I-adic filtration.

Lemma 3.1.5. *Let A be a Noetherian ring and set $I \subset A$. Then*

$$\mathrm{gr}^I A = \bigoplus_{n=0}^{\infty} I^n / I^{n+1}$$

is a Noetherian graded ring.

Proof. Because I is finitely-generated, then I/I^2 is a finitely-generated A/I-module. Thus $\mathrm{gr}^I(A)$ is a finitely-generated A/I-algebra. If $x_1, \ldots, x_r$ is a set of generators of I, then

$$A/I[x_1, \ldots, x_r] \to \mathrm{gr}^I A$$

is surjective, so because A/I is Noetherian, so is $A/I[x_1, \ldots, x_r]$ and thus so is $\mathrm{gr}^I A$. □

Let A be an Artinian ring and $B = A[x_1, \ldots, x_r]$ be a graded ring. Then let M be a finitely-generated graded B-module. Each graded piece M_n is an A-module, so write $F_M(n) = \ell_A(M_n)$. Because M is finitely generated, we have a map

$$\bigoplus_{i=1}^{r} B(d_i) \twoheadrightarrow M.$$

Here, $B(d_i) = B$ as a B-module with the gradation $B(d)_n = B_{n-d}$. Thus M is generated by homogeneous elements x_{d_i} of degree d_i. This gives us the map

$$\bigoplus_{i=1}^{r} B_{m-d_i} \hookrightarrow M_m$$

$$(f_i) \mapsto \sum_{i=1}^{r} f_i x_{d_i}$$

and thus $\ell_A(M_m) \leq \sum_{i=1}^r \ell_A(B_{m-d_i})$. But then B_m is a free A-module, and thus

$$\ell_A(B_m) \leq \binom{r+m-1}{m-1} \ell(A).$$

Theorem 3.1.6. *Let A, B, M be as above. Then there is a polynomial $f_M(x) \in \mathbb{Q}[x]$ such that*

$$\ell_A(M_n) = f_M(n)$$

for $n \gg 0$. This is called the Hilbert-Samuel polynomial for M. The degree of this polynomial will give the first definition for the dimension of M.

Proof. Say that M satisfies the property $P(M)$ if there exists $f \in \mathbb{Q}(x)$ such that $\ell(M_n) = f(n)$ for $n \gg 0$.

1. First, we will show that if $N_1, N_2 \subset M$ and $P(M/N_1), P(M/N)2$ hold, then $P(M/N_1 \cap N_2)$ holds.
2. Second, if N is irreducible, then $P(M/N)$ holds.

If we prove these two things, then we simply use a primary decomposition of $0 \subset M$. Then the second statement implies that $P(M/N_i)$ holds and then we simply repeatedly apply the first to see that $P(M)$ holds.

1. Suppose $N = N_1 \cap N_2$ with N, N_1, N_2 graded. We then have an exact sequence

$$0 \to N_1/(N_1 \cap N_2) \to M/(N_1 \cap N_2) \to M/N_1 \to 0$$

and we know that $N_1/(N_1 \cap N_2) = (N_1 + N_2)/N_1$ is graded. Then we see that $F_{M/(N_1 \cap N_2)} = F_{M/N} + F_{(N_1+N_2)/N_1}$, so we only need to prove that $F_{N_1+N_2/N_1}$ exists. But then $F_{N_1+N_2/N_1} = F_{M/N_2} - F_{M/N_1+N_2}$ and because $P(M/N_1 + N_2)$ holds, so does $P(M/N_1 \cap N_2)$.

2. Let N be irreducible. We know that $M' = M/N$ is coprimary, so N is $\mathfrak{p}$-primary for some prime ideal $\mathfrak{p} \subset B$. Write $I = (x_1, \ldots, x_m)$. If $I \subset \mathfrak{p}$, then $M'_m = 0$ for $n \gg 0$. Indeed, if d is the maximal degree of a system of generators of M', then $M'_{n+d} = I^n \cdot M'_d$. On the other hand, because M' is $\mathfrak{p}$-primary, then elements in $\mathfrak{p}$ are locally nilpotent. Thus there exists $k \gg 0$ such that $p^k \cdot M'_d = 0$ and thus $M'_{n+d} = 0$ for $n \geq k$. Thus $F_{M/N}$ exists and is identically zero.

In the second case, $I \not\subset \mathfrak{p}$. Then suppose that $x_1 \notin \mathfrak{p}$. Thus x_1 is not a zero divisor for M'. Thus, we have an exact sequence

$$0 \to M' \to x_1 \to M' \to M'/x_1M' \to 0$$

which then gives

$$0 \to (M/N)_{n-1} \to (M/N)_n \to (M/N + x_1M)_n \to 0$$

when restricting to a single graded piece. Thus $N \subsetneq N + x_1M$. This implies that $f_{M/N+x_1M}$ exists because above, we proved that if $P(M/N')$ holds for any $N' \supsetneq N$ implies that $P(M/N)$ holds. Then for $n \geq n_0$, we have $\ell((M/N)_m) - \ell((M/N)_{n-1}) = f_{M/N+x_1M}(n)$. This implies that

$$\ell((M/N)_m) = f(n) + f(n-1) + \cdots + \ell(M/N)_{n_0}.$$

Then $f(n) + \cdots + f(n_0) = g(n)$ for some polynomial g of degree $\deg f + 1$ and then $f_{M/N} = g + \ell((M/N)_{n_0})$. $\square$

Now let $A \supset I$ and M be an A-module with filtration

$$M_0 = M \supset M_1 \supset \cdots \supset M_n \supset \cdots$$

We say that the filtration is

1. *I-admissible* if $IM_n \subset M_{n+1}$ for all $n \gg 0$;
2. *I-acic* if $IM_n = M_{n+1}$ for all $n \geq 0$;
3. *essentially I-adic* if $IM_n = M_{n+1}$ for $n \gg 0$.

Remark 3.1.7. A filtration on M defines a topology on M so that M is a topological group. Here, a system of neighborhoods of 0 is $(M_n)_{n \gg 0}$. If $\bigcap M_n = 0$, then the topology is Hausdorff. If the filtration is essentially I-adic, then the topology is called the I-adic topology.

Lemma 3.1.8. *Let A and I be as before. Let M be an A-module with an admissible filtration. Let $A' = \bigoplus_{n=1}^{\infty} I^n x^n \subset A[x]$ and*

$$M' = \bigoplus M_n \otimes_A Ax^n = \bigoplus M_n x^n.$$

1. *M' is a A'-module.*
2. *The filtration is essentially I-adic if and only if M' is a finitely-generate A'-module.*

Proof. 1. This is trivial.

2. Note that M' is a graded A'-module. If M' is finitely generated, then write $M' = A'm_1 + \cdots + A'm_r$. Then we see that $M'_n = IxM'_{n-1}$ for $n > \max\{\deg m_i\}$. Thus M_n is essentially I-adic.

   Conversely, if $M_n = I^{n-n_0} M_{n_0}$ for $n \geq n_0$, then, then it is clear that M' is generated by $M_{n_0} x^{n_0} + \cdots + M_1 x + M_0$ and is thus finitely generated. □

Theorem 3.1.9 (Artin-Rees)**.** *Let A be a Noetherian ring and $I \subset A$. Then let M be a finitely-generated A-module and $N \subset M$ be a submodule. Then there exists $r > 0$ such that*

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

for all $n \geq r$.

Proof. Let $M_n = I^n M$ be the I-adic filtration. Then $N_n = I^n M \cap N$ is I-admissible. Then both $N' \subset M'$ are both A'-modules. We know that A' is Noetherian, so because M_n, M' is finitely generated. Thus N' is also Noetherian, so it is also finitely-generated. This implies that N_m is essentially I-adic, as desired. □

Remark 3.1.10. This theorem is saying that the filtration $I^n M \cap N$ is essentially I-adic.

Corollary 3.1.11 (Krull Intersection Theorem)**.** *Let A, I, M as above.*

1. *If $N = \bigcap_{n=0}^{\infty} I^n M$, then $IN = N$.*
2. *If $I \subset \mathrm{rad}(A)$, then $\bigcap_{n=0}^{\infty} I^n M = 0$.*

Proof. 1. Note that $N \subset M$. Then apply the Artin-Rees theorem to $N = I^n M \cap N$.

2. Apply Nakayama's lemma. □

Corollary 3.1.12. *Let A be a Noetherian domain and let $I \subset A$ be a proper ideal. Then $\bigcap_n I^n = 0$.*

Proof. Let $N = \bigcap_{n=0}^{\infty} I^n$. By the previous corollary, $IN = N$. Then N is finitely generated because A is Noetherian. Thus there exists $x \in I$ such that $(1+x)N = 0$, which implies that $N = 0$ because A is a domain. $\square$

Exercise 3.1.13. Let A be Noetherian and M a finitely-generated A-module. Then let I, J be generated by M-regular elements. Then there exists $r > 0$ such that $(I^n M : J) = I^{n-r}(I^r M : J)$. Here, $(N : J) = \{m \in M \mid Jm \subset N\}$.

3.2 Other Notions of Dimension

Let A be a ring. Then we define the *Krull dimension*

$$\dim A = \sup \{\mathrm{ht}(\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Spec} A\}.$$

Then for any ideal $I \subset A$, define the height of I to be

$$\mathrm{ht}(I) = \inf \{\mathrm{ht}(\mathfrak{p}) \mid \mathfrak{p} \supset I\}.$$

Proposition 3.2.1. *For any ideal I, we have* $\dim(A/I) + \mathrm{ht}(I) \leq \dim A$.

Proof. Consider a chain

$$\mathfrak{p}_{d'} \supsetneq \cdots \supsetneq \mathfrak{p}_0 \supset I$$

where $d' = \dim(A/I)$. Then we see that $\dim A \geq d' + \mathrm{ht}(\mathfrak{p}_0) \geq d' + \mathrm{ht}(I)$, as desired. $\square$

Then if M is an A-module, define $\dim M = \dim(A/\operatorname{Ann}_A M)$.

Proposition 3.2.2. *Assume that A is Noetherian and M is a finite A-module. Then the following are equivalent:*

1. *M is of finite length.*
2. *$A/\operatorname{Ann}_A M$ is Artinian.*
3. $\dim M = 0$.

Proof. Clearly conditions 2 and 3 are equivalent. Then M is a quotient of $(A/\operatorname{Ann}_A M)^r$, so 2 implies 1. Thus we need to prove that 1 implies 3.

Assume that $\ell(M) < \infty$. If we write $A' = A/\operatorname{Ann}_A(M)$, then M is a finite A'-module. If $\dim A' > 0$, then there exists $\mathfrak{p} \subset A'$ that is minimal but not maximal. Then because $\operatorname{Ann}_{A'}(M) = 0$, we have $\mathfrak{p} \in V((0)) = \operatorname{Supp}(M)$. But then $\mathfrak{p} \in \operatorname{Ass}_{A'}(M)$ and thus we have an embedding $A'/\mathfrak{p} \hookrightarrow M$. But then $\dim M'/\mathfrak{p} > 0$, so $\ell(A'/\mathfrak{p}) = \infty$ and thus $\ell(M) = \infty$. $\square$

Now let A be a semilocal ring. Let $\mathfrak{m} = \operatorname{Rad} A$. Then an ideal $I \subset A$ is called an *ideal of definition* of A if there exists $s > 0$ such that $\mathfrak{m}^s \subset I \subset \mathfrak{m}$.

Remark 3.2.3. I is an ideal of definition if and only if A/I is Artinian.

Let $A^* = \mathrm{gr}^I(A) = \bigoplus_{n=0}^{\infty} I^n/I^{n+1}$ be the graded ring with respect to the I-adic filtration and let $M^* = \mathrm{gr}^I(M)$ be the corresponding graded A^*-module. Then if $I = (x_1, \dots, x_i) \subset A$, define

$$B = A/I[x_1, \dots, x_r].$$

Then we have a map $B \twoheadrightarrow A^*$, so M^* is a B-module. Now define $\chi(M, I, n) := \ell(M/I^n M)$. If M is a finite A-module, then $M/I^n M$ is of finite length (because A/I^n is Artinian) and thus

$$\ell(M/I^n M) = \ell(M/IM) + \ell(IM/I^2 M) + \cdots + \ell(I^{n-1}M/I^n M).$$

Then if $\ell(I^s M/I^{s+1}M)$ is a polynomial in s of degree at most $r-1$ for $s \gg 0$, then $\ell(M/I^n M)$ is a polynomial of degree at most r for $n \gg 0$.

Now if J is another ideal of definition, then there exists s such that $J^s \subset I$ and thus $\chi(M, J, ns) \geq \chi(M, I, n)$. Therefore

$$d^\bullet \chi(M, J, n) \geq d^\bullet \chi(M, I, n)$$

and so the degree of $\chi(M, I, n)$ is independent of I. Denote this degree by $d(M)$. We know that $d(M) \geq r$, which is the number of generators of I.

Lemma 3.2.4. *Assume we have an exact sequence of finite A-modules*

$$0 \to M' \to M \to M'' \to 0.$$

Then $d(M) = \max\{d(M'), d(M'')\}$ and $\chi(M, I, n) - \chi(M', I, n) - \chi(M'', I, n)$ is a polynomial of degree strictly less that $d(M'')$.

Proof. For each n we have an exact sequence

$$0 \to \frac{M'}{I^n M \cap M'} \to \frac{M}{I^n M} \to \frac{M''}{I^n M''} \to 0.$$

Then $\Delta := \chi(M, I, n) - \chi(M'', I, n) = \ell(M/I^n M) - \ell(M''/I^n M) = \ell(M'/I^n M \cap M')$. By Artin-Rees, there exists r such that $M' \cap I^n M = I^{n-r} \cdot (M' \cap I^r M)$. But then

$$\chi(M', I, n-r) \leq \Delta \leq \chi(M', I, n)$$

because $\chi(M', I, n) - \chi'(M', I, n-r)$ has degree strictly less than $d(M')$, and the desired result follows. □

Lemma 3.2.5. *Let A be a Noetherian semilocal ring. Then $d(A) \geq \dim A$. In particular, $\dim A < \infty$.*

Proof. We will induct on $d(A)$. If $d(A) = 0$, then $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ for $n \gg 0$. By Nakayama, we see that $\mathfrak{m}^n = 0$, so $\ell(A) < \infty$ and thus A is Artinian.

Assume that $d(A) > 0$ and $\dim A > 0$. Let

$$\mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_\ell = \mathfrak{p}$$

be a chain of prime ideals of length $\ell > 0$. Choose $x \in \mathfrak{p}_{\ell-1} \setminus \mathfrak{p}_\ell$. Then $\dim(A/\mathfrak{p} + xA) \geq \ell - 1$. Because we have the exact sequence

$$0 \to A/\mathfrak{p} \xrightarrow{\times x} A/\mathfrak{p} \to A/\mathfrak{p} + xA \to 0,$$

we have $d(A/\mathfrak{p}) = \max(d(A/\mathfrak{p}), d(A/\mathfrak{p} + xA))$ and that $\chi(A/\mathfrak{p} + xA, I, n)$ has degree less than $d(A/\mathfrak{p})$. Therefore

$$d(A/\mathfrak{p} + xA) < d(A/\mathfrak{p}) \leq d(A).$$

By induction, $\dim(A/\mathfrak{p} + xA) \leq d(A/\mathfrak{p} + xA)$ and thus $\ell - 1 \leq d(A/\mathfrak{p} + xA) \leq d(A) - 1$. This holds for any chain of ideals, so $\dim A \leq d(A)$. □

Corollary 3.2.6. *If A is Noetherian and $\mathfrak{p} \in \operatorname{Spec} A$, then $\mathfrak{ht}(\mathfrak{p}) < \infty$.*

Proof. $\operatorname{ht}(\mathfrak{p}) = \dim A_{\mathfrak{p}} < \infty$ by the previous lemma. $\square$

Lemma 3.2.7. *Let A be a Noetherian semilocal ring and M a finite A-module. Choose $x \in \operatorname{Rad}(A)$. Then $d(M) \geq d(M/xM) \geq d(M) - 1$.*

Proof. Let $I \subset A$ be an ideal of definition such that $x \in I$. Then

$$\chi(M/xM, I, n) = \ell(M/xM + I^n M) = \ell(M/I^n M) - \ell\left(\frac{xM + I^n M}{I^n M}\right).$$

Then because $x \in I$, we see that $I^{n-1}M \subset (I^n M : x)$, so

$$\ell\left(\frac{xM + i^n M}{I^n M}\right) \leq \ell(M/I^{n-1}M).$$

This implies that $\chi(M/xM, I, n) \geq \chi(M, I, m) - \chi(M, I, n-1)$, so $d(M/xM) \geq d(M) - 1$. $\square$

Lemma 3.2.8. *Let A and M be as before. Let $r = \dim M > 0$. Then there exists $x_1, \ldots, x_r \in \operatorname{Rad}(A)$ such that $\ell(M/x_1 M + \cdots + x_r M) < \infty$.*

Proof. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ be the minimal prime ideals containing $\operatorname{Ann}_A(M)$ such that $\dim(A/\mathfrak{p}_i) = r$. Because $r > 0$, then the $\mathfrak{p}_i$ are not maximal and therefore $\operatorname{Rad}(A) \not\subset \mathfrak{p}_i$. In particular, it is not contained in $\bigcup \mathfrak{p}_i$. Choose $x_1 \in \operatorname{Rad}(A) \setminus \bigcup \mathfrak{p}_i$.

If $\mathfrak{q} \supset \operatorname{Ann}(M/x_1 X) \supset \operatorname{Ann}(M) + x_1 A$ is prime and minimal, then $\mathfrak{q} \notin \mathfrak{p}_i$ because $x_1 \notin \mathfrak{p}_i$. This implies $\dim A/\mathfrak{q} \leq r - 1$. By induction, we can then find $x_2, \ldots, x_r$ such that

$$\ell(\overline{M}/x_2\overline{M} + \cdots + x_r\overline{M}) < \infty,$$

where $\overline{M} = M/x_1 M$. $\square$

Theorem 3.2.9. *Let A be semilocal and M a finite A-module. Then $d(M) = \dim M$ is the smallest integer r such that there exists $x_1, \ldots, x_r \in \operatorname{Rad}(A)$ such that $\ell(M/x_1 M + \cdots + x_r M) < \infty$.*

Proof. Choose $x_1, \ldots, x_r \in \mathfrak{m} = \operatorname{Rad}(A)$. If $\ell(M/x_1 M + \cdots + x_r M) < \infty$, then we know that $d(M/x_1 M + \cdots | x_r M) \geq d(M) - r$. Then because $M/x_1 M + \cdots + x_r M$ has finite length, its dimsnion is zero and thus $r \geq d(M)$. Then let r_0 be the smallest such integer. By the previous lemma, we deduce that $\dim M \geq r_0 \geq d(M)$.

We will show that $d(M) \geq \dim M$. Consider a sequence

$$M = M_0 \supset M_1 \supset \cdots \supset M_{n+1} = 0$$

such that $M_i/M_{i+1} \cong A/\mathfrak{p}_i$ for some prime ideals $\mathfrak{p}_i$. Then $\operatorname{Ass}(M) \subset \{\mathfrak{p}_0, \ldots, \mathfrak{p}_n\} \subset \operatorname{Supp} M$ are the minimal primes containing $\operatorname{Ann}_A(M)$, so we see that

$$d(M) = \max\{d(A.\mathfrak{p}_i)\} \geq \max\{\dim(A/\mathfrak{p}_i)\} = \dim(A/\operatorname{Ann}_A M). \qquad \square$$

Remark 3.2.10. If $M = A$, then $d(M)$ is the smallest integer r such that there exists $x_1, \ldots, x_r \in \operatorname{Rad}(A)$ such that $(x_1, \ldots, x_r)$ is an ideal of definition.

Corollary 3.2.11. *If A is Noetherian and $I = (x_1, \ldots, x_r) \subset A$, then any minimal prime ideal $\mathfrak{p}$ containing I has height at most r. In particular, $\operatorname{ht}(I) \leq r$.*

Proof. First, note that $A_\mathfrak{p}/IA_\mathfrak{p}$ is Artinian because the image of $\mathfrak{p}A_\mathfrak{p}$ is both maximal and minimal. Then $\ell(A_\mathfrak{p}/x_1A_\mathfrak{p} + \cdots + x_rA_\mathfrak{p}) < \infty$ and thus $\mathrm{ht}(\mathfrak{p}) = \dim(A_\mathfrak{p}) \leq r$. $\square$

Now let M be a finitely generated A-module. Define $\widehat{M} = \lim_{\leftarrow} M/I^nM$ for an ideal of definition I. We call $\widehat{M}$ the I-adic completion of M.

Corollary 3.2.12. $\dim \widehat{M} = \dim M$.

Proof. We know that $\widehat{M}/I^n\widehat{M} = M/I^nM$. Thus the two modules have the same Hilbert-Samuel polynomial. $\square$

Corollary 3.2.13. *Let A be Noetherian with $\mathfrak{p} \in \operatorname{Spec} A$. Let n be an integer. The following are equivalent:*

1. $\mathrm{ht}(\mathfrak{p}) \leq n$.
2. *There exits I generated by n elements such that $\mathfrak{p}$ is minimal in $V(I)$.*

Proof. **1 implies 2** Suppose that $\mathrm{ht}(\mathfrak{p}) \leq n$. Then there exists an ideal of definition J of $A_\mathfrak{p}$ generated by n elements. If $J = (\frac{x_1}{s}, \ldots, \frac{x_n}{s})$, then $I = (x_1, \ldots, x_n) \subset \mathfrak{p}$ and $\mathfrak{p}$ is minimal containing I.

2 implies 1 Let $I = (x_1, \ldots, x_n)$ such that $\mathfrak{p} \supset I$ is minimal. Therefore $A_\mathfrak{p}/IA_\mathfrak{p}$ is Artinian, so it has finite length. Thus $\dim A_\mathfrak{p} \leq n$, as desired. $\square$

Definition 3.2.14. A *system of parameters* for M is a set of elements $x_1, \ldots, x_s \in \mathrm{Rad}(A)$ such that

- $\ell(M/x_1M + \cdots + x_sM) < \infty$;
- $s = \dim M$.

Proposition 3.2.15. *Let $x_1, \ldots, x_r \in \mathrm{Rad}(A)$. Then $\dim(M/(x_1, \ldots, x_i)M) \geq \dim M - r$ and we have equality if and only if $x_1, \ldots, x_r$ belong to a system of parameters for M.*

Proof. By induction $d(M/xM) \geq d(M) - 1$ for any $x \in \mathrm{Rad}(A)$. Then we know that

$$d(M/(x_1, \ldots, x_r)M) \geq d(M) - r = \dim M - r.$$

Then assume that we have equality. Let $y_1, \ldots, y_p$ be a system of parameters for $M/(x_1, \ldots, x_r)M$. Then $\dim(M/(x_1, \ldots, x_r)M) = p = \dim M - r$. However, if $\overline{M} = M/(x_1, \ldots, x_r)$, then

$$\ell(\overline{M}/(y_1, \ldots, y_p)\overline{M}) = \ell(M/(y_1, \ldots, y_p, x_1, \ldots, x_r)M) < \infty$$

and thus $y_1, \ldots, y_p, x_1, \ldots, x_r$ is a system of parameters for M.

Conversely suppose that $x_1, \ldots, x_r, y_1, \ldots, y_p$ is a system of parameters for M. Then

$$\dim(M/(x_1, \ldots, x_r)M) \geq \dim M - r = p,$$

but we have equality because

$$0 = d(M/x_1, \ldots, x_r, y_1, \ldots, y_p) \geq d(M/(x_1, \ldots, x_r)M) - p,$$

and so $p \geq d(M/(x_1, \ldots, x_r)M)$. $\square$

Now we turn to the case of local Noetherian rings A with maximal ideal $\mathfrak{m}$ and residue field k. Then if $d = \dim A$, any ideal of definition has at least d generators. Then let $x_1, \ldots, x_d \in \mathfrak{m}$ such that $\ell(A/(x_1, \ldots, x_d)) < \infty$. Thus $I = (x_1, \ldots, x_d)$ is an ideal of definition and $(x_1, \ldots, x_d)$ is a system of parameters of A.

Definition 3.2.16. A local ring A is a *regular local ring* if there is a system of parameters generating the maximal ideal of A. Such a system is called a *regular system of parameters*.

Note that $\dim A \leq \dim_k \mathfrak{m}/\mathfrak{m}^2$ and that A is regular if and only if $\dim A = \dim_k \mathfrak{m}/\mathfrak{m}^2$.

Proposition 3.2.17. *Let $(A, \mathfrak{m}, k)$ be a local Noetherian ring. Let $(x_1, \ldots, x_d)$ be a system of parameters of A. Then $\dim(A/(x_1, \ldots, x_i)A) = d - i$ and the image of $(x_{i+1}, \ldots, x_d)$ in $A/(x_1, \ldots, x_i)A$ is a system of parameters of this quotient.*

3.3 Dimension in the Relative Setting

Consider a morphism $A \xrightarrow{\varphi} B$. We have the pullback $\varphi^*\colon \operatorname{Spec} B \to \operatorname{Spec} A$. For $\mathfrak{p} \in \operatorname{Spec} A$, we have a bijection between $(\varphi^*)^{-1}(\mathfrak{p})$ and $\operatorname{Spec}(B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p})$. This latter ring is isomorphic to $B \otimes k(\mathfrak{p})$, where $k(\mathfrak{p})$ is the residue field of $A_\mathfrak{p}$.

Theorem 3.3.1. *Let $\mathfrak{P} \in \operatorname{Spec} B$ lie over $\mathfrak{p}$. Then*

1. $\operatorname{ht}(\mathfrak{P}) \leq \operatorname{ht}(\mathfrak{p}) + \operatorname{ht}(\mathfrak{P}/\mathfrak{p}\mathfrak{P})$. *Equivalently,* $\dim B_\mathfrak{P} \leq \dim A_\mathfrak{p} + \dim(B_\mathfrak{P}/\mathfrak{p}B_\mathfrak{P})$.
2. *Equality holds is equivalent to the going-down property for φ and in particular if φ is flat.*
3. *If φ^* is surjective and the going-down property holds, then* $\dim B \geq \dim A$ *and* $\operatorname{ht}(I) = \operatorname{ht}(IB)$ *for* $I \subset A$.

Proof.

1. Set $A = A_\mathfrak{p}, B = B_\mathfrak{P}$. We need to prove that $\dim B \leq \dim A + \dim B/\mathfrak{p}B$, where $\mathfrak{p}$ is the maximal ideal of A. Write $r = \dim A$ and let $x_1, \ldots, x_r$ be a system of parameters for A. Then $I = (x_1, \ldots, x_r)$ is an ideal of definition, so $\mathfrak{p}^n \subset I \subset \mathfrak{p}$ for some n. Thus $\mathfrak{p}^n B \subset IB \subset \mathfrak{p}B$ and all of these ideals have the same nilradical. Therefore
$$\dim B/OB = \dim B/\mathfrak{p}^n B = \dim B/\mathfrak{p}B = s$$
for some integer s. If $y_1, \ldots, y_s$ is a system of paramaters for B/IB, then $x_1, \ldots, x_r, y_1, \ldots, y_s$ generate an ideal of definition for B, so $r + s \geq \dim B$.

2. Let $\mathfrak{P} = \mathfrak{P}_0 \supsetneq \mathfrak{P}_1 \supsetneq \cdots \supsetneq \mathfrak{P}_s$ be a chain of ideals of $B/\mathfrak{p}B$ of length $s = \dim B/\mathfrak{p}B$. Then for $i = 0, \ldots, s$ we know $\mathfrak{p} \subset \varphi^*(\mathfrak{P}_i)$ and thus $\varphi^*(\mathfrak{P}_i) = \mathfrak{p}$ for all i. Now by the Going Down property we can find
$$\mathfrak{P}_s \supsetneq \cdots \supsetneq \mathfrak{P}_{r+s}$$
such that $\mathfrak{p}_i = \varphi^{-1}(\mathfrak{P}_{s+i})$. Thus we have
$$\mathfrak{p} = \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_r$$
where $r = \dim A$. This gives us the chain
$$\mathfrak{P}_0 \supsetneq \cdots \supsetneq \mathfrak{P}_{r+s}$$
and thus $\dim B \geq r + s$.

3. The first inequality follows from 2. Note that $\dim B = \dim A + \dim(B/\mathfrak{p}B) \geq \dim A$.

   To prove the equality, let $\mathfrak{P} \in V(IB)$ be minimal such that $\operatorname{ht}(\mathfrak{P}) = \operatorname{ht}(IB)$. Let $\mathfrak{p} = \varphi^*(\mathfrak{P})$. Then $\mathfrak{p} \supset I$ and $\mathfrak{P}/\mathfrak{p}B$ is minimal, so $\operatorname{ht}(\mathfrak{P}/\mathfrak{p}B) = 0$. This tells us that $\dim B_\mathfrak{P} = \dim A_\mathfrak{p}$ and thus $\operatorname{ht}(\mathfrak{P}) = \operatorname{ht}(\mathfrak{p})$. Thus $\operatorname{ht}(\mathfrak{P}) \geq \operatorname{ht}(I)$.

Conversely, let $\mathfrak{p} \supset I$ be minimal with $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(I)$. Let $\mathfrak{P} \in \operatorname{Spec} B$ such that $\varphi^*(\mathfrak{P}) = \mathfrak{p}$. Then $\mathfrak{P} \supset \mathfrak{p}B \supset IB$ and so we may suppose it is minimal for this property. Then we see that

$$\mathrm{ht}(IB) \leq \mathrm{ht}(\mathfrak{P}) = \mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(I)$$

as desired. □

Corollary 3.3.2. *Let $B \supset A$ be Noetherian rings such that B is inegral over A.*

1. $\dim A = \dim B$*;*
2. *For all $\mathfrak{P} \in \operatorname{Spec} B$, $\mathrm{ht}(\mathfrak{P}) \leq \mathrm{ht}(\mathfrak{P} \cap A)$.*
3. *If the going-down property holds, then for any ideal $J \subset B$, have $\mathrm{ht}(J) = \mathrm{ht}(J \cap A)$.*

Proof. THe proof of this is left as an exercise to the reader. □

Exercise 3.3.3. Let $A \xrightarrow{\phi} B$ be a morphism of rings and assume that going-down holds for ϕ. Let $\mathfrak{p} \supset \mathfrak{q}$ be prime ideals of A. Prove that $\dim(B \otimes k(\mathfrak{p})) \geq \dim(B \otimes k(\mathfrak{q}))$.

Now we will consider finitely generated extensions of rings. Here B will be a finitely-generated A-algebra.

Theorem 3.3.4. *Let A be Noetherian. Then $\dim A[X] = \dim A + 1$.*

Proof. Let $\mathfrak{p} \in \operatorname{Spec} A$ and let $\mathfrak{P} \in \operatorname{Spec} B$ such that $\mathfrak{P} \cap A = \mathfrak{p}$. Choose $\mathfrak{P}$ to be maximal for this property. We will show that $\mathrm{ht}(\mathfrak{P}/\mathfrak{p}B) = 1$. After localization at $\mathfrak{p}$, we may assume that $\mathfrak{p}$ is maximal and A is local. Then $B/\mathfrak{p}B = A/\mathfrak{p}[X]$, and $A/\mathfrak{p}$ is a field. Thus $B/\mathfrak{p}B$ is a PID, so $\mathfrak{P}/\mathfrak{p}B$ is a nonzero principal ideal, so it must have height exactly equal to 1.

Previous we have seen that because B is flat, $\dim B_{\mathfrak{P}} = \dim A_{\mathfrak{p}} + 1$, and thus $\mathrm{ht}\mathfrak{P} = \mathrm{ht}(\mathfrak{p}) + 1$, and we obtain the desired result. □

Corollary 3.3.5.

1. $\dim A[x_1, \ldots, x_m] = \dim A + m$.
2. *If k is a field, then $\dim k[x_1, \ldots, x_m] = m$. Moreover, $\mathrm{ht}((x_1, \ldots, x_i)) = i$.*

Proof. We only need to prove the part about the height of $(x_1, \ldots, x_i)$. Then we have

$$0 \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, \ldots, x_i) \subsetneq \cdots \subsetneq (x_1, \ldots, x_n).$$

Then clearly $\mathrm{ht}((x_1, \ldots, x_i)) \geq i$ and the inequality cannot be strict because otherwise $(x_1, \ldots, x_n)$ has height strictly larger than n. □

Exercise 3.3.6. Let A be Noetherian, $I \subset A$, and $I' \subset A[X]$. Suppose $I' = I[X]$. Show that $\mathrm{ht}(I') = \mathrm{ht}(I)$.

Theorem 3.3.7 (Noether Normalization)**.** *Let A be a finitely generated k-algebra over a field k. Let $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \cdots \subsetneq \mathfrak{a}_p$ be a chain of prime ideals of A. Then there exist elements $x_1, \ldots, x_m \in A$ algebraically independent such that:*

1. *A is integral over $B = k[x_1, \ldots, x_m]$;*
2. *For all $i = 1, \ldots, p$, there exists an integer $h(i) \geq 0$ such that $\mathfrak{a}_i \cap B = (x_1, x_2, \ldots, x_{h(i)})$. In particular, $\mathrm{ht}(\mathfrak{a}_i) = h(i)$.*

Remark 3.3.8. Recall that $x_1, \dots, x_m$ are algebraically independent means that the map $k[X_1, \dots, X_m] \to A$ sending $X_i \mapsto x_i$ is injective.

Proof of Theorem. We will treat the case where $A = k[y_1, \dots, y_m]$ because any finitely generated algebra over k which is an integral domain is integral over such a ring. We will prove the result by induction on m and p. The case when $m = 1$ is clear because $k[y_1]$ is a PID.

We will assume the result is true for $m-1$. Now we will form an induction on p. In the case $p = 1$, first assume that $\mathfrak{a}_1 = (x_1)$, where $x_1 \notin k$. Then $x_1 = f(y_1, \dots, y_m) \in k[y_1, \dots, y_m]$. For $i = 2, \dots, m$ we will introduce $x_i = y_i - y_1^{r_i}$ for some integer r_i. We want to choose the r_i such that y_1 is integral over $k[x_1, \dots, x_m]$. Writing

$$\begin{aligned} x_1 &= f(y_1, \dots, y_m) \\ &= \sum_{\underline{p}} a_{\underline{p}} y^{\underline{p}} \\ &= \sum_{\underline{p}} a_{\underline{p}} y_1^{p_1} (x_2 + y_1^{r_2})^{p_2} \cdots (x_m + y_1^{r_m})^{p_m}, \end{aligned}$$

we see that $f(\underline{p}) = p_1 + r_2 p_2 + \cdots r_m p_m$ is the maximal degree of y_1 in this expression. Then it is possible to choose $r_2, \dots, r_m$ such that $f(\underline{p})$ are all distinct, for example $r_i = k^i$ for $k > \max\{p_i\}$, where the max is taken over all p_i that occur in the polynomial.

Then choosing the $\underline{p}$ for which $f(\underline{p})$ is maximal, we can write

$$x_1 = a_{\underline{p}} y_1^{f(\underline{p})} + \sum_{j \le f(\underline{p})} Q_j(\underline{x}) y_1^j.$$

Thus y_1 is integral over $k[x_1, \dots, x_m]$, so $y_i = x_i + y_1^{r_i}$ is integral over $k[x_1, \dots, x_m]$. Therefore A is integral over $k[x_1, \dots, x_m]$. Finally, $x_1, \dots, x_m$ are algebraically independent because otherwise the transcendance degree of $\mathrm{Frac}(A)$ is smaller than m. We now show that $\mathfrak{a}_1 \cap B = (x_1)$. If $y \in \mathfrak{a}_1 \cap B$, then write $y = b' x_1$ for some $b' \in A$. But then $b' \in A \cap \mathrm{Frac}(B)$, so because B is integrally closed, $b' \in B$ and thus $y \in B x_1$.

For the general case, suppose $\mathfrak{a}_1$ is generated by more than one element. Choose $x_1 \in \mathfrak{a}_1 \setminus k$ and choose $t_2, \dots, t_m$ such that A is integral over $C = k[x_1, t_2, \dots, t_m]$ and $x_1 A \cap C = C x_1$. By the induction hypothesis on m, there exist $x_2, \dots, x_m$ such that $k[t_2, \dots, t_m]$ is integral over $k[x_1, \dots, x_m]$ and $\mathfrak{a}_1 \cap k[t_1, \dots, t_m] \cap k[x_2, \dots, x_m] = (x_2, \dots, x_h)$. To see this, choose $z \in \mathfrak{a}_1 \cap k[x_1, \dots, x_h]$. Then there exist $h_j \in k[x_2, \dots, x_m]$ such that

$$z = \sum_{j=1}^{d} h_j x_1^j$$

bceause $x_1 \in \mathfrak{a}_1 \cap k[x_1, \dots, x_m]$. Thus $h_0 \in \mathfrak{a}_1 \cap k[x_1, \dots, x_m] = (x_2, \dots, x_h)$ and thus $z \in (x_1, \dots, x_h)$. This finishes the case $p = 1$.

Now we complete the induction on p. Suppose we have a chain of prime ideals $\mathfrak{a}_1 \subsetneq \cdots \subsetneq \mathfrak{a}_p$ in A. Then we choose $t_1, \dots, t_m$ such that

- A is integral over $k[t_1, \dots, t_m]$
- $\mathfrak{a}_i \cap k[t_1, \dots, t_m] = (t_1, \dots, t_{h(i)})$ for $i \le p-1$.

Now we apply the case $p = 1$ to the ideal $\mathfrak{a}_p \cap k[t_{r+1}, \dots, t_m]$ where $r = h(p-1)$. Thus there exist $x_{r+1}, \dots, x_m$ such that $k[t_{r+1}, \dots, t_m]$ is integral over $k[x_1, \dots, x_m]$ and $\mathfrak{a}_p \cap k[x_{r+1} \dots, x_m] = (x_{r+1}, \dots, x_h)$.

First, it is clear that A is integral over $k[t_1, \ldots, t_r, x_{r+1}, \ldots, x_m]$. If we set $x_i = t_i$ for $i \leq i$, then we will show that
$$\mathfrak{a}_p \cap k[x_1, \ldots, x_m] = (x_1, \ldots, x_h).$$
One direction is obvious from the inductive hypothesis. In the other direction, if we write $y = \sum a_{\underline{h}} \underline{x}^{\underline{h}}$, then because $x_1, \ldots, x_r \in \mathfrak{a}_{p-1} \in \mathfrak{a}_{p-1} \cap k[x_1, \ldots, x_m]$, we see that
$$a_{\underline{0}} \in \mathfrak{a}_p \cap k[x_{r+1}, \ldots, x_m] = (x_{r+1}, \ldots, x_h).$$
Thus $y \in (x_1, \ldots, x_h)$, as desired. □

Corollary 3.3.9. *Let A be an integral domain of finite type over a field k. Then* $\dim A$ *equals the transcendence degree of the fraction field of A.*

Proof. There exist $x_1, \ldots, x_m$ such that A is integral over $k[x_1, \ldots, x_m]$. Then $\operatorname{Frac}(A)$ is algebraic over $k(x_1, \ldots, x_m)$. On the other hand, we know that $\dim A = m$, which is the transcendance degree of $k(x_1, \ldots, x_m)$. □

Corollary 3.3.10 (Nullstellensatz)**.** *Let A be an algebra of finite type over a field k. Then for any maximal ideal $\mathfrak{m} \subset A$, $A/\mathfrak{m}$ is algebraic over k.*

Proof. Note that $\dim A/\mathfrak{m} = 0$, but this is also the transcendence degree over k by the previous corollary. □

Proposition 3.3.11. *Let A be an integral domain of finite type over a field k. Then for any prime ideal $\mathfrak{p} \in \operatorname{Spec} A$, we have* $\operatorname{ht}(\mathfrak{p}) + \dim A/\mathfrak{p} = \dim A$.

Proof. Let $\mathfrak{p} \in \operatorname{Spec} A$ and $h$be its height. Then by Noether normalization, there exist $x_1, \ldots, x_m$, where $m = \dim A$, such that A is integral over $A' = k[x_1, \ldots, x_m]$ and $\mathfrak{p}' = \mathfrak{p} \cap A' = (x_1, \ldots, x_h)$. Then we know that $A'/\mathfrak{p}' \cong k[x_{h+1}, \ldots, x_n]$. Because $A/\mathfrak{p}$ is integral over $A'/\mathfrak{p}'$, we see that $\dim A/\mathfrak{p} = \dim A'/\mathfrak{p}' = n - h$. But then $\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\mathfrak{p}') = h$ because A' is integrally closed and A is integral over A'. Therefore,
$$\operatorname{ht}(\mathfrak{p}) + \dim A/\mathfrak{p} = h + n - h = n = \dim A.$$
□

Remark 3.3.12. Let A be a finitely generated k-algebra. Then for any maximal ideal $\mathfrak{m} \subset A$, we know that $A/\mathfrak{m}$ is an algebraic extension of k. Therefore we have a correspondence
$$\left\{ \begin{matrix} \text{Maximal ideals} \\ \text{of Spec } A \end{matrix} \right\} \longrightarrow \left\{ \begin{matrix} \text{Galois orbits of points in } \overline{k}^n \\ \text{satisfying certain algebraic equations} \end{matrix} \right\}.$$
In addition, any prime ideal $\mathfrak{p}$ defines a subvariety $\operatorname{Spec} A/\mathfrak{p} = V(\mathfrak{p})$ of $\operatorname{Spec} A$.

Proposition 3.3.13. *Let A, A' be two finitely-generated k-algebras that are domains. Then for any minimal prime ideal $\mathfrak{p} \subset A \otimes_k A'$, we have* $\dim A \otimes_k A'/\mathfrak{p} = \dim A + \dim A'$.

Proof. Choose B, B' polynomials over k such that A (resp A') is integral over B (resp B'). Then write $d, d' = \dim A, \dim A'$. Then $A \otimes A'$ is torsion free over $B \otimes B'$. Then because $\mathfrak{p} \subset \operatorname{Spec}(A \otimes A')$ is minimal, we see that $B \otimes B' \cap \mathfrak{p} = 0$. Therefore $A \otimes A'/\mathfrak{p}$ is integral over $B \otimes B'$ and thus the desired result follows using integrality. □

Remark 3.3.14. We can think of $\operatorname{Spec} A \otimes A'$ as the product $\operatorname{Spec} A \times \operatorname{Spec} A'$. The proposition says that irreducible components of the product variety have the expected dimension.

Proposition 3.3.15 (Hilbert's Nullstellensatz). *Let k be a field, A be a finitely-generated k-algebra and $I \subsetneq A$ be a proper ideal. Then $\sqrt{I} = \bigcap_{\substack{\mathfrak{m} \supset I \\ \mathfrak{m} \text{ maximal}}} \mathfrak{m}$.*

Proof. One direction is obvious because $\sqrt{I}$ is the intersection of all prime ideals containing I. Let $a \in J = \bigcap \mathfrak{m} \setminus \sqrt{I}$. Then $S = \{1, a, a^2, \ldots\} \cap I = \emptyset$ and thus $S^{-1}I \subset S^{-1}A$ is a proper ideal. Thus there exists a maximal ideal of $S^{-1}A$ such that $S^{-1}I \subset \mathfrak{m}_0$. Because $S^{-1}A$ is a finitely generated k-algebra, we have

$$\dim(S^{-1}A/\mathfrak{m}_0) = \operatorname{trdeg}_k S^{-1A/\mathfrak{m}_0} = 0.$$

Then writing $\mathfrak{m} = \mathfrak{m}_0 \cap A$, we see that $k \subset A/\mathfrak{m} \subset S^{-1}A/\mathfrak{m}_0$ and thus $\dim A/\mathfrak{m} = 0$ and therefore $\mathfrak{m} \supset I$ is maximal. However, $a \notin \mathfrak{m}$ by hypothesis, which gives us a contradiction. $\square$

3.4 Rings of Dimension 1

Definition 3.4.1. A local ring A is called a *discrete valuation ring* if it is a principal ideal domain and has a nonzero prime ideal.

This prime ideal is naturally maximal becuase if $\mathfrak{p} \subset \mathfrak{m} \subset A$ given by $(a) \subset (b)$, then we know $a = bs$ for some $s \in A$, but then $s \in \mathfrak{p}$, so $s = as'$ and thus $a = bas'$, so $bs' = 1$. In particular, $\dim A = 1$.

Definition 3.4.2. A *discrete valuation* on A is a surjective function $v \colon A^* \to \mathbb{Z}$ such that

- $v(xy) = v(x) + v(y)$;
- $v(x + y) \geq \min\{v(x), v(y)\}$.

We define $v(0) = \infty$.

If A is a DVR, then choose $x \neq 0$. We define $v(x) = \sup\{n \geq 0 \mid x \in (\pi^n)\}$, where π generates the maximal ideal of A. Then $v(x)$ is well-defined because $\bigcap_0(\pi^n) = 0$ by the Krull intersection theorem. We can extend this valuation to $K = \operatorname{Frac} A$ by $v(x/y) = v(x) - v(y)$.

Proposition 3.4.3. *If K is a field and $v \colon K^* \to \mathbb{Z}$ is a valuation, then $A = \{x \in K \mid v(x) \geq 0\} \cup \{0\}$ is a discrete valuation ring.*

Proof of this is left as an exercise.

Example 3.4.4. Consider the ring $\mathbb{Z}_{(p)}$ where p is a prime number. Then for any $\frac{x}{y}$ with y coprime to p, define $v_p\left(\frac{x}{y}\right)$ to be the maximal power of p dividing x.

Now let k be a field and let $k[[T]]$ be the ring of formal power series in T. Then any series $a_0 + a_1T + \cdots$ is invertible iff $a_0 \neq 0$, and thus any element is a product of T^n and a unit for some n. Thus $v(F)$ is the degree of the first monomial with nonzero coefficient.

Proposition 3.4.5. *Let A be a ring. Then the following are equivalent:*

1. *A is a DVR.*
2. *A is a local noetherian ring and $\mathfrak{m}_A$ is generated by an element π which is not nilpotent.*

Proof. One direction is clear. If A is a DVR, then it is a domain, and thus the generator of the prime ideal is not nilpotent.

In the other direction, suppose $\mathfrak{m} = (\pi)$. Then by the Krull intersection theorem, $\bigcap_n (\pi^n) = 0$. Then for $0 \neq x \in A$, there exists a maximal n such that $x \in (\pi^n)$, so $x = \pi^n u$ for some $u \in A^\times$. But then for $y \in A, y \neq 0$, write $y = \pi^m v$ for $v \in A^\times$. Thus $xy = \pi^{m+n} uv \neq 0$ because π is not nilpotent. Therefore A is a domain and thus is a DVR. □

Proposition 3.4.6. *Let A be a local Noetherian ring. Then A is a DVR if and only if*

1. *A is integrally closed;*

2. *A has a unique nonzero prime ideal.*

Proof. One direction is clear. In the other direction, assume A is integrally closed and has a unique nonzero prime. First, we note that A must be local and $\mathfrak{m} \neq 0$. Then if we write

$$\mathfrak{m}' = \{x \in K \mid x\mathfrak{m} \subset A\} \supset A,$$

this is an A-module. If we write $y \in \mathfrak{m}$, then $y\mathfrak{m}' \subset A$ and thus $\mathfrak{m}' \subset Ay^{-1}$. This implies that $\mathfrak{m}'$ is finitely generated. Then we have $\mathfrak{m} \subset \mathfrak{m}\mathfrak{m}' \subset A$. We will show that this cannot equal $\mathfrak{m}$ by contradiction.

Let $x \in \mathfrak{m}'$. Then $x\mathfrak{m} \subset \mathfrak{m}$ and thus x is integral over A. Because A is integrally closed, $x \in A$. Thus $\mathfrak{m}' = A$. Now we set $S = \{1, x, x^2, \dots\}$. Then $S^{-1}A = K$ because it has no nonzero prime ideals. If we choose $z \in A \setminus 0$, then we can write $\frac{1}{z} = \frac{y}{x^n}$ for some $n \geq 0$. This tells us that $x^n \in (z)$. Because $\mathfrak{m}$ is finitely generated, we see that $\mathfrak{m}^N \subset (z)$. Then let N_0 be the smallestt integer such that $\mathfrak{m}^{N_0} \subset (z) \subset \mathfrak{m}$ and let $y \in \mathfrak{m}^{N_0 - 1} \setminus (z)$. Then we have $\mathfrak{m}y \subset \mathfrak{m}^{N_0} \subset (z)$ and thus $\frac{y}{z} \in \mathfrak{m}'$. This implies that $\mathfrak{m}' \supsetneq A$ and thus $\mathfrak{m}\mathfrak{m}' = A$. Therefore we can write

$$1 = \sum x_i y_i^{-1}$$

where $x_i \in \mathfrak{m}, y_i \in \mathfrak{m}'$. Therefore there exists i such that $x_i y_i^{-1} \notin \mathfrak{m}$ and thus $y_i^{-1}\mathfrak{m} = A$. Therefore $\mathfrak{m} = (y_i)$ is a principal ideal, so A is a DVR. □

Proposition 3.4.7. *Let A be a Noetherian domain. The following are equivalent:*

1. *For all $0 \neq \mathfrak{p} \in \operatorname{Spec} A$, the localization $A_\mathfrak{p}$ is a discrete valuation ring.*

2. *A is integrally closed and of dimension 1.*

Proof. **1 implies 2:** Let $x \in K$ be integral over A. But then $x \in A_\mathfrak{p}$ for all $\mathfrak{p} \neq 0$ and thus $x \in \bigcap_{\mathfrak{p} \neq 0} A_\mathfrak{p} = A$. Being of dimension 1 is easy. If $0 \neq \mathfrak{p} \subset \mathfrak{m} \subset A$, we localize at $\mathfrak{m}$ and see that $\mathfrak{p}A_\mathfrak{m} = \mathfrak{m}A_\mathfrak{m}$, so $\mathfrak{p} = \mathfrak{m}$.

2 implies 1: For all $\mathfrak{p}$, we know that $A_\mathfrak{p}$ is integrally closed. Because it has dimension 1, it must be a DVR.

□

Definition 3.4.8. A ring A is called a *Dedekind domain* if it is a domain satisfying the properties of the previous proposition.

Example 3.4.9. $\mathbb{Z}$ is a Dedekind domain. It is clearly a domain, having dimension 1 follows from being a PID, and being integrally closed is obvious. More generally, any principal ideal domain is a Dedekind domain.

Example 3.4.10. Let A be a Dedekind domain and $K = \mathrm{Frac}(A)$. Then let L/K be a finite extension and B be the integral closure of A in L. Then B is a Dedekind domain. In particular, if K is a number field, then its ring of integers $\mathcal{O}_K$ is a Dedekind domain.

Here is another example of this. Let k be a field and $A = k[x], k = k(X)$. Then if L/K is a field extension and B is the integral closure of A in L, then $\mathrm{Spec}\, B \to \mathrm{Spec}\, A$ is a smooth affine curve with a map to $\mathbb{A}^1$.

Remark 3.4.11. All smooth curves can be obtained in this way (of taking the integral closure of some ring). Also, normalization resolves all singluarities of curves.

Definition 3.4.12. A *fractional ideal* $\mathfrak{a} \subset K = \mathrm{Frac}(A)$ is an A-submodule of finite type.

Note that for $\mathfrak{a}, \mathfrak{b}$ nonzero fractional ideals, then $\mathfrak{a} \cdot \mathfrak{b}$ is a fractional ideal.

Proposition 3.4.13. *If A is a Dedekind domain, then the set of nonzero fractional ideals form an abelian group.*

Proof. It is easy to see that the multiplication is associative and commutative. Now we need to show that inverses exist. For $\mathfrak{a} \subset K$ a fractional ideal, we need to find another fractional ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = A$. Set

$$\mathfrak{b} = \mathfrak{a}^{-1} := \{x \in K \mid x \cdot \mathfrak{a} \subset A\}.$$

Clearly we know that for $0 \neq x \in \mathfrak{a}$, we have $\mathfrak{a}^{=1} \subset x^{-1}A$ and thus $\mathfrak{a}^{-1}$ is of finite type. Then for any prime ideal $\mathfrak{p}$ we know that $\mathfrak{a}_\mathfrak{p} \cdot \mathfrak{b}_\mathfrak{p} = (\mathfrak{a} \cdot \mathfrak{b})_\mathfrak{p}$, and thus $\mathfrak{a}_\mathfrak{p}^{-1} = (\mathfrak{a}^{-1})_\mathfrak{p}$. Therefore we have

$$(\mathfrak{a} \cdot \mathfrak{a}^{-1})_\mathfrak{p} = \mathfrak{a}_\mathfrak{p} \cdot \mathfrak{a}_\mathfrak{p}^{-1} = A_\mathfrak{p},$$

and thus $\mathfrak{a} \cdot \mathfrak{a}^{-1} = A$. □

Now if A is a Dedekind domain and $0 \neq \mathfrak{p} \neq \mathfrak{p}' \subset A$, then $\mathfrak{p} + \mathfrak{p}' = A$, so $\mathfrak{p}\mathfrak{p}' = \mathfrak{p} \cap \mathfrak{p}'$. This implies that for any $0 \neq \mathfrak{a} \subset A$ that $\mathfrak{p} \cdot \mathfrak{a} \subsetneq \mathfrak{a}$ because otherwise $\mathfrak{p} = A$.

Lemma 3.4.14. *If $x \in A$ is nonzero, then there are only finitely many maximal ideals $\mathfrak{p}$ such that $x \in \mathfrak{p}$.*

Proof. Let $x \in \mathfrak{p}$. Then $\mathfrak{a}^{-1} \subset x^{-1}A$, so if $x \in \mathfrak{p}_1, \mathfrak{p}_2, \ldots$ for infinitely many maximal ideals, then

$$x \in \mathfrak{p}_1 \supsetneq \mathfrak{p}_1\mathfrak{p}_2 \supset \cdots \subset \prod_{i=1}^{n} \mathfrak{p}_i \supset \cdots$$

is a strictly decreasing infinite chain of ideals containing x. Thus we have

$$\mathfrak{p}_1^{-1} \subset \mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1} \subset \cdots \subset \prod_{i=1}^{n} \mathfrak{p}_i^{-1} \subset \cdots \subset x^{-1}A,$$

but this is impossible because $x^{-1}A$ is Noetherian. □

Remark 3.4.15. For any nonzero ideal $I \subset A$, there are only finitely many prime ideals $\mathfrak{p}$ such that $I \subset \mathfrak{p}$.

Definition 3.4.16. Let $\mathfrak{p}$ be a maximal ideal of A. Then let $v_\mathfrak{p}(I)$ be the $n_\mathfrak{p}$ such that $IA_\mathfrak{p} = \omega_\mathfrak{p}^{n_\mathfrak{p}} A_\mathfrak{p}$. Thus $I \subset \mathfrak{p}^{n_\mathfrak{p}}$ but $I \not\subset \mathfrak{p}^{n_\mathfrak{p}+1}$.

Corollary 3.4.17. *Let I be a fractional ideal of A, where A is a Dede,ind domain. Then*

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)}.$$

Proof. If we denote the product by J, then $I_{\mathfrak{p}} = J_{\mathfrak{p}}$ for all $\mathfrak{p}$ and thus $I = J$. □

Remark 3.4.18. This corollary gives the primary decomposition of an ideal in a Dedekind domain. In number theory, this replaces the prime factorization of an integer.

3.5 Depth

Let A be a ring and M be an A-module. Then for $a_1, \dots, a_r \in A$, write $\underline{a} = (a_1, \dots, a_r) \subset A$.

Definition 3.5.1. The sequence $a_1, \dots, a_r$ is an *M-regular sequence* if it satisfies the following:

1. a_i is not a zero divisor of $M/(a_1, \dots, a_{i-1})M$ for $i = 1, \dots, r$.
2. $\underline{a} \cdot M \subsetneq M$. Therefore we have

$$a_1 M \subsetneq (a_1, a_2)M \subsetneq \cdots \subsetneq (a_1, \dots, a_r)M.$$

Lemma 3.5.2. *Assume that $\underline{a} = (a_1, \dots, a_r)$ is M-regular and let $m_1, \dots, m_r \in M$ such that $\sum_{i=1}^r a_i m_i = 0$. Then $m_i \in \underline{a} \cdot M$ for all i.*

Proof. We will induct on r. If $r = 1$, then $a_1 m_1 = 0$ implies $m_1 = 0$. Now assume $a_1 m_1 + \cdots + a_r m_r = 0$ implies that $a_r \overline{m}_r = 0$ in $M/(a_1, \dots, a_{r-1})M$. Then there exists $n_1, \dots, n_{r-1}$ such that $m_r = a_1 n_1 + \cdots + a_{r-1} n_{r-1}$, and thus

$$\sum_{i=1}^{r-1} a_i (m_i + a_r n_i) = 0.$$

Thus $m_i + a_r n_i \in (a_1, \dots, a_{r-1})M$ and thus $m_i \in (a_1, \dots, a_r)M$. □

Theorem 3.5.3. *Assume that $(a_1, \dots, a_r)$ is an M-regular sequence. Then for any integers $n_1, \dots, n_r$, the sequence $a_1^{n_1}, \dots, a_r^{n_r}$ is M-regular.*

Proof. It is sufficient to prove that $a_1^n, a_2, \dots, a_r$ is an M-regular sequence. We will induct on n. Assume that $a_1^{n-1}, \dots, a_2, a_r$ is M-regular. First, multiplication by a_1^n is clearly injective.

Now if $a_1^n, a_2, \dots, a_{j-1}$ is M-regular, then let $m \in M$ such that

$$a_j m = a_1^n m_1 + \cdots + a_{j-1} m_{j-1}.$$

By induction on n, we can write

$$m = a_1^{n-1} m_1' + \cdots + a_{j-1} m_{j-1}'.$$

Multiplying this by a_j and combining the two equations, we obtain

$$0 = a_1^{n-1}(a_1 m_1 - a_j m_1') + a_2(m_2 - a_j m_2') + \cdots + a_{j-1}(m_{j-1} - a_j m_{j-1}').$$

By the previous lemma, we see that $a_1 m_1 - a_j m_1' \in (a_1^{n-1}, \dots, a_{j-1})M$. Therefore, $a_j m_1' \in (a_1, \dots, a_{j-1})M$, so $m_1' \in (a_1, \dots, a_{j-1})M$. This implies that $m \in (a_1^n, \dots, a_{j-1})M$. □

Definition 3.5.4. The sequence $(a_1, \ldots, a_r)$ is said to be *M-quasi-regular* if one of the following equivalent conditions holds:

- For all $F(x_1, \ldots, x_r) \in M[x_1, \ldots, x_r] = A[x_1, \ldots, x_r] \otimes_A M$ homogeneous of degree n such that $F(a_1, \ldots, a_r) \in I^{n+1}M$, this implies that $F(x_1, \ldots, x_r) \in IM[x_1, \ldots, x_r]$, where $I = (a_1, \ldots, a_r)$.
- If $F(x_1, \ldots, x_r) \in M[x_1, \ldots, x_r]$ is homogeneous and such that $F(a_1, \ldots, a_r) = 0$, then $F \in IM[x_1, \ldots, x_r]$
- The map

$$M/IM[x_1, \ldots, x_r] \to \mathrm{gr}^I M = \bigoplus_{n=0}^{\infty} I^n M / I^{n-1} M, \; F \mapsto F(a_1, \ldots, a_r)$$

 is an isomorphism.

Lemma 3.5.5. *Assume that $(a_1, \ldots, a_r)$ is M-quasi-regular and $x \in A$. Then if $(IM : x) = IM$, then $(I^n M : x) = I^n M$ for all $n \geq 1$.*

Proof. We will induct on n. Suppose that $m \in (I^n M : x)$. Then $xm \in I^n M \subset I^{n-1}$ and thus $m \in I^{n-1}M$. Therefore there exists $g(X_1, \ldots, X_r)$ homogeneous of degree $n-1$ such that $m = g(a_1, \ldots, a_r)$. This implies that $xg(X_1, \ldots, X_r) \in M[\underline{X}]$, so

$$xg(a_1, \ldots, a_r) = xm \in I^n M$$

and then quasi-regularity gives us that $xg(X_1, \ldots, X_r) \in IM[\underline{X}]$. This implies that

$$g(X_1, \ldots, X_r) \in (IM : X)[\underline{X}] = IM[\underline{X}],$$

as desired. ☐

Proposition 3.5.6. *Using the same notation, if $(a_1, \ldots, a_r)$ is M-regular, then it is M-quasi-regular. Conversely, if $(a_1, \ldots, a_r)$ is M-quasi-regular and $M, M/a_1M, \ldots, M/(a_1, \ldots, a_r)M$ are Hausdorff in the I-adic topology, then $(a_1, \ldots, a_r)$ is M-regular.*

Proof. First we prove that regular implies quasi-regular by induction on r. Clearly $r = 1$ is obvious. Suppose $g(x_1) \in M[x]$ is homogeneous of degree n. Then if $g(a_1) \in a_1^{n+1M}$, we have $a_1^{n+1}m' = a_1^n m$ and thus $a_1^n(m - a_1 m') = 0$. By regularity, we have $m = a_1 m'$ and thus $g(x_1) \in a_1 M[x_1]$.

For the inductive step, suppose that $(a_1, \ldots, a_r)$ is regular. Then we know that $(a_1, \ldots, a_{r-1})$ is M-quasi-regular, so now choose $F(x_1, \ldots, x_r) \in M[x_1, \ldots, x_r]$ homogeneous of degree q and such that $F(a_1, \ldots, a_r) = 0$. Then we can write

$$F(x_1, \ldots, x_r) = G(x_1, \ldots, x_{r-1}) + x_r H(x_1, \ldots, x_r)$$

where H is homogeneous of degree $q-1$. Then $G(a_1, \ldots, a_{r-1}) \in I_0^q M$, where $I_0 = (a_1, \ldots, a_{r-1})$. This implies that $a_r H(a_1, \ldots, a_{r-1}) \in I_0^q M$, which implies that $H(a_1, \ldots, a_{r-1}) \in (I_0^q M : a_r)$. Because $a_1, \ldots, a_{r-1}$ is quasi-regular and $a_1, \ldots, a_r$ is regular, we have $(I_0 M : a_r) = I_0 M$. This implies that $(I_0^q M : a_r) = I_0^q M$ and thus $H(a_1, \ldots, a_r) \in I_0^q M$. Then $H(a_1, \ldots, a_r) = h(a_1, \ldots, a_{r-1})$ where h is homogeneous of degree q. Now let

$$g(x_1, \ldots, x_{r-1}) = G(x_1, \ldots, x_{r-1}) + a_r h(x_1, \ldots, x_{r-1}).$$

Because $g(a_1,\ldots,a_{r-1}) = F(a_1,\ldots,a_r) = 0$, we see that $g(x_1,\ldots,x_{r-1}) \in I_0M[x_1,\ldots,x_{r-1}]$ by induction. We conclude that $G \in IM[x_1,\ldots,x_{r-1}]$. Because $H \in I_0M[x_1,\ldots,x_r]$, we have $F \in IM[x_1,\ldots,x_r]$.

Now in the other direction, we will induct on r. If $r = 1$, assume that a_1 is M-quasi-regular. We need to show that $m \mapsto a_1m$ is injective. Suppose that $a_1m = 0$. Then if we consider the polynomial $g_0(x) = m$, we see that $a_1g_0(a_1) = 0$ and thus $x_1g_0(x_1) \in a_1M[x_1]$. This means that $g_0(x_1) \in a_1M[x_1]$ and thus $m \in a_1M$. Then there exists g_1 homogeneous of degree 1 such that $m = g_1(a_1)$. Then we see that $x_1g_1(x_1) \in IM[x_1]$ and thus $g_1(x_1) \in IM[x_1]$, so $m = g_1(a_1) \in I^2M$. Then there exists $g_2 \in M[x_1]$ homogeneous of degree 2 such that $m = g_2(a_1)$. Then $a_1m = a_1g_2(a_1) = 0$, so we deduce that $x_1g_2(x_1) \in IM$ and thus $g_2(x_1) \in IM$. Evaluating at a_1, we see that $m \in I^3M$. In particular, we see that $m \in \bigcap_{n\geq 1} I^nM = 0$, where the last equality uses the Hausdorff condition, and thus $m = 0$.

Now for the induction, we know that a_1 is M-regular. We need to show that $(a_2,\ldots,a_r)$ is M/a_1M-regular. This follows from the inductive hypothesis if we check that $(a_2,\ldots,a_r$ is $M/a_1M =: \overline{M})$-quasi-regular. Choose $F(x_2,\ldots,x_r) \in M[x_2,\ldots,x_r]$ homogeneous of degree n such that $F(a_2,\ldots,a_r) \in a_1M$. Then we can write $F(a_1,\ldots,a_r) = a_1m$, so let i be such that $m \in I^iM$. Then let $G \in M[x_1,\ldots,x_r]$ be homogeneous of degree i and satisfy $m = G(a_1,\ldots,a_r)$. Then the polynomial

$$F(x_2,\ldots,x_r) - x_1G(x_1,\ldots,x_r)$$

vanishes at $(a_1,\ldots,a_r)$. If $i < n-1$, then $a_1G(a_1,\ldots,a_r) = F(a_2,\ldots,a_r) \in I^nM \subset I^{i+2}M$. But then $x_1G(x_1,\ldots,x_r)$ is homogeneous of degree $i+1$ and thus $x_1G(x_1,\ldots,x_r) \in IM[x_1,\ldots,x_r]$ by quasi-regularity. This implies that

$$m = G(a_1,\ldots,a_n) \in I^{i+1}M.$$

We can repeat this until $m \in I^{n-1}M$ and G is of degree $n-1$. Then

$$g(x) = F(x_2,\ldots,x_r) - x_1G(x_1,\ldots,x_r)$$

is homogeneous of degree n and $g(a_1,\ldots,a_r) = 0$. This implies that $g(x_1,\ldots,x_r) \in IM[x_1,\ldots,x_r]$ and thus $F(x_2,\ldots,x_r) \in IM[x_2,\ldots,x_r]$. Thus

$$\overline{F}(x_2,\ldots,x_r) \in I\overline{M}[x_2,\ldots,x_r].$$

Then $(a_2,\ldots,a_r)$ is $\overline{M}$-quasi-regular, so they are $\overline{M}$-regular by induction. $\square$

Remark 3.5.7. For A Noetherian and M of finite type, regular and quasi-regular are equivalent.

Definition 3.5.8. Let $I \subset A$ be an ideal and M and A-module. Then the *I-depth* of M is the (possibly infinite) length of the longest M-regular sequence in I.

Before we continue, recall that $\mathrm{Ext}^\bullet$ are the right derived functors of Hom and are computed by taking projective resolutions of the first argument or injective resolution of the second argument. In particular, if $0 \to A \to B \to C \to 0$ is an exact sequence, we have an exact sequence

$$\cdots \to \mathrm{Ext}^i(M,A) \to \mathrm{Ext}^i(M,B) \to \mathrm{Ext}^i(M,C) \to \mathrm{Ext}^{i+1}(M,A) \to \cdots$$

and similarly,

$$\cdots \to \mathrm{Ext}^i(C,N) \to \mathrm{Ext}^i(B,N) \to \mathrm{Ext}^i(A,N) \to \mathrm{Ext}^{i+1}(C,N) \to \cdots$$

Theorem 3.5.9. *Assume that A is Noetherian, M a finite A-module, and $I \subset A$ an ideal such that $IM \neq M$. Let $m \in \mathbb{Z}_{>0}$. Then the following are equivalent:*

1. $\mathrm{Ext}^n(N, M) = 0$ *for all* $i < n$ *and any finitely A-module* N *such that* $\mathrm{supp}(N) \subset V(I)$.

2. $\mathrm{Ext}^i(A/I, M) = 0$ *for all* $i < n$.

3. $\mathrm{Ext}^i(N, M) = 0$ *for all* $i < n$ *for some finite A-module* N *such that* $\mathrm{supp}(N) = V(I)$.

4. *There exists a M-regular sequence* $(a_1, \ldots, a_n)$ *of length* n *inside* I.

Proof. Clearly **1** implies **2** implies **3**. Now we prove **3** implies **4** implies **1**.

3 implies 4: Assume that $\mathrm{Hom}(N, M) = 0$. If I does not contain any M-regular element, then $I \subset \bigcup_{\mathfrak{p} \in \mathrm{Ass}\, M} \mathfrak{p}$ and thus $I \subset \mathfrak{p}$ for some $\mathfrak{p} \in \mathrm{Ass}(M)$. Then $A/\mathfrak{p} \hookrightarrow M$, which is equivalent to $A_\mathfrak{p}/\mathrm{p}A_\mathfrak{p} \hookrightarrow M_\mathfrak{p}$. On the other hand, we know $\mathfrak{p} \in V(I) = \mathrm{supp}(N)$, so $N_\mathfrak{p} \neq 0$. By Nakayama, we see that $N_\mathfrak{p} \otimes k(\mathfrak{p}) \neq 0$, and thus $\mathrm{Hom}_{A_\mathfrak{p}}(N_\mathfrak{p}, M_\mathfrak{p}) \neq 0$, but this is simply $\mathrm{Hom}_A(N, M)_\mathfrak{p}$. Thus $\mathrm{Hom}(N, M) \neq 0$ and thus there exists $a_1 \in I$ that is M-regular. Then we have an exact sequence

$$0 \to M \to M \to M/a_1 M \to 0.$$

Writing $M_1 = M/a_1 M$, we have proved the case $n = 1$ and now proceed by induction on n. Applying $\mathrm{Ext}^n(N, -)$ to the above exact sequence, we have the exact sequence

$$\cdots \to \mathrm{Ext}^i(N, M) \to \mathrm{Ext}^i(N, M_1) \to \mathrm{Ext}^{i+1}(N, M)$$

and deduce that $\mathrm{Ext}^i(N, M_1) = 0$ for $i < n - 1$. Applying the case $n - 1$ to M_1, we obtain an M_1-regular sequence $a_2, \ldots, a_n \in I$ and thus $(a_1, \ldots, a_n)$ is M-regular.

4 implies 1: We will induct on n. We have a sequence $a_1, \ldots, a_n \in I$ that is M-regular. Then set $M_1 = M/a_1 M$, so we have an exact sequence

$$0 \to M \to M \to M_1 \to 0.$$

Then choose N such that $\mathrm{supp}(N) \subset V(I)$. Then we have an exact sequence

$$\mathrm{Ext}^{i-1}(N, M_1) \to \mathrm{Ext}^i(N, M) \to \mathrm{Ext}^i(N, M).$$

If $i < n$, then $i - 1 < n - 1$. By the inductive hypothesis, this implies that $\mathrm{Ext}^i - 1(N, M_1) = 0$. Thus the map $\mathrm{Ext}^i(N, M) \xrightarrow{\times a_1} \mathrm{Ext}^i(N, M)$ is injective, so because $\mathrm{supp}(N) \subset V(I)$, we have $I \subset \sqrt{\mathrm{Ann}(N)}$. Thus there exists m such that $a_1^m \in \mathrm{Ann}(N)$. From the exact sequence, we know $\mathrm{Ext}^i(N, M) \xrightarrow{\times a_1^m} \mathrm{Ext}^i(N, M)$ is injective, which means that $\mathrm{Ext}^i(N, M) = 0$. □

Definition 3.5.10. If A is a local Noetherian ring and M is an A-module, then we define the depth of M to be

$$\mathrm{depth}(M) := \mathfrak{m}\text{-depth of } M.$$

This is the same as the maximal length of an M-regular sequence in $\mathfrak{m}$.

Corollary 3.5.11. *Let A be local Noetherian and M be a finitely-generated A-module. Then* $\mathrm{depth}(M) = n$ *if and only if there exists a M-regular sequence* $a_1, \ldots, a_n$ *such that* $\mathrm{Ext}^i(k, M) = 0$ *for all* $i < n$ *and* $\mathrm{Ext}^n(k, M) = \mathrm{Hom}(k, \overline{M})$, *where* $\overline{M} = M/(a_1, \ldots, a_m)M$ *and* $k = A/\mathfrak{m}$.

Proof. We know that the equivalence of **2** and **4** from the theorem implies the corollary except for $\mathrm{Ext}^n(k, M) = \mathrm{Hom}(k, \overline{M})$, but this fact be proved by induction on n using the fact that

$$0 \to M \xrightarrow{\times a_1} M \to M/a_1 M \to 0$$

is exact because this implies that $\mathrm{Ext}^{n-1}(k, M/a_1 M) = \mathrm{Ext}^n(k, M)$. This gives the desired result. $\square$

Lemma 3.5.12. *Let A be a local Noetherian and M, N finite A-modules. Then if $k = \mathrm{depth}(M)$ and $r = \dim(N)$, then $\mathrm{Ext}^i(N, M) = 0$ for all $i < k - r$.*

Proof. We use induction on r. For the case $r = 0$, we know that $\mathrm{supp}(N) = \{\mathfrak{m}\}$ and this follows by the previous theorem. Now for the inductive hypothesis, we may assume that $N = A/\mathfrak{p}$ and $\dim A/\mathfrak{p} = r$. This is possible because we can consider a filtration on N with successive quotients of the form $A/\mathfrak{p}_i$ with $\dim A/\mathfrak{p}_i \leq r$. We know that $\mathfrak{m} \neq \mathfrak{p}$, so there exists $x \in \mathfrak{m} \setminus \mathfrak{p}$, and this x is N-regular. Then we have the exact sequence

$$0 \to N \xrightarrow{\cdot x} N \to N' \to 0,$$

where $N' = N/xN$. Because $\overline{x}$ is not in any minimal prime ideal of $A/\mathfrak{p}$, we know that $r' := \dim N' < \dim A/\mathfrak{p}$. By induction, we know that $\mathrm{Ext}^j(N', M) = 0$ for $k < k - r'$. Now if $i < k - r$, we know that $i + 1 < k - r'$ and thus $\mathrm{Ext}^{i+1}(N', M) = 0$. Now considering the exact sequence of Ext groups, we have

$$\mathrm{Ext}^i(N', M) \to \mathrm{Ext}^i(N, M) \to \mathrm{Ext}^i(N, M) \to \mathrm{Ext}^{i+1}(N', M)$$

and thus $\mathrm{Ext}^i(N, M)/x\,\mathrm{Ext}^i(N, M) = 0$ and thus $\mathrm{Ext}^i(N, M) = 0$ by Nakayama's lemma. $\square$

Remark 3.5.13. If N, M are finitely-generated, then $\mathrm{Ext}^i(N, M)$ is also finitely-generated.

Theorem 3.5.14. *Let A be local Noetherian and M be a finitely-generated A-module. Then for all $\mathfrak{p} \in \mathrm{Ass}(M)$, we have $\mathrm{depth}\, M \leq \dim A/\mathfrak{p}$.*

Proof. We know $A/\mathfrak{p} \hookrightarrow M$, so $\mathrm{Hom}(A/\mathfrak{p}, M) \neq 0$. Thus $0 \geq \mathrm{depth}\, M - \dim A/\mathfrak{p}$ by the lemma. $\square$

Corollary 3.5.15. *Let A be local Noetherian. Then $\mathrm{depth}\, A \leq \dim A$.*

In general, this inequality is strict, so we will later study the rings for which this is an equality.

Lemma 3.5.16. *Let A be a local Noetherian ring. Then let M be a finitely-generated A-module and $(a_1, \ldots, a_r)$ be an M-regular sequence. Then $\dim M/(a_1, \ldots, a_r) <= \dim M - r$.*

Proof. We prove this by induction on M. It suffices to do this for $r = 1$, so choose $x \in A$ an M-regular element. We know that $\dim M/xM \geq \dim M - 1$ for any $x \in A$, so we need to prove this is an equality. Then we know $\mathrm{supp}(M/xM) = \mathrm{supp}(M) \cap V(x)$, and thus x is not contained in any minimal prime ideal in $\mathrm{supp}(M)$ by regularity. Therefore $\mathrm{supp}(M/xM)$ does not contain any minimal ideal of $V(\mathrm{Ann}(M)) = \mathrm{supp}(M)$. In particular, this means that $\dim M/xM < \dim M$, as desired. $\square$

Lemma 3.5.17. *Let M, N be finitely-generated A-modules. Then $\mathrm{supp}(M \otimes N) = \mathrm{supp}(M) \cap \mathrm{Supp}(N)$.*

Proof. Let $\mathfrak{p} \in \mathrm{Supp}(M) \cap \mathrm{Supp}(N)$. Then $M_\mathfrak{p}, N_\mathfrak{p} \neq 0$. By Nakayama, we have $M_\mathfrak{p} \otimes k(\mathfrak{p}) \neq 0$ and $N_\mathfrak{p} \otimes k(\mathfrak{p}) \neq 0$ where $k(\mathfrak{p}) = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. This implies that

$$M_\mathfrak{p} \otimes k(\mathfrak{p}) \otimes_{k(\mathfrak{p})} \otimes N_\mathfrak{p} \otimes k(\mathfrak{p}) \neq 0$$

and therefore $M_\mathfrak{p} \otimes k_\mathfrak{p} N_\mathfrak{p} = (M \otimes_A N)_\mathfrak{p} \neq 0$. Thus $\mathrm{supp}(M) \cap \mathrm{supp}(N) \subset \mathrm{supp}(M \otimes N)$. Note that for $N = A/xA$, we have $\mathrm{supp}(M/xM) = \mathrm{supp}(M) \cap V(x)$ because $M \otimes N = M/xM$. □

3.6 Cohen-Macaulay Rings and Modules

Let A be a local Noetherian ring and M be a finitely-generated A-module.

Definition 3.6.1. Recall that $\dim M \geq \operatorname{depth} M$. Then M is *Cohen-Macaulay* if $\dim M = \operatorname{depth} M$.

Theorem 3.6.2. *Let A be local Noetherian and M be finitely generated.*

1. *If M is Cohen-Macaulay, then for any $\mathfrak{p} \in \mathrm{Ass}(M)$, $\operatorname{depth} M = \dim A/\mathfrak{p}$.*

2. *If $f \in A$ is M-regular and $M' = M/fM$, then M is Cohen-Macaulay if and only if M' is.*

3. *If M is Cohen-Macaulay, then for all $\mathfrak{p} \in \operatorname{Spec} A$, $M_\mathfrak{p}$ is Cohen-Macaulay and $\operatorname{depth}_\mathfrak{p} M = \operatorname{depth}_{A_\mathfrak{p}} M_\mathfrak{p}$.*

Proof.

1. Let $M \neq 0$ and $\dim M = \operatorname{depth} M$. Then let $\mathfrak{p} \in \mathrm{Ass}(M) \subset \mathrm{supp}(M)$. This implies that $\dim A/\mathfrak{p} \leq \dim M$, but also $\dim A/\mathfrak{p} \geq \operatorname{depth}(M) = \dim M$.

2. Let f be M-regular. Then we know $\operatorname{depth} M/fM = \operatorname{depth} M - 1$ (this follows from the Theorem 3.5.9, applying $\mathrm{Ext}(k, -)$ to the exact sequence $0 \to M \to M \to M/fM \to 0$). But then we proved earlier that $\dim M/fM = \dim M - 1$, and thus M is C-M if and only if M/fM is C-M.

3. Let $\mathfrak{p} \in \mathrm{supp}(M)$. Then $\mathfrak{p} \supset \mathrm{Ann}(M)$ and $M_\mathfrak{p} \neq 0$. But then if $x_1, \ldots, x_r \in \mathfrak{p}$ is M-regular where $r = \operatorname{depth}_\mathfrak{p} M$, then $x_1, \ldots, x_r \in \mathfrak{p}A_\mathfrak{p}$ is $M_\mathfrak{p}$-regular by exactness of localization. This implies that $\operatorname{depth} M_\mathfrak{p} \geq r = \operatorname{depth}_\mathfrak{p} M$. We know that $\dim M_\mathfrak{p} \geq \operatorname{depth} M_\mathfrak{p}$, so we need to prove that $r = \dim M_\mathfrak{p}$. We do this by induction on $\operatorname{depth}_\mathfrak{p} M$. If $r = 0$, then we know $\mathrm{Hom}(A/\mathfrak{p}, M) \neq 0$. Thus there exists $\mathfrak{p}' \supset \mathfrak{p}$ such that $A/\mathfrak{p}' \hookrightarrow M$, so $\mathfrak{p}' \in \operatorname{Ass} M$. By minimality of associated primes, we have $\mathfrak{p}' = \mathfrak{p}$. Now $\dim M_{\mathfrak{p}'} = 0$ because $\mathfrak{p}$ is maximal in $A_\mathfrak{p}$ and minimal in $\mathrm{supp}(M)$.

   Now in general, assume $\operatorname{depth}_\mathfrak{p}(M) > 0$. Let $a \in \mathfrak{p}$ be M-regular. Thus a is $M_\mathfrak{p}$-regular, so set $M_1 = M/aM$. We know that $\dim(M_1)_\mathfrak{p} = \operatorname{depth}_\mathfrak{p} M_1$ by the inductive hypothesis. This implies that $\dim M_\mathfrak{p} = \operatorname{depth}_\mathfrak{p} M$ because $\dim(M_1)_\mathfrak{p} = \dim M_\mathfrak{p} - 1$ and $\operatorname{depth}_\mathfrak{p} M_1 = \operatorname{depth}_\mathfrak{p} M - 1$. □