Introduction to Commutative Algebra

December 20, 2019

About This Document

This document was typeset by Jason McCullough. It is based on course notes from a course taught by Professor S.P. Dutta at the University of Illinois texed by Jason McCullough and Bart Snapp. The notes have been redone in 2019 for Math 619 at Iowa State taught by Jason McCullough. Special thanks to: Michael Dewar, Jordan Disch, Dan Lior, Christian McRoberts, Elizabeth Sprangel, and Patrick Szuta, for making many comments and corrections concerning these notes.

Please report corrections, suggestions, gripes, complaints, and criticisms to: `jmccullo@iastate.edu`

Contents

Notation and Terminology

All rings are commutative and contain multiplicative identity, moreover we will always insist that ring homomorphisms respect the multiplicative identity element. Local rings are assumed to be Noetherian. Additionally, all modules are unitary modules. We have made an attempt to be consistent with our notation:

(1) Rings are often denoted by A, B, R, S.

(2) Modules are often denoted by M or N.

(3) Fields are often denoted by k, K, L, or F.

(4) Ideals are denoted by I, J, $\mathfrak{a}$, and $\mathfrak{b}$, with $\mathfrak{m}$ usually reserved for maximal ideals. We will try to reserve $\mathfrak{p}$, $\mathfrak{q}$, P, and Q for prime ideals.

(5) X is often used to denote indeterminants and in general $\mathbf{X} := X_1, \ldots, X_n$ and $\mathbf{x} := x_1, \ldots, x_n$ with the value of n (which is possibly infinite) being given by the context.

(6) The symbol $\mathbb{1}_M$ will denote the identity map $\mathbb{1}_M : M \to M$.

(7) The letter η will be often used to denote the canonical or *natural* map.

(8) If φ is a map, $\widetilde{\varphi}$ will often stand for the map induced by φ.

(9) We use the notation $\subseteq$ for set inclusion and use $\subsetneq$ for strict inclusion.

(10) The notion $\hookrightarrow$ is used to denote an injective map and $\twoheadrightarrow$ denotes a surjective map. If a commutative diagram is drawn, the induced map will be dashed.

(11) If A is a domain, $\mathrm{Frac}(A)$ will stand for the field of fractions of A.

(12) If $(A, \mathfrak{m})$ is a local ring, $\widehat{A}$ will often stand the $\mathfrak{m}$-adic completion of A.

(13) If A is a ring, $\widetilde{A}$ will often stand for the integral closure of A.

(14) If k is a field, $\overline{k}$ will often stand for the algebraic closure of k.

Chapter 0

Background

0.1 Operations on Ideals

Definition Given two ideals $I, J \subseteq A$, the **sum** of I and J is defined as

$$I + J = \{x + y : x \in I \text{ and } y \in J\}.$$

Exercise 0.1 *Show that if I and J are ideas in a ring A, then $I + J$ is an ideal.*

Definition Given two ideals $I, J \subseteq A$, the **product** of I and J is defined as

$$I \cdot J = \left\{ \sum_{i=1}^{n} x_i \cdot y_i : x_i \in I \text{ and } y_i \in J \right\}.$$

Exercise 0.2 *Show that if I and J are ideas in a ring A, then $I \cdot J$ is an ideal.*

Definition Given two ideals $I, J \subseteq A$, the **intersection** of I and J is defined as the set-theoretic intersection of I and J.

Exercise 0.3 *Show that if I and J are ideas in a ring A, then $I \cap J$ is an ideal.*

Exercise 0.4 *If $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ are ideals of A, show that*

$$\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}.$$

Exercise 0.5 *If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of A and M is an A-module, show that*

$$\mathfrak{a}(M/\mathfrak{b}M) = \frac{(\mathfrak{a} + \mathfrak{b})M}{\mathfrak{b}M}.$$

Exercise 0.6 *Assuming that $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ are ideals of A and that $\mathfrak{a} \supseteq \mathfrak{b}$ or $\mathfrak{a} \supseteq \mathfrak{c}$, prove the **modular law**:*

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}.$$

Definition Two ideals $I, J \subseteq A$ are called **comaximal** if $I + J = (1)$.

Remark Sometimes people use the term *coprime* for comaximal. We will refrain from doing this to avoid confusion later on with *coprimary* ideals.

Exercise 0.7 *Show that if I and J are comaximal ideals of A, then $IJ = I \cap J$.*

Definition An element x of a ring is called **nilpotent** if there exists $n \in \mathbb{N}$ such that $x^n = 0$.

Definition The set of nilpotent elements of a ring A is called the **nilradical** of A. We will use $\sqrt{0}$ to denote this set. Note that $\sqrt{0}$ is an ideal.

We can generalize the idea of the nilradical as follows:

Definition The **radical** of an ideal I is denoted by $\sqrt{I}$ and is defined to be the set

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

Note that $\sqrt{I}$ is an ideal.

Proposition 0.8 *Given a ring A, the radical of an ideal I is equal to the intersection of all the prime ideals which contain I.*

Proof ($\subseteq$) Suppose that $x \in \sqrt{I}$. Then $x^n \in I$ and for each prime ideal containing I, $x^n \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, $x \in \mathfrak{p}$. Thus

$$\sqrt{I} \subseteq \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p}.$$

($\supseteq$) By the Correspondence Theorem, the prime ideals of A containing I correspond bijectively to the ideals of A/I, hence we reduce to the case where $I = (0)$.

Suppose that x is not nilpotent. We'll show that

$$x \notin \bigcap_{\mathfrak{p} \supseteq (0)} \mathfrak{p}.$$

Consider the set of ideals of A:

$$\mathcal{S} = \{\mathfrak{a} : x^i \notin \mathfrak{a} \text{ for } i > 0\}$$

Note that $(0) \in \mathcal{S}$ and that $\mathcal{S}$ may be ordered by inclusion. Now let $\mathcal{C}$ be any chain of ideals in $\mathcal{S}$. This chain has an upper bound in $\mathcal{S}$, namely the ideal:

$$\bigcup_{\mathfrak{a} \in \mathcal{C}} \mathfrak{a}$$

Hence by Zorn's Lemma, $\mathcal{S}$ has a maximal element, call it $\mathfrak{p}$. We claim that $\mathfrak{p}$ is prime. Suppose that $a, b \notin \mathfrak{p}$. Hence $(a) + \mathfrak{p}$ and $(b) + \mathfrak{p}$ are ideals not contained in $\mathcal{S}$. Thus for some $m, n \in \mathbb{N}$:

$$x^m \in (a) + \mathfrak{p} \qquad \text{and} \qquad x^n \in (b) + \mathfrak{p}$$

Moreover,

$$x^{m+n} \in (ab) + \mathfrak{p}$$

and so we see that $ab \notin \mathfrak{p}$. Hence $\mathfrak{p}$ is prime and $x \notin \mathfrak{p}$. Thus x is not in the intersection of the prime ideals of A. ■

Corollary 0.9 (Properties of Radicals) *If I, J are ideals of A, the following hold:*

(1) $I \subseteq \sqrt{I}$.

(2) $\sqrt{I} = \sqrt{\sqrt{I}}$.

(3) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

(4) $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$.

WARNING 0.10 *The union of two ideals is **not** generally an ideal.*

Despite this fact there are some things we can say about unions of ideals.

Lemma 0.11 (Prime Avoidance) *Let A be a ring and I be an ideal of A. If $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are prime ideals such that*

$$I \not\subseteq \mathfrak{p}_i \qquad \text{for all } i,$$

then

$$I \not\subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i.$$

Proof We proceed by induction on n. The base case $n = 1$ is trivial. So assume $n \geq 2$. By induction, there exist for each $1 \leq i \leq n$ an element $a_i \in I - \bigcup_{j \neq i} \mathfrak{p}_j$. If any a_i avoid $\mathfrak{p}_i$ we are done; hence we may assume that $a_i \in \mathfrak{p}_i$ for all i. Consider $b = a_1 a_2 \cdots a_{n-1} + a_n$. Since $a_n \notin \mathfrak{p}_i$ for all $i < n$ and $a_1 \cdots a_{n-1} \in \mathfrak{p}_i$ for all $i < n$, we have $b \notin \mathfrak{p}_i$ for all $i < n$. Suppose $b \in \mathfrak{p}_n$. Since $\mathfrak{p}_n$ is prime and $a_n \in \mathfrak{p}_n$, we have $a_1 \cdots a_{n-1} \in \mathfrak{p}_n$ and hence $a_i \in \mathfrak{p}_n$ for some $i < n$. But this contradicts that $a_i \notin \mathfrak{p}_n$ for all $i < n$. Therefore $b \notin \mathfrak{p}_n$ and we are done. ■

Remark The above lemma is called *prime avoidance* as if $I \not\subseteq \mathfrak{p}_i$ for all i, then there is some element of $a \in I$ which *avoids* being contained in any $\mathfrak{p}_i$. Note also that we only used that $\mathfrak{p}_3, \ldots, \mathfrak{p}_n$ were prime ideals.

Definition If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of A, then the **colon ideal** $(\mathfrak{b} :_A \mathfrak{a})$ is defined as follows:

$$(\mathfrak{b} :_A \mathfrak{a}) = \{x \in A : x\mathfrak{a} \subseteq \mathfrak{b}\}$$

Moreover if M is an A-module and N is a submodule of M, then this can be generalized to modules by defining the **colon submodule** $(N :_M \mathfrak{a})$ as follows:

$$(N :_M \mathfrak{a}) = \{x \in M : x\mathfrak{a} \subseteq N\}$$

Remark Sometimes the colon ideal is called the *ideal quotient*. However, we will refrain from using that terminology as the word *quotient* is overused in mathematics.

Definition If M is an A-module, the **annihilator** of M over A, is defined as:

$$\mathrm{Ann}_A(M) := (0 :_A M) = \{x \in A : xm = 0 \text{ for all } m \in M\}$$

Proposition 0.12 (Properties of the Colon Ideal) *If $\mathfrak{a}, \mathfrak{b}$ are ideals of A, the following hold:*

(1) $\mathfrak{b} \subseteq (\mathfrak{b} :_A \mathfrak{a})$.

(2) $(\mathfrak{b} :_A \mathfrak{a})\mathfrak{a} \subseteq \mathfrak{b}$.

(3) $((\mathfrak{c} :_A \mathfrak{b}) : \mathfrak{a}) = (\mathfrak{c} :_A \mathfrak{b}\mathfrak{a}) = ((\mathfrak{c} :_A \mathfrak{a}) :_A \mathfrak{b})$.

(4) $(\bigcap_i \mathfrak{b}_i :_A \mathfrak{a}) = \bigcap_i (\mathfrak{b}_i :_A \mathfrak{a})$.

(5) $(\mathfrak{b} :_A \sum_i \mathfrak{a}_i) = \bigcap_i (\mathfrak{b} :_A \mathfrak{a}_i)$.

0.2 Chain Conditions

Definition Given a ring A, an A-module M is **Noetherian** if it satisfies the following equivalent conditions:

(1) Every non-empty set of submodules has a maximal element.

(2) M satisfies the ascending chain condition (ACC) on submodules.

(3) Every submodule in M is finitely generated.

Definition A ring A is **Noetherian** if it is a Noetherian A-module. Note that the only A-submodules of A are the ideals of the ring A.

Definition Given a ring A, an A-module M is **Artinian** if it satisfies the following equivalent conditions:

(1) Every non-empty set of submodules has a minimal element.

(2) M satisfies the descending chain condition (DCC) on submodules.

Definition A ring A is **Artinian** if it is an Artinian A-module. Note that the only A-submodules of A are the ideals of the ring A.

Example 0.13 *$\mathbb{Z}$ is a Noetherian ring which is not an Artinian ring.*

Example 0.14 *If k is a field $k[x_1, \ldots, x_n, \ldots]$, is neither Artinian nor Noetherian.*

Example 0.15 *Any field is both an Artinian and Noetherian ring.*

Remark As we will soon state, every Artinian ring is also a Noetherian ring.

Example 0.16 *A finite Abelian group is a $\mathbb{Z}$-module which is both Noetherian and Artinian.*

Proposition 0.17 *Given a short exact sequence of A-modules*

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

we have that:

(1) *M is Noetherian if and only if both M' and M'' are Noetherian.*

(2) *M is Artinian if and only if both M' and M'' are Artinian.*

Proof Exercise. ■

Proposition 0.18 *If a ring A is Noetherian and M is a finitely generated A-module, then M is Noetherian.*

Proof It follows by inductively applying the previously lemma that every finitely generated free A-module is Noetherian if A is. Since M is finitely generated, there is a surjection $A^n \to M \to 0$ to M from a finitely generated free A-module. Again by the previous lemma it follows that M is Noetherian. ■

Example 0.19 *The hypothesis that A is Noetherian in the previous proposition is necessary. The ring $A = k[x_1, \ldots, x_n, \ldots]$ is a finitely generated A-module which is not Noetherian.*

Example 0.20 *In general, Artinian modules, even those over Noetherian rings, need not be Noetherian. $\mathbb{Z}_{p^\infty}$ is an Artinian $\mathbb{Z}$-module which is not a Noetherian $\mathbb{Z}$-module. Recall that $\mathbb{Z}_{p^\infty}$ is the $\mathbb{Z}$-submodule of $\mathbb{Q}/\mathbb{Z}$ generated by*

$$\{1/p^n : p \text{ is a prime in } \mathbb{Z}\}.$$

Definition A chain of A-modules

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = (0)$$

is a **Jordan-Hölder chain**, also known as a **composition series**, if for each i, $M_i/M_{i+1} \cong A/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ in A.

While one can show that all compositions series have the same length by using the Jordan-Hölder Theorem from group theory, we present a direct proof here.

Proposition 0.21 *Each composition series for M has the same length.*

Proof Let $\lambda(M)$ denote the length of a shortest composition series of M. First we show that if $N \subseteq M$, then $\lambda(N) \leq \lambda(M)$. Suppose $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = (0)$ is a composition series of M of minimal length and set $N_i = N \cap M_i$. Since $N_i/N_{i+1} \subseteq M_i/M_{i+1} \cong A/\mathfrak{m}$ for all i, either $N_i/N_{i+1} \cong 0$ or $N_i/N_{i+1} \cong A/\mathfrak{m}$. (Here we are using that $A/\mathfrak{m}$ is a simple A-module.) Removing repeated terms we have a composition series of N so that $\lambda(N) \leq \lambda(M)$. If $\lambda(N) = \lambda(M)$, then $N_i = M_i$ for all i and in particular $N = M$. Therefore if $N \subsetneq M$, then $\lambda(N) < \lambda(M)$. Now let $M = M'_0 \supsetneq M'_1 \supsetneq \cdots \supsetneq M'_t = (0)$ be any composition series of M. By above, we have $\lambda(M) = \lambda(M'_0) > \lambda(M'_1) > \cdots > \lambda(M'_n) = 0$ and so $\lambda(M) \geq t$. By the definition of $\lambda(M)$, we have $\lambda(M) = t$ and so all composition series have the same length.

■

Definition The **length** of an A-module, denoted by $\lambda_A(M)$, is the length of a composition series for M. That is, if

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = (0)$$

is a composition series, then $\lambda_A(M) = n$.

Proposition 0.22 *Given a short exact sequence of A-modules*

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

such that $\lambda_A(M)$ is finite, then length is an additive function, that is,

$$\lambda_A(M) = \lambda_A(M') + \lambda_A(M'').$$

In particular, $\lambda_A(M)$ is finite if and only if $\lambda_A(M')$ and $\lambda_A(M'')$ are finite.

Proof It is not hard to check that the images in M of a composition series of M' and the inverse images of a composition series of M'' fit together to form a composition series of M. ■

Theorem 0.23 *An A-module M has finite length if and only if M is both Artinian and Noetherian.*

Proof Clearly if $\lambda(M) < \infty$, then M is both Artinian and Noetherian. Conversely, if M is Noetherian, M has a maximal proper submodule $M_1 \subsetneq M$; M_1 has a maximal proper submodule $M_2 \subsetneq M_1$; and so on. If M is Artinian, this process must eventually stop, yielding a finite composition series of M. ■

Theorem 0.24 (Hilbert's Basis Theorem) *If A is a Noetherian ring, then $A[x]$ is a Noetherian ring.*

Proof See [5, Theorem 9.21]. ■

Corollary 0.25

(1) $\mathbb{Z}[x_1, \ldots, x_n]$ *is Noetherian.*

(2) *If k is a field, then $k[x_1, \ldots, x_n]$ is Noetherian.*

Exercise 0.26 *Show that if A is Noetherian, then $A[\![x]\!]$ is Noetherian.*

Definition Let A be a ring. The **Jacobson radical** $\mathcal{J}(A)$ is the intersection of all maximal ideals of A.

Exercise 0.27 *Let A be a ring and let $x \in A$. Show that $x \in \mathcal{J}(A)$ if and only if $1 - ax$ is a unit for all $a \in A$.*

Theorem 0.28 (Krull's Intersection Theorem) *Let A be a ring with an ideal I and M a finitely generated A-module such that $IM = M$. Then there exists $a \in I$ such that*

$$(1 - a)M = 0.$$

Proof Let $x_1, \ldots, x_d$ be a set of generators for M. Since $IM = M$ we have

$$x_i = a_{i,1}x_1 + \cdots + a_{i,d}x_d$$

for each $i = 1, \ldots, d$, where $a_{i,j} \in I$ for all i and j. Therefore

$$\begin{array}{rcl} x_1 & = & a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,d}x_d \\ x_2 & = & a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,d}x_d \\ \vdots & \vdots & \vdots \qquad\quad \vdots \qquad\qquad \vdots \\ x_d & = & a_{d,1}x_1 + a_{d,2}x_2 + \cdots + a_{d,d}x_d. \end{array}$$

We can write this in matrix form as

$$\begin{bmatrix} 1 - a_{1,1} & -a_{1,2} & \cdots & -a_{1,d} \\ -a_{2,1} & 1 - a_{2,2} & \cdots & -a_{2,d} \\ \vdots & \vdots & & \vdots \\ -a_{d,1} & -a_{d,2} & \cdots & 1 - a_{d,d} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Let B be the above $n \times n$ matrix. Then we see that $\det(B) \cdot x_i = 0$ for all $i = 1, \ldots, d$, say by Cramer's Rule. Observe that $a = 1 - \det(B) \in I$ and that $(1 - a)M = \det(B)M = 0$, which completes the proof. ■

Corollary 0.29 (Nakayama's Lemma) *Let A be a ring and I be an ideal of A such that $I \subseteq \mathfrak{J}(A)$. If M is a finitely generated A-module such that $IM = M$, then $M = 0$.*

Proof By Krull's Intersection Theorem, Theorem 0.28, there exists $a \in I$ such that $(1 - a)M = 0$. Since $I \subseteq \mathfrak{J}(A)$ we have that $1 - a$ is a unit. Therefore $M = 0$. ■

Exercise 0.30 *Prove Krull's Intersection Theorem, Theorem 0.28, assuming you know Nakayama's Lemma. One can start to see why Nakayama himself said that the lemma bearing his name is a theorem of Krull and Azumaya.*

Exercise 0.31 *Let A be a commutative ring and let M be a finitely generated A-module. Suppose $f : M \to M$ is surjective. Then f is an isomorphism. This a result due to Vasconcelos.*

Proposition 0.32 *If a ring A is Artinian, then A has finitely many maximal ideal.*

Proof Suppose A has infinitely many maximal ideals $\mathfrak{m}_1, \mathfrak{m}_2, \ldots$. Then $\mathfrak{m}_1 \supsetneq \mathfrak{m}_1 \cap \mathfrak{m}_2 \supsetneq \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \mathfrak{m}_3 \subsetneq \cdots$ is a strictly descending chain of ideals, meaning A is not Artinian. ■

Theorem 0.33 (Akizuki) *A ring A is Artinian if and only if $\lambda(A) < \infty$. In particular, every Artinian ring is Noetherian.*

Proof Clearly if $\lambda(A) < \infty$, A is both Noetherian and Artinian by Theorem 0.23. So suppose A is Artinian. By the previous Proposition, A has finitely many maximal ideals, say $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$. Then $J := \mathcal{J}(A) = \mathfrak{m}_1 \cdots \mathfrak{m}_t = \bigcap_{i=1}^{t} \mathfrak{m}_i$. Since A is Artinian, the descending chain of ideals $J \supseteq J^2 \supseteq \cdots$ stabilizes and hence $J^n = J^{n+1}$ for some n. Set $I = (0) : J^n$. Then $I : J = ((0) : J^n) : J = (0) : J^{n+1} = (0) : J^n = I$. We claim that $I = A$. If not, by the Artinian property there exists a minimal ideal $I' \supsetneq I$, which must be of the form $I' = Ax + I$ for some $x \in A - I$. Since $I \neq I'$, it follows by Nakayama's Lemma 0.29 that $I' \neq Jx + I$ (as otherwise we would have $Ax + I = Jx + I$ in A/I). By minimality of I', $Jx + I = I$ and hence $Jx \subseteq I$, i.e. $x \in I : J = I$ contradicting that $x \notin I$. Therefore $I = A$ and thus $J^n = 0$.

Now consider the chain of ideals

$$\begin{aligned} A \supsetneq \mathfrak{m}_1 \supsetneq \mathfrak{m}_1\mathfrak{m}_2 \supsetneq \cdots \supsetneq \mathfrak{m}_1 \cdots \mathfrak{m}_{t-1} \supsetneq J \supsetneq J\mathfrak{m}_1 \supsetneq J\mathfrak{m}_1\mathfrak{m}_2 \supsetneq \cdots \\ \supsetneq J^2 \supsetneq J^2\mathfrak{m}_1 \supsetneq \cdots \supsetneq J^n = 0. \end{aligned}$$

Then any two consecutive terms are of the form M and $M\mathfrak{m}_i$ and thus consecutive quotients are vector spaces over $A/\mathfrak{m}_i$. It follows that $\lambda(A) < \infty$. ■

0.3 Flat Modules

Definition An A-module F is **flat** if

$$M \hookrightarrow M'$$

implies that

$$M \otimes_A F \hookrightarrow M' \otimes_A F.$$

Remark If F is flat then $- \otimes_A F$ and $F \otimes_A -$ are exact functors from the category of A-modules to the category of A-modules.

Proposition 0.34 *An A-module F is flat if and only if for all finitely generated A-modules M and M', $M \hookrightarrow M'$ implies that*

$$M \otimes_A F \hookrightarrow M' \otimes_A F.$$

Proof One direction is clear. We prove the contrapositive for the other. Suppose that F is not flat. Then there is an injective map of A-modules $\phi : M \to M'$ such that the map $\phi \otimes_A \mathbb{1}_F : M \otimes_A F \to M' \otimes_A F$ is not injective. Let $x \in \mathrm{Ker}(\phi \otimes_A \mathbb{1}_F)$ be nonzero. Then we can write $x = \sum_{i=1}^{n} m_i \otimes f_i$. Let $N = Am_1 + \cdots + Am_n \subseteq M$. Since $\phi \otimes_A \mathbb{1}_F(x) = 0$, this element can be written as a finite linear combination of the defining relations of the tensor product in $M' \times F$. Setting $N' \subseteq M'$ to be the submodule generated by all elements of M' appearing in this linear combination, along with $\phi(m_1), \ldots, \phi(m_n)$ we have an injective $N \hookrightarrow N'$ of finitely generated modules such that $N \otimes_A F \to N' \otimes_A F$ is not injective as x is in the kernel. ■

Proposition 0.35 *If A and B are rings, where B is an A-module, then B is flat over A if and only if any solution $\mathbf{x} \in B$ of homogeneous equations*

$$\sum a_{i,j} x_j = 0 \qquad \text{where} \qquad \mathbf{a} \in A$$

is a B-linear combination of solutions in A.

Proof Exercise. ■

Proposition 0.36 *Every free module is projective. Every projective module is flat.*

Proof See [5, Corollary 10.31, Corollary 10.42]. ■

Example 0.37 *$\mathbb{Q}$ is flat over $\mathbb{Z}$ but not projective over $\mathbb{Z}$.*

Example 0.38 *$\mathbb{Z}/2\mathbb{Z}$ is a projective $\mathbb{Z}/6\mathbb{Z}$-module that is not free.*

0.4 Localization

Let U be a subset of A which is closed under multiplication and contains 1. Given an A-module M, we may now write "fractions"

$$\frac{m}{u},$$

where $m \in M$ and $u \in U$. For $m' \in M$ and $u' \in U$, we will say

$$\frac{m}{u} = \frac{m'}{u'} \quad \text{when} \quad (mu' - m'u)z = 0$$

for some $z \in U$. This defines an equivalence relation and we denote the set of equivalence classes by $U^{-1}M$. We can put the canonical module structure on $U^{-1}M$. If M is an A-algebra, we may put the canonical ring structure on $U^{-1}M$.

Proposition 0.39 (Universal Property of Localization) *If $\varphi : A \to B$ is a homomorphism of rings such that $\varphi(u)$ is a unit in B for all $u \in U$, then there exists a unique homomorphism $\widetilde{\varphi} : U^{-1}A \to B$ making the diagram below commute.*

$$\begin{array}{ccc} A & \xrightarrow{\eta} & U^{-1}A \\ {\scriptstyle\varphi}\downarrow & \swarrow_{\widetilde{\varphi}} & \\ B & & \end{array}$$

Proof Exercise. ■

WARNING 0.40 *If A is a domain, then the map $A \to U^{-1}A$ is injective but this is not true in general; for example, consider $A = \mathbb{Z}/6\mathbb{Z}$ and $U = \{1, 3\}$.*

Proposition 0.41 *If M is an A-module and U is a multiplicatively closed subset of A, then there is a canonical isomorphism $M \otimes_A U^{-1}A \cong U^{-1}M$. Moreover, this isomorphism is functorial. That is, if $f : M \to N$ is a map of A-modules, then the following diagram commutes*

$$\begin{array}{ccc} M \otimes_A U^{-1}A & \xrightarrow{\eta_M} & U^{-1}M \\ {\scriptstyle f\otimes \mathbb{1}_{U^{-1}A}}\downarrow & & \downarrow{\scriptstyle U^{-1}f} \\ N \otimes_A U^{-1}A & \xrightarrow[\eta_N]{} & U^{-1}N \end{array}$$

where η_M and η_N represent the canonical isomorphisms.

Proof Exercise. ■

Proposition 0.42 *$U^{-1}A$ is a flat A-module.*

Proof Let $0 \to M' \to M$ be an exact sequence of A-modules. View M' as a submodule of M and let $x \in M'$ and $u \in U$. Then $\frac{x}{u} = 0$ in $U^{-1}M'$ if and only if $tx = 0$ for some $t \in U$ if and only if $\frac{x}{u} = 0$ in $U^{-1}M$. Thus $0 \to U^{-1}M' \to U^{-1}M$ is exact. ■

As an immediate corollary we have:

Corollary 0.43 *If the following sequence of A-modules is exact*

$$0 \to M' \to M \to M'' \to 0,$$

then

$$0 \to U^{-1}M' \to U^{-1}M \to U^{-1}M'' \to 0$$

is exact.

Definition For $a \in A$, if $U = \{1, a, a^2, a^3, \dots\}$, we denote $U^{-1}M$ by either M_a or $M[\frac{1}{a}]$.

Definition If A is a domain, then the **field of fractions** is given by:

$$\mathrm{Frac}(A) := (A - \{0\})^{-1}A$$

Definition If $U = A - \mathfrak{p}$ where $\mathfrak{p}$ is a prime ideal of A, we denote $U^{-1}M$ by $M_{\mathfrak{p}}$. We say this as "M localized at $\mathfrak{p}$."

Definition A ring A is **local** if it is Noetherian and has a unique maximal ideal. When dealing with local rings, one often writes

$$(A, \mathfrak{m}) \qquad \text{or} \qquad (A, \mathfrak{m}, k)$$

to denote the ring and its maximal ideal or the ring, its maximal ideal, and $k = A/\mathfrak{m}$ respectively.

Remark Some authors do not insist that local rings are Noetherian. We will call local rings which are not Noetherian **quasilocal**.

Proposition 0.44 *If A is a ring and $\mathfrak{p}$ is a prime ideal, then $A_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$.*

Proof By construction, $\frac{x}{s} \in A_{\mathfrak{p}} - \mathfrak{p}A_{\mathfrak{p}}$ if and only if $x \notin \mathfrak{p}$ if and only if x is a unit in $A_{\mathfrak{p}}$. It follows that $A_{\mathfrak{p}}$ is a local ring with unique maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$. ■

Definition For a ring A with a prime ideal $\mathfrak{p}$ we define the **residue field** of $\mathfrak{p}$, denoted $\boldsymbol{\kappa}(\mathfrak{p})$, by

$$\boldsymbol{\kappa}(\mathfrak{p}) := A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} = (A/\mathfrak{p})_{\mathfrak{p}} = \mathrm{Frac}(A/\mathfrak{p}).$$

Now we come to some very important properties of localization:

Proposition 0.45 *Given an A-module M, the following are equivalent:*

(1) $M = 0$.

(2) $M_{\mathfrak{p}} = 0$ *for all prime ideals* $\mathfrak{p}$ *of* A.

(3) $M_{\mathfrak{m}} = 0$ *for all maximal ideals* $\mathfrak{m}$ *of* A.

Proof (1) $\Rightarrow$ (2) $\Rightarrow$ (3) are obvious. Now suppose $M \neq 0$ but $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$. Let $x \in M$ be nonzero. Then $\mathrm{Ann}_A(x)$ is a proper ideal, necessarily contained in some maximal ideal $\mathfrak{m}'$ of A. Since $M'_{\mathfrak{m}} = 0$, $xt = 0$ for some $t \notin \mathfrak{m}'$, but this contradicts $\mathrm{Ann}_A(x) \subseteq \mathfrak{m}'$. This completes the proof. ■

Corollary 0.46 *Let M, M', and M'', be A-modules. The following are equivalent:*

(1) $0 \to M' \to M \to M'' \to 0$ *is exact.*

(2) $0 \to M'_{\mathfrak{p}} \to M_{\mathfrak{p}} \to M''_{\mathfrak{p}} \to 0$ *is exact for all prime ideals* $\mathfrak{p}$ *in* A.

(3) $0 \to M'_{\mathfrak{m}} \to M_{\mathfrak{m}} \to M''_{\mathfrak{m}} \to 0$ *is exact for all maximal ideals* $\mathfrak{m}$ *in* A.

Proof Exercise. ■

The above corollary tells us that if we can show that an A-module homomorphism is injective [resp. surjective] after localizing at an arbitrary prime or maximal ideal, then we can conclude that the homomorphism is injective [resp. surjective]. This is why it is sometimes said that the injectivity or surjectivity of an A-module homomorphism is a **local property**.

Chapter 1

Primary Decomposition

1.1 Primary and Coprimary Modules

In this section we will mostly consider the case when A is Noetherian and A-modules are finitely generated.

Definition Let A be a Noetherian ring. A nonzero finitely generated A-module M is **coprimary** if for all $a \in A$, the map defined via multiplication by a

$$M \xrightarrow{a} M$$

is injective or nilpotent.

Proposition 1.1 *If M is coprimary, then the set*

$$\mathfrak{p} = \{a \in A : M \xrightarrow{a} M \text{ is nilpotent}\}$$

forms a prime ideal in A.

Proof Suppose that $a \notin \mathfrak{p}$ and $b \notin \mathfrak{p}$. Then the map defined via multiplication by a is injective and the map defined via multiplication by b is injective. Hence the map defined via multiplication by ab is injective and we see that $ab \notin \mathfrak{p}$. ■

Definition The coprimary module M which gives the above prime ideal $\mathfrak{p}$ is called **$\mathfrak{p}$-coprimary**.

Proposition 1.2 *If N is any nonzero submodule of a finitely generated $\mathfrak{p}$-coprimary A-module M, then N is also $\mathfrak{p}$-coprimary.*

Proof This follows easily from the definition. ■

Proposition 1.3 *If A is a Noetherian ring and M is a $\mathfrak{p}$-coprimary A-module, then we have an injection*

$$A/\mathfrak{p} \hookrightarrow M.$$

Proof Consider any $m \in M$ such that $m \neq 0$ and let

$$I = \mathrm{Ann}_A(m) = \{a \in A : am = 0\}.$$

Since A is Noetherian, $\mathfrak{p}$ is finitely generated, and so we write $\mathfrak{p} = (p_1, \ldots, p_t)$. Because M is $\mathfrak{p}$-coprimary, there exist integers n_i such that for each i,

$$p_i^{n_i} m = 0.$$

Thus there exists n such that $\mathfrak{p}^n \subseteq I \subseteq \mathfrak{p}$. If $\mathfrak{p} = I$, we are done since we have an injection $A/I \hookrightarrow M$. If $\mathfrak{p} \neq I$, there exists a l such that $\mathfrak{p}^l \subseteq I$ but $\mathfrak{p}^{l-1} \not\subseteq I$.

Take $x \in \mathfrak{p}^{l-1} - I$ and consider $\varphi : A \to M$ via $1 \mapsto m$. We have that $\mathrm{Ker}(\varphi) = I$. Hence

$$A/I \hookrightarrow M.$$

Let $\overline{x}$ be the image of x in A/I. Since $\mathfrak{p}x \subseteq \mathfrak{p}^l \subseteq I$, $\mathrm{Ann}_A(\overline{x}) \supseteq \mathfrak{p}$. Moreover, if there exists $a \in A$ such that $ax \in I$, then since $A/I \hookrightarrow M$ and M is $\mathfrak{p}$-coprimary, we have that $a \in \mathfrak{p}$. Therefore $\mathrm{Ann}_A(\overline{x}) = \mathfrak{p}$. So

$$A/\mathfrak{p} \xhookrightarrow{\overline{x}} A/I \hookrightarrow M.$$

This is the injection we were looking for. ■

Proposition 1.4 *Let M be a finitely generated $\mathfrak{p}$-coprimary A-module. If*

$$A/\mathfrak{q} \hookrightarrow M$$

for some prime ideal $\mathfrak{q} \subseteq A$, then $\mathfrak{q} = \mathfrak{p}$.

Proof By Proposition 1.2 it suffices to show that $A/\mathfrak{q}$ is $\mathfrak{p}$-coprimary. But this follows from the definition. ■

Definition Let A be a Noetherian ring. Given finitely generated A-modules $N \hookrightarrow M$, N is a **primary** [resp. **$\mathfrak{p}$-primary**] submodule of M if M/N is coprimary [resp. $\mathfrak{p}$-coprimary].

Proposition 1.5 *If $\mathfrak{p}$ is a prime ideal, then $\mathfrak{p}$ is $\mathfrak{p}$-primary.*

Proof Exercise. ■

Proposition 1.6 *I is a primary ideal of A if and only if whenever $xy \in I$ and $y \notin I$, we then have $x^n \in I$ for some $n \in \mathbb{N}$.*

Proof ($\Rightarrow$) Assume I is a primary ideal of A. So the map

$$A/I \xrightarrow{x} A/I$$

is either injective or nilpotent. If $xy \in I$ where $y \notin I$, we see that $x\overline{y} = 0$ and $\overline{y} \neq 0$. Thus x must be a nilpotent map, and so $x^n \in I$.

($\Leftarrow$) Fix $x \in A$. If $xy \in I$ and $y \notin I$, then by assumption $x^n \in I$ for some $n \in \mathbb{N}$. Thus the map

$$A/I \xrightarrow{x} A/I$$

is nilpotent. On the other hand, if $xy \notin I$ for any $y \notin I$, then the above map is injective. ■

Corollary 1.7 *If I is $\mathfrak{p}$-primary, then $\sqrt{I} = \mathfrak{p}$.*

Proof Let $xy \in \sqrt{I}$. Then $(xy)^m \in I$ for some $m \in \mathbb{N}$. Since I is $\mathfrak{p}$-primary, either $x^m \in I$ or $y^{mn} \in I$ for some $n \in \mathbb{N}$. Therefore $x \in \sqrt{I}$ or $y \in \sqrt{I}$ and so $\sqrt{I}$ is prime. Since $I \subseteq \mathfrak{p}$ and since $\sqrt{I}$ is the intersection of all primes containing I, we must have $\mathfrak{p} = \sqrt{I}$. ■

Proposition 1.8 *Let A be a Noetherian ring. Suppose I is an ideal and $\mathfrak{m}$ is a maximal ideal such that $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$. Then I is $\mathfrak{m}$-primary.*

Proof Let $a \in A$. We wish to show that if $a \in \mathfrak{m}$, the map $A/I \xrightarrow{a} A/I$ is nilpotent and if $a \notin \mathfrak{m}$, then the map is injective. If $a \in \mathfrak{m}$, then $a^n \in \mathfrak{m}^n \subseteq I$. Thus $a^n(A/I) = (0)$ and so the map is nilpotent.

Assume $a \notin \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, $\mathfrak{m} + aA = A$. Thus there are $x \in \mathfrak{m}$ and $y \in A$ such that $x + ay = 1$. Taking the nth power we get

$$\begin{aligned}(x + ay)^n &= x^n + ay' \\ &= 1,\end{aligned}$$

where y' is some element of A. Since $x^n \in \mathfrak{m}^n \subseteq I$, $\overline{a}$ and $\overline{y'}$ are units in A/I. Thus the map defined by multiplication by a is an isomorphism. In particular, it is injective. ■

WARNING 1.9 *It is not true in general that an ideal I is $\mathfrak{p}$-primary if*

$$\mathfrak{p}^n \subseteq I \subseteq \mathfrak{p}.$$

Consider the ring $A = k[x, y, z]/(z^2 - xy)$ where k is a field. Set $\mathfrak{p} = (\overline{x}, \overline{z})$, where $\overline{x} = x + (z^2 - xy)$ and $\overline{z} = z + (z^2 - xy)$. Then $A/\mathfrak{p} \cong k[x, y, z]/(x, z) \cong k[y]$, which is a domain. Thus $\mathfrak{p}$ is a prime ideal.

We claim $\mathfrak{p}^2$ is not $\mathfrak{p}$ primary. To see this, note that $z^2 = xy \in \mathfrak{p}^2$ and so the map $A/\mathfrak{p}^2 \xrightarrow{\overline{z}} A/\mathfrak{p}^2$ is not injective. It follows that $\mathfrak{p}^2$ is not $\mathfrak{p}$-primary.

Exercise 1.10 *Suppose A is a UFD and $\mathfrak{p} = (p)$ where p is a prime element. Show that $\mathfrak{p}^n$ is $\mathfrak{p}$-primary for all $n > 0$.*

Exercise 1.11 *Let $\mathfrak{p} = (xz - y^2, x^3 - yz, x^2y - z^2)$ in $k[x, y, z]$ where k is a field. Show that $\mathfrak{p}$ is a prime ideal. (Hint: Show that $\mathfrak{p}$ is the kernel of some map $\phi : k[x, y, z] \to k[t]$.) Is $\mathfrak{p}^2$ $\mathfrak{p}$-primary?*

1.2 The Primary Decomposition Theorem

Definition If M is an A-module, a proper submodule $N \subsetneq M$ is called **irreducible** if $N \neq N_1 \cap N_2$ for any submodules N_1, N_2 of M that properly contain N.

Lemma 1.12 *Let A be a Noetherian ring and M be a finitely generated A-module. Any proper submodule N of M can be expressed as a finite intersection of irreducible submodules of M.*

Proof Suppose not and let $\mathcal{S}$ be the collection of proper submodules of M that cannot be expressed as a finite intersection of irreducible submodules of M. By assumption, $\mathcal{S} \neq \varnothing$. M is Noetherian, so $\mathcal{S}$ has a maximal element N_0. Then N_0 is not irreducible, so there are submodules N_1, N_2 of M which properly contain N_0 such that $N_0 = N_1 \cap N_2$. Note that N_1 and N_2 are proper submodules of M. Since N_0 is maximal in $\mathcal{S}$, N_1 and N_2 can be expressed as finite intersections of irreducible submodules. Thus N_0 can be expressed as a finite intersection of submodules, contradicting $N_0 \in \mathcal{S}$. Therefore, $\mathcal{S} = \varnothing$ and every proper submodule of M can be expressed as a finite intersection of irreducible submodules of M. ■

Lemma 1.13 *Let A be a Noetherian ring and M be a finitely generated A-module. Suppose N is an irreducible submodule of M. Then N is a primary submodule of M.*

Proof To show that N is a primary submodule of M, we must show that $\overline{M} = M/N$ is coprimary. Since N is irreducible in M, $(0) = \overline{N}$ is irreducible in $\overline{M}$. Let $a \in A$ and consider the map $\varphi : \overline{M} \to \overline{M}$ given by $\varphi(\overline{m}) = a\overline{m}$.

$$\mathrm{Ker}(\varphi) \subseteq \mathrm{Ker}(\varphi^2) \subseteq \cdots$$

forms an ascending chain of submodules of $\overline{M}$. Since M is Noetherian, $\overline{M}$ is Noetherian. Thus the above chain of submodules halts; that is, there is an integer n such that

$$\mathrm{Ker}(\varphi^n) = \mathrm{Ker}(\varphi^{n+1}) = \mathrm{Ker}(\varphi^{n+2}) = \cdots .$$

Set $g = \varphi^n$. Then $\mathrm{Ker}(g) = \mathrm{Ker}(g^2)$ from which it follows that

$$\mathrm{Im}(g) \cap \mathrm{Ker}(g) = (0).$$

Since (0) is irreducible, either $\mathrm{Im}(g) = (0)$ or $\mathrm{Ker}(g) = (0)$. If $\mathrm{Im}(g) = (0)$, then $a^n\overline{M} = (0)$ and φ is nilpotent. If $\mathrm{Ker}(g) = (0)$, then $\mathrm{Ker}(\varphi) = (0)$ and φ is injective. Thus $\overline{M}$ is coprimary and N is a primary submodule of M. ■

Example 1.14 *It is not true that every primary submodule or even ideal is irreducible. Consider $I = (x, y)^2 \subseteq K[x, y]$, where K is a field. By Proposition 1.8, I is (x, y)-primary. However, $I = (x, y^2) \cap (x^2, y)$ and so I is not irreducible.*

Lemma 1.15 *Let M be a finitely generated A-module. If N_1 and N_2 are both $\mathfrak{p}$-primary submodules of M, then $N_1 \cap N_2$ is also $\mathfrak{p}$-primary.*

Proof By definition, M/N_1 and M/N_2 are $\mathfrak{p}$-coprimary. It follows easily from the definition that $M/N_1 \oplus M/N_2$ is also $\mathfrak{p}$-coprimary. Consider the map:

$$\begin{aligned} \varphi : M &\to M/N_1 \oplus M/N_2 \\ m &\mapsto (m + N_1, m + N_2) \end{aligned}$$

Then $\mathrm{Ker}(\varphi) = N_1 \cap N_2$ and we have an injection:

$$M/(N_1 \cap N_2) \hookrightarrow M/N_1 \oplus M/N_2$$

Thus by Proposition 1.2, $M/(N_1 \cap N_2)$ is $\mathfrak{p}$-coprimary. Therefore $N_1 \cap N_2$ is $\mathfrak{p}$-primary. ■

Theorem 1.16 (Primary Decomposition Theorem) *Let A be a Noetherian ring. If N is a proper submodule of a finitely generated A-module M, we can write*

$$N = \bigcap_{i=1}^{n} N_i$$

such that:

(1) *Each N_i is $\mathfrak{p}_i$-primary for some prime ideal $\mathfrak{p}_i$.*

(2) *If $i \neq j$, then $\mathfrak{p}_i \neq \mathfrak{p}_j$.*

(3) *If $N = \bigcap_{i=1}^{s} N_i'$ is another such decomposition, where N_i' is $\mathfrak{p}_i'$-primary for $i = 1, \ldots, s$, then*

$$\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} = \{\mathfrak{p}_1', \ldots, \mathfrak{p}_s'\}$$

and in particular, $n = s$.

Proof By Lemmas 1.12, 1.13, and 1.15, we can express N as a finite intersection of submodules $\bigcap_{i=1}^{n} N_i$ where for each i, N_i is $\mathfrak{p}_i$-primary, with the prime ideals $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ distinct.

To finish the proof, we will show:

$$\mathfrak{p} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \Leftrightarrow A/\mathfrak{p} \hookrightarrow M/N.$$

($\Rightarrow$) Suppose that $\mathfrak{p} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. WLOG assume $\mathfrak{p} = \mathfrak{p}_1$. Write

$$\begin{aligned} N_2/N \cap \cdots \cap N_n/N &\cong (N_2 \cap \cdots \cap N_n)/N \\ &\cong (N_1 + (N_2 \cap \cdots \cap N_n))/N_1 \\ &\subseteq M/N_1, \end{aligned}$$

with the middle line following from the Second Isomorphism Theorem. Since we have an injection

$$N_2/N \cap \cdots \cap N_n/N \hookrightarrow M/N_1,$$

and since M/N_1 is $\mathfrak{p}$-coprimary, $N_2/N \cap \cdots \cap N_n/N$ is $\mathfrak{p}$-coprimary by Proposition 1.2. Thus by Proposition 1.3, we have injections

$$A/\mathfrak{p} \hookrightarrow N_2/N \cap \cdots \cap N_n/N \hookrightarrow M/N.$$

($\Leftarrow$) Now suppose we we have an injection $\iota : A/\mathfrak{p} \hookrightarrow M/N$. Consider the map

$$\begin{aligned} \varphi : M &\to M/N_1 \oplus \cdots \oplus M/N_n \\ m &\mapsto (m + N_1, \ldots, m + N_n) \end{aligned}$$

Clearly $\mathrm{Ker}(\varphi) = N$, and so we see that

$$\overline{\varphi} : M/N \hookrightarrow \bigoplus_{i=1}^{n} M/N_i$$

is an injection. For $i = 1, \ldots, n$ let $\pi_i : \bigoplus_{i=1}^n M/N_i \to M/N_i$ be the projection map onto the ith coordinate. Then we have the following commutative diagram:

$$\begin{array}{ccc} M/N & \xhookrightarrow{\overline{\varphi}} & \displaystyle\bigoplus_{i=1}^{n} M/N_i \\ \uparrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \pi_i} \\ A/\mathfrak{p} & \xrightarrow{\iota_i} & M/N_i \end{array}$$

We wish to show that ι_i is injective for some $i = 1, \ldots, n$. Suppose not, then $\mathrm{Ker}(\iota_i) \neq (0)$ for all i. Since $A/\mathfrak{p}$ is a domain,

$$(0) \neq \mathrm{Ker}(\iota_1) \cdots \mathrm{Ker}(\iota_n) \subseteq \mathrm{Ker}(\iota_1) \cap \cdots \cap \mathrm{Ker}(\iota_n) = \mathrm{Ker}(\overline{\varphi} \circ \iota).$$

This contradicts that $\overline{\varphi} \circ \iota$ is an injection. Thus $\iota_i : A/\mathfrak{p} \hookrightarrow M/N_i$ is an injection for some i. By assumption M/N_i is $\mathfrak{p}_i$-coprimary, so again by Proposition 1.3, we see that $A/\mathfrak{p}$ is $\mathfrak{p}_i$-coprimary. By Proposition 1.4, $\mathfrak{p} = \mathfrak{p}_i \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. ■

1.2.1 Primary Decomposition and Localization

Proposition 1.17 *Let M be a $\mathfrak{p}$-coprimary A-module and let U be a multiplicatively closed subset of A. The following hold:*

(1) *If $\mathfrak{p} \cap U = \varnothing$, then $U^{-1}M$ is $U^{-1}\mathfrak{p}$-coprimary.*

(2) *If $\mathfrak{p} \cap U \neq \varnothing$, then $U^{-1}M = 0$.*

Proof (1) We need to show if $\frac{a}{u} \in U^{-1}\mathfrak{p}$, then $U^{-1}M \xrightarrow{\frac{a}{u}} U^{-1}M$ is nilpotent. Since $\frac{1}{u}$ is a unit in $U^{-1}A$, we can assume $u = 1$. If $a \in \mathfrak{p}$, then $M \xrightarrow{a} M$ is nilpotent. So for some integer $n > 0$, $M \xrightarrow{a^n} M$ is the zero map. Thus $U^{-1}M \xrightarrow{a^n} U^{-1}M$ is the zero map.

If $a \notin \mathfrak{p}$, then $M \xrightarrow{a} M$ is injective. So $U^{-1}M \xrightarrow{a} U^{-1}M$ is injective by the exactness of localization.

(2) If $\mathfrak{p} \cap U \neq \varnothing$, then there is some $u \in \mathfrak{p} \cap U$. Since M is $\mathfrak{p}$-coprimary, $M \xrightarrow{u} M$ is nilpotent. So there is an integer $n > 0$ such that $M \xrightarrow{u^n} M$ is the zero map. Thus $U^{-1}M \xrightarrow{u^n} U^{-1}M$ is the zero map. Since u^n is a unit in $U^{-1}A$, multiplication by u^n is an isomorphism. Thus $U^{-1}M = (0)$. ■

Corollary 1.18 *If N is a $\mathfrak{p}$-primary submodule of M and $\mathfrak{p} \cap U = \varnothing$, then $U^{-1}N$ is a $\mathfrak{p}$-primary submodule of $U^{-1}M$.*

Theorem 1.19 *Let A be a Noetherian ring and suppose N is a proper submodule of a finitely generated A-module M. Let*

$$N = N_1 \cap \cdots \cap N_n$$

be a primary decomposition for N, where N_i is $\mathfrak{p}_i$-primary. Then

$$U^{-1}N = U^{-1}N_{i_1} \cap \cdots \cap U^{-1}N_{i_m}$$

is a primary decomposition of $U^{-1}N$ in $U^{-1}M$, where $m \leq n$ and $i_j \in \{1, \ldots, n\}$ for $j = 1, \ldots, m$.

Proof First note that if $N = N_1 \cap N_2$, then $U^{-1}N = U^{-1}N_1 \cap U^{-1}N_2$. To see this, consider the commutative diagram of exact sequences below.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & N_1 \cap N_2 & \longrightarrow & N_1 & \longrightarrow & N_1/(N_1 \cap N_2) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & N_2 & \longrightarrow & M & \longrightarrow & M/N_2 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & N_2/(N_1 \cap N_2) & \longrightarrow & M/N_1 & \longrightarrow & M/(N_1 + N_2) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

By tensoring this diagram with $U^{-1}A$ and by diagram chasing, the claim follows. Therefore, $U^{-1}N = U^{-1}N_1 \cap \cdots \cap U^{-1}N_n$. By Proposition 1.17, if $\{i_1, \ldots, i_m\}$ are the indices such that $\mathfrak{p}_{i_m} \cap U = \varnothing$, then $U^{-1}N = U^{-1}N_{i_1} \cap \cdots \cap U^{-1}N_{i_m}$. ■

Exercise 1.20 *Let T be a submodule of $U^{-1}M$. Show that there exists a submodule N of M such that $U^{-1}N = T$.*

Remark By Theorem 1.19 and the above exercise, we know how to find a primary decomposition of any submodule of $U^{-1}M$.

Lemma 1.21 *Suppose that $N \subsetneq M$ is $\mathfrak{p}$-primary and U is a multiplicatively closed set. Consider the canonical map:*

$$\begin{aligned} \eta : M &\to U^{-1}M \\ m &\mapsto \frac{m}{1} \end{aligned}$$

The following hold:

(1) *If $\mathfrak{p} \cap U = \varnothing$, then $\eta^{-1}(U^{-1}N) = N$.*

(2) *If* $\mathfrak{p} \cap U \neq \varnothing$, *then* $\eta^{-1}(U^{-1}N) = M$.

Proof (1) Let $x \in \eta^{-1}(U^{-1}N)$, thus $x/1 \in U^{-1}N$. Hence for some $y \in N$:

$$\frac{x}{1} = \frac{y}{u}$$

Thus there is an element $v \in U$ such that

$$\begin{aligned}(xu - y)v &= 0\\ xuv &= yv.\end{aligned}$$

From this we see that $xuv \in N$. Since U is multiplicatively closed, $uv \in U$. However,

$$\frac{M}{N} \xrightarrow{uv} \frac{M}{N}$$

is injective as M/N is $\mathfrak{p}$-coprimary and $uv \notin \mathfrak{p}$. Since $xuv \in N$ we see that $x \in N$. Thus $\eta^{-1}(U^{-1}N) \subseteq N$. The other containment is clear.

(2) This follows by Proposition 1.17. ■

Using the techniques of localization and the above lemma, we are able to say more about different primary decompositions of the same module:

Proposition 1.22 *Suppose*

$$N_1 \cap \cdots \cap N_n \qquad \text{and} \qquad N_1', \cap \cdots \cap N_n'$$

are two primary decompositions of $N \subsetneq M$ *where* N_i *and* N_i' *are* $\mathfrak{p}_i$*-primary. If* $\mathfrak{p}_i$ *is a minimal prime in* $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, *then* $N_i = N_i'$.

Proof Suppose $\mathfrak{p}_i$ is minimal in $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ and let $U = A - \mathfrak{p}_i$. Let $\eta : M \to U^{-1}M$ be the canonical map. Then

$$U^{-1}N = U^{-1}N_1 \cap \cdots \cap U^{-1}N_n = U^{-1}N_1' \cap \cdots \cap U^{-1}N_n'.$$

Since $\mathfrak{p}_i$ is minimal, $\mathfrak{p}_j \cap U \neq \varnothing$ for all $j \neq i$. Thus by Proposition 1.17, $U^{-1}N_i = U^{-1}N_i'$. Therefore by Lemma 1.21,

$$N_i = \eta^{-1}(U^{-1}N_i) = \eta^{-1}(U^{-1}N_i') = N_i'.$$

■

Definition Primes appearing in a primary decomposition that are not minimal are called the **embedded primes**.

Example 1.23 *Note that the preceding proposition guarantees that* $\mathfrak{p}$*-primary submodules in a primary decomposition are unique if* $\mathfrak{p}$ *is a minimal prime but this need not be the case if* $\mathfrak{p}$ *is an embedding prime. Consider* $I = (x^2, xy) \subseteq k[x, y] = A$. *Then* $I = (x) \cap (x^2, y) = (x) \cap (x^2, xy, y^2)$ *are two different primary decompositions of* I. *The minimal prime* (x) *corresponds to the* (x)*-primary component* (x) *and the embedding prime* (x, y) *corresponds to the* (x, y)*-primary ideals* (x^2, y) *and* $(x, y)^2$. *Thus* $\operatorname{Ass}(A/I) = \{(x), (x, y)\}$, *but the primary decompositions of* I *are not unique.*

Proposition 1.24 *Let U be a multiplicatively closed subset of A, and consider the canonical map:*

$$\eta : M \to U^{-1}M$$
$$m \mapsto \frac{m}{1}$$

Suppose N is a submodule of $U^{-1}M$ such that N is $U^{-1}\mathfrak{p}$-primary for some prime ideal $\mathfrak{p}$. Then $\eta^{-1}(N)$ is $\mathfrak{p}$-primary.

Proof Exercise. ■

Let $\mathfrak{p}$ be a prime ideal, and $\eta : A \to A_{\mathfrak{p}}$ is the canonical map:

$$\eta : A \to A_{\mathfrak{p}}$$
$$a \mapsto \frac{a}{1}$$

So $\mathfrak{p}^n A_{\mathfrak{p}}$ is a $\mathfrak{p}A_{\mathfrak{p}}$-primary ideal, since $\mathfrak{p}A_{\mathfrak{p}}$ is maximal in $A_{\mathfrak{p}}$. By Proposition 1.24, $\eta^{-1}(\mathfrak{p}^n A_{\mathfrak{p}})$ is $\mathfrak{p}$-primary.

Definition Using the above notation, $\eta^{-1}(\mathfrak{p}^n A_{\mathfrak{p}})$ is called the nth **symbolic power** of $\mathfrak{p}$ and is denoted by $\mathfrak{p}^{(n)}$. Note that $\mathfrak{p}^{(n)} \supseteq \mathfrak{p}^n$ and that $\mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary.

Exercise 1.25 *Can you find a prime ideal $\mathfrak{p}$ such that $\mathfrak{p}^n \neq \mathfrak{p}^{(n)}$? If so what is it? If not why not?*

1.2.2 Associated Primes

Definition Let A be a Noetherian ring and M be a finitely generated A-module. If $N = \bigcap_{i=1}^{n} N_i$ is a primary decomposition of $N \subseteq M$ such that N_i is $\mathfrak{p}_i$-primary, then the prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ are called the **essential primes** of N. If $N = 0$, then the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are called the **associated primes** of M and are denoted by $\mathrm{Ass}_A(M)$, or $\mathrm{Ass}(M)$ when there is no confusion.

The following are corollaries of the definition and theorems above:

Corollary 1.26 *Let A be a Noetherian ring and let M be a finitely generated A-module. Then $M = 0$ if and only if $\mathrm{Ass}_A(M) = \varnothing$.*

Corollary 1.27 *Let A be a Noetherian ring. Given a finitely generated A-module M, a submodule N is $\mathfrak{p}$-primary if and only if $\mathrm{Ass}_A(M/N) = \{\mathfrak{p}\}$.*

Corollary 1.28 *Let A be a Noetherian ring and M be a finitely generated A-module. A prime ideal $\mathfrak{p}$ is in $\mathrm{Ass}_A(M)$ if and only if there is an A-module homomorphism*

$$A/\mathfrak{p} \hookrightarrow M$$
$$1 + \mathfrak{p} \mapsto x,$$

where x is an element of M which is killed by $\mathfrak{p}$. Note that any $x \in M$ which is killed by $\mathfrak{p}$ defines an injection via the above map.

Exercise 1.29 *What is wrong with the following argument: Consider the polynomial ring $k[x, y]$ where k is a field. Since the prime ideal (x) is clearly (x)-primary, by Corollary 1.27:*

$$\mathrm{Ass}(k[x, y]/(x)) = \{(x)\}$$

However,

$$\frac{k[x, y]}{(x, y)} \cong k \hookrightarrow \frac{k[x, y]}{(x)}$$

and so by Corollary 1.28, $(x, y) \in \mathrm{Ass}(k[x, y]/(x))$. What!?

Definition A nonzero element $a \in A$ is called a **zerodivisor** on M if there exists a nonzero element $m \in M$ such that $am = 0$. A nonzero element $a \in A$ is called a **nonzerodivisor** on M if a is not a zerodivisor.

Corollary 1.30 *Let A be a Noetherian ring, M be a finitely generated nonzero A-module, and let*

$$D = \{a \in A : a \text{ is a zerodivisor on } M\}.$$

Then

$$D \cup \{0\} = \bigcup_{\mathfrak{p} \in \mathrm{Ass}_A(M)} \mathfrak{p}.$$

Proof ($\subseteq$) Clearly $0 \in \bigcup_{\mathfrak{p} \in \mathrm{Ass}_A(M)} \mathfrak{p}$, since $\mathrm{Ass}_A(M) \neq \varnothing$. Let $d \in D$, then there exists $m \in M$ with $m \neq 0$ and $dm = 0$. By the Primary Decomposition Theorem, we have that

$$(0) = N_1 \cap \cdots \cap N_n$$

where each submodule N_i of M is $\mathfrak{p}_i$-primary. Since $m \neq 0$, there exists $i = 1, \ldots, n$ such that $m \notin N_i$. Hence the image of m is nonzero in M/N_i. Since M/N_i is $\mathfrak{p}_i$-coprimary and since $M/N_i \xrightarrow{d} M/N_i$ is not injective,

$$d \in \mathfrak{p}_i \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i = \bigcup_{\mathfrak{p} \in \mathrm{Ass}_A(M)} \mathfrak{p}.$$

($\supseteq$) Suppose that a is a nonzero element of $\mathfrak{p} \in \mathrm{Ass}_A(M)$. We have an injection

$$\begin{aligned} A/\mathfrak{p} &\hookrightarrow M \\ 1 + \mathfrak{p} &\mapsto x \end{aligned}$$

where x is a nonzero element of M that is killed by $\mathfrak{p}$. Then $ax = 0$ in M and so $a \in D$. ■

Corollary 1.31 *Let A be a Noetherian ring and N be a submodule of a finitely generated A-module M. Then*

$$\mathrm{Ass}_A(N) \subseteq \mathrm{Ass}_A(M) \subseteq \mathrm{Ass}_A(N) \cup \mathrm{Ass}_A(M/N).$$

Proof If $\mathfrak{p} \in \mathrm{Ass}_A(N)$, then we have injections $A/\mathfrak{p} \hookrightarrow N \hookrightarrow M$. Thus $\mathfrak{p} \in \mathrm{Ass}_A(M)$. Now suppose $\mathfrak{p} \in \mathrm{Ass}_A(M)$. Then we have an injection $\iota : A/\mathfrak{p} \hookrightarrow M$.

Case 1. Suppose that $\iota(A/\mathfrak{p}) \cap N \neq (0)$. For any nonzero submodule $T \subseteq A/\mathfrak{p}$ and any nonzero $t \in T$, the map $A/\mathfrak{p} \xrightarrow{t} T$ is injective since $A/\mathfrak{p}$ is a domain. Since $T = \iota^{-1}(\iota(A/\mathfrak{p} \cap N)$ is a nonzero submodule of $A/\mathfrak{p}$, we have injections $A/\mathfrak{p} \hookrightarrow T \hookrightarrow N$. Thus $\mathfrak{p} \in \mathrm{Ass}_A(N)$.

Case 2. Suppose that $\iota(A/\mathfrak{p}) \cap N = (0)$. Then ι induces an injection $A/\mathfrak{p} \hookrightarrow M/N$ and so $\mathfrak{p} \in \mathrm{Ass}_A(M/N)$. ■

Corollary 1.32 *Let A be a Noetherian ring and M be a finitely generated A-module such that $M = M_1 \oplus M_2$. Then*

$$\mathrm{Ass}_A(M) = \mathrm{Ass}_A(M_1) \cup \mathrm{Ass}_A(M_2).$$

Theorem 1.33 (Prime Filtration Theorem) *Let A be a Noetherian ring. For any finitely generated, nonzero A-module M, there exists a filtration of M,*

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = (0),$$

such that for all $i = 1, \ldots, n$, $M_{i-1}/M_i \cong A/\mathfrak{p}_i$ where each $\mathfrak{p}_i$ is a prime ideal. Moreover, given any such filtration, $\mathrm{Ass}_A(M) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

Proof Let $\mathcal{S}$ be the collection of submodules of M that have a prime filtration as stated above. $\mathcal{S} \neq \varnothing$, since for any $\mathfrak{p} \in \mathrm{Ass}_A(M)$, we have an injection $\iota : A/\mathfrak{p} \hookrightarrow M$ so that $\iota(A/\mathfrak{p}) \in \mathcal{S}$. Since M is Noetherian, $\mathcal{S}$ has a maximal element, say M_0.

We claim $M = M_0$. Suppose not, then we have the exact sequence

$$0 \longrightarrow M_0 \longrightarrow M \xrightarrow{\varphi} M/M_0 \longrightarrow 0.$$

By assumption $M/M_0 \neq (0)$, so there exists a prime $\mathfrak{p}' \in \mathrm{Ass}_A(M/M_0)$. Thus we have an injection $j : A/\mathfrak{p}' \hookrightarrow M/M_0$. Set $T = j(A/\mathfrak{p}')$ and $Q = \varphi^{-1}(T)$. Then we have a new exact sequence

$$0 \longrightarrow M_0 \longrightarrow Q \longrightarrow T \longrightarrow 0.$$

Since M_0 has a prime filtration, and since $Q/M_0 \cong T \cong A/\mathfrak{p}'$, Q has a prime filtration. However, $Q \supsetneq M_0$ contradicts that M_0 is maximal in $\mathcal{S}$. Thus, we must have that $M = M_0$.

The second part of the theorem follows from Corollary 1.31. ■

Proposition 1.34 *Let A be a Noetherian ring, M be a finitely generated A-module, and $I = \mathrm{Ann}_A(M)$. Then any essential prime of I is an associated prime of M.*

Proof Since M is finitely generated, we may write $M = (\alpha_1, \ldots, \alpha_n)A$. Set $\varphi : A \to \bigoplus_{i=1}^n M$ defined by

$$a \mapsto (a\alpha_1, \ldots, a\alpha_n).$$

It's easy to see that $I = \mathrm{Ker}(\varphi)$, and thus $A/\mathrm{Ker}(\varphi) \hookrightarrow \bigoplus_{i=1}^{n} M$. By Corollary 1.31, it follows that

$$\mathrm{Ass}_A(A/I) \subseteq \mathrm{Ass}_A\left(\bigoplus_{i=1}^{n} M\right) \subseteq \mathrm{Ass}_A(M).$$

By definition, associated primes of A/I are essential primes of I. Thus essential primes of I are associated primes of M. ■

Remark The converse of the previous proposition is not true. For example, if $A = k[x, y]$ and $M = A/(x) \oplus A/(x, y)$. Then $\mathrm{Ann}_A(M) = (x)$, which is (x)-primary but that $\mathrm{Ass}(M) = \{(x), (x, y)\}$.

Remark Since essential primes of an ideal $I \subseteq A$ correspond to associated primes of the quotient ring A/I, we sometimes call these associated primes of I as well.

Proposition 1.35 *Let A be a Noetherian ring and M be a finitely generated A-module. Then*

$$\sqrt{\mathrm{Ann}_A(M)} = \bigcap_{\mathfrak{p} \in \mathrm{Ass}_A(M)} \mathfrak{p}.$$

Proof Exercise. ■

Proposition 1.36 *Let $\mathcal{P}$ be the collection of prime ideals of A that are minimal in $\mathrm{Ass}_A(A)$. Then*

$$\sqrt{0} = \bigcap_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}.$$

Proof Exercise. ■

Proposition 1.37 *Let A be a Noetherian ring, M be a finitely generated A-module, and $\mathfrak{p}$ be a prime ideal. The following are equivalent:*

(1) *$\mathfrak{p}$ is an essential prime ideal of a submodule N of M.*

(2) $M_{\mathfrak{p}} \neq 0$.

(3) $\mathfrak{p} \supseteq \mathrm{Ann}_A(M)$.

(4) $\mathfrak{p} \supseteq \mathfrak{q}$ *for some prime ideal* $\mathfrak{q} \in \mathrm{Ass}_A(M)$.

Proof Exercise. ■

Definition The set of prime ideals $\mathfrak{p}$ satisfying the four equivalent conditions above are called the **support** of M, denoted $\mathrm{Supp}_A(M)$.

Corollary 1.38 *Let A be a Noetherian ring and M be a finitely generated A-module. The minimal elements of $\mathrm{Ass}_A(M)$ are the minimal elements of $\mathrm{Supp}_A(M)$.*

Exercise 1.39 *Let A be a Noetherian ring and*

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

be an exact sequence of finitely generated A-modules. Show that

$$\mathrm{Supp}_A(M) = \mathrm{Supp}_A(M') \cup \mathrm{Supp}_A(M'').$$

Proposition 1.40 *Let A be a Noetherian ring and M be a finitely generated A-module. M has finite length if and only if $\mathrm{Ass}_A(M)$ consists of maximal ideals only.*

Proof ($\Rightarrow$) Suppose we have a composition series of M,

$$M = M_0 \subsetneq \cdots \subsetneq M_n = (0).$$

Then for $i = 1, \ldots, n$, $M_i/M_{i+1} \cong A/\mathfrak{m}_i$ for some maximal ideal $\mathfrak{m}_i$. Since every maximal ideal is a prime ideal, this is a prime filtration. Thus by the Prime Filtration Theorem, Theorem 1.33, $\mathrm{Ass}_A(M) \subseteq \{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$.

($\Leftarrow$) Now assume $\mathrm{Ass}_A(M)$ consists of maximal ideals only. By the Prime Filtration Theorem there is a prime filtration of M, say

$$M = M_0 \subsetneq \cdots \subsetneq M_n = (0).$$

Then for $i = 1, \ldots, n$, $M_i/M_{i+1} \cong A/\mathfrak{p}_i$ for some prime ideal $\mathfrak{p}_i$. We want to show $\mathfrak{p}_i$ is maximal for each i. So fix $\mathfrak{p} = \mathfrak{p}_i$. Then

$$(M_i/M_{i+1})_{\mathfrak{p}} \cong (A/\mathfrak{p})_{\mathfrak{p}} \neq (0).$$

Since $(M_i)_{\mathfrak{p}}/(M_{i+1})_{\mathfrak{p}} \cong (M_i/M_{i+1})_{\mathfrak{p}} \neq (0)$, we have that $(M_i)_{\mathfrak{p}} \neq (0)$. Moreover, $M_i \hookrightarrow M$ implies that $(M_i)_{\mathfrak{p}} \hookrightarrow M_{\mathfrak{p}}$ by the exactness of localization. Therefore $M_{\mathfrak{p}} \neq (0)$. By Proposition 1.37, $\mathfrak{p} \supseteq \mathfrak{q}$ for some prime ideal $\mathfrak{q} \in \mathrm{Ass}_A(M)$. ■

Corollary 1.41 (Finite Length Criteria) *Let $(A, \mathfrak{m})$ be a local ring and M a finitely generated A-module. Then the following are equivalent:*

(1) $\lambda(M) < \infty$.

(2) *M is Artinian and Noetherian.*

(3) $\mathrm{Supp}(M) = \mathrm{Ass}(M) = \{\mathfrak{m}\}$.

(4) *There exists $t \in \mathbb{N}$ such that $\mathfrak{m}^t M = 0$.*

1.3 Arbitrary Modules

In this section we assume our ring A is still Noetherian but A-modules are no longer assumed to be finitely generated.

Definition Let A be a Noetherian ring. A prime ideal $\mathfrak{p}$ is an **associated prime** of M if there exists an injection $A/\mathfrak{p} \hookrightarrow M$. We denote this set of primes by $\mathrm{Ass}_A(M)$.

Definition If $a \in A$, the map $M \xrightarrow{a} M$ is called **locally nilpotent** if for all $m \in M$, there is a positive integer n (possibly depending on m) such that $a^n m = 0$.

Definition Let A be a Noetherian ring. An A-module M is **$\mathfrak{p}$-coprimary** if the map $M \xrightarrow{a} M$ is locally nilpotent for all $a \in \mathfrak{p}$ and is injective for all $a \notin \mathfrak{p}$.

Definition Let A be a Noetherian ring. Given A-modules $N \hookrightarrow M$, N is a **$\mathfrak{p}$-primary** submodule of M if M/N is $\mathfrak{p}$-coprimary.

Note that these definitions agree those in the finitely generated case, and that the definition of a locally nilpotent map reduces to the definition of a nilpotent map for finitely generated modules.

Proposition 1.42 *Let A be a Noetherian ring. Given an A-module M, there are submodules $N(\mathfrak{p})$ such that*

$$(0) = \bigcap_{\mathfrak{p} \in \mathrm{Ass}_A(M)} N(\mathfrak{p})$$

where $N(\mathfrak{p})$ is $\mathfrak{p}$-primary.

Proof Fix $\mathfrak{p} \in \mathrm{Ass}_A(M)$. Let

$$\mathcal{S} = \{N : N \text{ is a submodule of } M \text{ and } \mathfrak{p} \notin \mathrm{Ass}_A(N)\}.$$

Note $\mathcal{S} \neq \varnothing$ since $(0) \in \mathcal{S}$. Since A is Noetherian, $\mathcal{S}$ has a maximal element, say $N(\mathfrak{p})$. We want to show that $N(\mathfrak{p})$ is $\mathfrak{p}$-primary. This is equivalent to saying

$$\mathrm{Ass}_A(M/N(\mathfrak{p})) = \{\mathfrak{p}\}.$$

Suppose that this is not the case, that is suppose there exists $\mathfrak{q} \in \mathrm{Ass}_A(M/N(\mathfrak{p}))$ and $\mathfrak{q} \neq \mathfrak{p}$. Then

$$A/\mathfrak{q} \cong M'/N(\mathfrak{p}) \subseteq M/N(\mathfrak{p}).$$

By Corollary 1.31

$$\mathrm{Ass}_A(N(\mathfrak{p})) \subseteq \mathrm{Ass}_A(M') \subseteq \mathrm{Ass}_A(M'/N(\mathfrak{p})) \cup \mathrm{Ass}_A(N(\mathfrak{p})).$$

But by assumption, $\mathfrak{p} \notin \mathrm{Ass}(N(\mathfrak{p}))$ and as $M'/N(\mathfrak{p}) \cong A/\mathfrak{q}$ and $\mathfrak{q}$ is $\mathfrak{q}$-primary, we have by Corollary 1.27 that $\mathrm{Ass}_A(M'/N(\mathfrak{p})) = \{\mathfrak{q}\}$. Thus $\mathfrak{p} \notin \mathrm{Ass}_A(M')$ which contradicts the maximality of $N(\mathfrak{p})$. Thus $N(\mathfrak{p})$ is $\mathfrak{p}$-primary. Furthermore, since

$$\mathrm{Ass}_A\left(\bigcap_{\mathfrak{p} \in \mathrm{Ass}_A(M)} N(\mathfrak{p})\right) = \varnothing$$

by construction, we have that $(0) = \bigcap_{\mathfrak{p} \in \mathrm{Ass}_A(M)} N(\mathfrak{p})$. ∎

Exercise 1.43 *Let A be a Noetherian ring and*

$$\mathcal{S} = \{I : I = \mathrm{Ann}_A(x) \text{ for some nonzero } x \in M\}.$$

Let J be a maximal element in $\mathcal{S}$. Show that J is a prime ideal. Moreover, conclude that $J \in \mathrm{Ass}_A(M)$.

Exercise 1.44 *Let $f : A \to B$ be a homomorphism of Noetherian rings. Let M be a finitely generated B-module. Show that*

$$\mathrm{Ass}_A(M) = \{f^{-1}(\mathfrak{p}) : \mathfrak{p} \in \mathrm{Ass}_B(M)\}.$$

Hence $\mathrm{Ass}_A(M)$ is finite even if M is not finitely generated over A.

Chapter 2

Filtrations and Completions

2.1 Limits

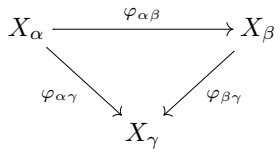
2.1.1 Direct Limits

Definition A nonempty set $\mathcal{I}$ is called a **directed set** if $(\mathcal{I}, \leq)$ is a partially ordered set such that for every $\alpha, \beta \in \mathcal{I}$ there exists $\gamma \in \mathcal{I}$ with $\alpha \leq \gamma$ and $\beta \leq \gamma$.

Definition A family of objects $(X_\alpha)_{\alpha \in \mathcal{I}}$ is a **direct system indexed by a directed set $\mathcal{I}$** if for every $\alpha, \beta \in \mathcal{I}$ with $\alpha \leq \beta$ there exists a morphism $\varphi_{\alpha\beta} : X_\alpha \to X_\beta$ such that:

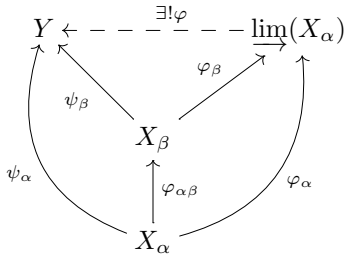
(1) $\varphi_{\alpha\alpha} = \mathbb{1}_{X_\alpha}$ for all $\alpha \in \mathcal{I}$.

(2) For any $\alpha, \beta, \gamma \in \mathcal{I}$ where $\alpha \leq \beta \leq \gamma$, the following diagram commutes:



Definition A **direct limit**, which is an example of a **colimit**, of a direct system $(X_\alpha)_{\alpha \in \mathcal{I}}$ is an object, denoted by $\varinjlim(X_\alpha)$, with morphisms $\varphi_\alpha : X_\alpha \to \varinjlim(X_\alpha)$ such that for every $\alpha, \beta \in \mathcal{I}$ with $\alpha \leq \beta$ we have $\varphi_\beta \circ \varphi_{\alpha\beta} = \varphi_\alpha$. Further, for every object Y with compatible morphisms $\psi_\alpha : X_\alpha \to Y$, there

exists a unique morphism φ making the diagram below commute for all $\alpha \leq \beta$:



Example 2.1 *If we consider the category of sets, where the morphisms are set inclusion, then given* $X_0 \subseteq X_1 \subseteq \cdots \subseteq X_n \subseteq \cdots$,

$$\varinjlim(X_i) = \bigcup_{i=0}^{\infty} X_i.$$

Example 2.2 *If* X_α *are Abelian groups, then*

$$\varinjlim(X_\alpha) = \frac{\bigoplus X_\alpha}{D},$$

where D *is the Abelian group generated by* $x'_\alpha - \varphi_{\alpha\beta}(x_\alpha)'$ *where* $x_\alpha \in X_\alpha$ *and* x'_α *and* $\varphi_{\alpha\beta}(x_\alpha)'$ *are the images of* x_α *and* $\varphi_{\alpha\beta}(x_i)$ *in* $\bigoplus X_\alpha$.

Exercise 2.3 *Suppose we have direct systems* $(A_\alpha)_{\alpha\in\mathcal{I}}$, $(B_\alpha)_{\alpha\in\mathcal{I}}$, *and* $(C_\alpha)_{\alpha\in\mathcal{I}}$, *over the directed set* $\mathcal{I}$ *and maps* $(\varphi_\alpha) : (A_\alpha) \to (B_\alpha)$ *and* $(\psi_\alpha) : (B_\alpha) \to (C_\alpha)$ *compatible with the direct systems, such that for every* $\alpha \in \mathcal{I}$

$$0 \longrightarrow A_\alpha \xrightarrow{\varphi_\alpha} B_\alpha \xrightarrow{\psi_\alpha} C_\alpha \longrightarrow 0$$

is exact. Then

$$0 \longrightarrow \varinjlim A_\alpha \xrightarrow{\varinjlim \varphi_\alpha} \varinjlim B_\alpha \xrightarrow{\varinjlim \psi_\alpha} \varinjlim C_\alpha \longrightarrow 0$$

is exact. In other words, direct limit is an exact functor from the category of direct systems of modules over a fixed directed set to the category of modules.

Exercise 2.4 *Let* U *be a multiplicatively closed set and* M *be an* A*-module. Let* M_u *denote* $\{1, u, u^2, \ldots\}^{-1}M$. *Note that the collection* $(M_u)_{u\in U}$ *forms a direct system since for any* $u, u' \in U$, *we have maps* $M_u \to M_{uu'}$ *and* $M_{u'} \to M_{uu'}$. *Show that* $U^{-1}M = \varinjlim(M_u)$.

Exercise 2.5 *Let* M *be an* A*-module. Show that* M *is the direct limit of its finitely generated submodules.*

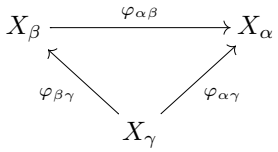
2.1.2 Inverse Limits

An inverse limit is the dual notion of a direct limit.

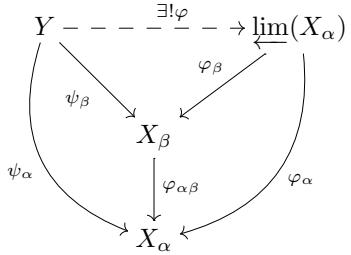
Definition A family of objects $(X_\alpha)_{\alpha\in\mathcal{I}}$ is a **inverse system indexed by a directed set $\mathcal{I}$** if for every $\alpha, \beta \in \mathcal{I}$ with $\alpha \leq \beta$ there exists a morphism $\varphi_{\alpha\beta} : X_\beta \to X_\alpha$ such that:

(1) $\varphi_{\alpha\alpha} = \mathbb{1}_{X_\alpha}$ for all $\alpha \in \mathcal{I}$.

(2) For any $\alpha, \beta, \gamma \in \mathcal{I}$, where $\alpha \leq \beta \leq \gamma$, the following diagram commutes:



Definition An **inverse limit**, which is an example of a **limit**, of a inverse system $(X_\alpha)_{\alpha\in\mathcal{I}}$, is an object, denoted by $\varprojlim(X_\alpha)$, with morphisms $\varphi_\alpha : \varprojlim(X_\alpha) \to X_\alpha$ such that for all $\alpha, \beta \in \mathcal{I}$ with $\alpha \leq \beta$ we have $\varphi_{\alpha\beta} \circ \varphi_\beta = \varphi_\alpha$. Further, for every object Y with compatible morphisms $\psi_\alpha : Y \to X_\alpha$, there exists a unique morphism φ making the diagram below commute for all $\alpha \leq \beta$:



Example 2.6 *If we consider the category of sets, where the morphisms are set inclusion, then given $X_0 \supseteq X_1 \supseteq \cdots \supseteq X_n \supseteq \cdots$,*

$$\varprojlim(X_i) = \bigcap_{i=0}^{\infty} X_i.$$

Example 2.7 *The inverse limit can be constructed as follows: For a given inverse system, $(X_\alpha)_{\alpha\in\mathcal{I}}$, write*

$$\varprojlim(X_\alpha) = \{(x_\alpha)_{\alpha\in\mathcal{I}} : \text{if } \alpha \leq \beta, \text{ then } x_\alpha = \varphi_{\alpha\beta}(x_\beta)\} \subseteq \prod_{\alpha\in\mathcal{I}} X_\alpha.$$

The reader should check that this construction agrees with the definition of an inverse limit.

We now will define the ring of formal power series as it will be very useful in this chapter:

Definition Given a ring A, we can form the ring of **formal power series** in $X_1, \ldots, X_n$ over A by considering all infinite sums of the form

$$\sum_{i=0}^{\infty} a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n}, \qquad \text{where} \qquad a_{i_1,\ldots,i_n} \in A.$$

Sums such as these form a ring under the canonical rules for summation and product. We denote the ring of formal power series over A in n variables by $A[\![X_1, \ldots, X_n]\!]$.

Exercise 2.8 *If $B = A[X_1, \ldots, X_n]$ and $I = (X_1, \ldots, X_n)$. Show (A/I^t) form an inverse system. Moreover, show that*

$$\varprojlim (B/I^n) \cong A[\![X_1, \ldots, X_n]\!].$$

Exercise 2.9 *Suppose we have inverse systems $(A_\alpha)_{\alpha\in\mathcal{I}}$, $(B_\alpha)_{\alpha\in\mathcal{I}}$, and $(C_\alpha)_{\alpha\in\mathcal{I}}$, over the directed set $\mathcal{I}$ and maps $(\varphi_\alpha) : (A_\alpha) \to (B_\alpha)$ and $(\psi_\alpha) : (B_\alpha) \to (C_\alpha)$ compatible with the inverse systems, such that for every $\alpha \in \mathcal{I}$*

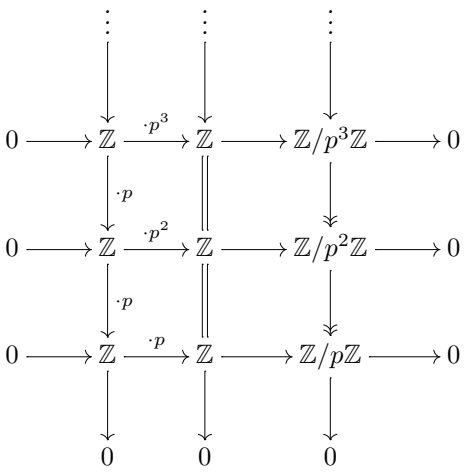
$$0 \longrightarrow A_\alpha \xrightarrow{\varphi_\alpha} B_\alpha \xrightarrow{\psi_\alpha} C_\alpha \longrightarrow 0$$

is exact. Then

$$0 \longrightarrow \varprojlim A_\alpha \xrightarrow{\varprojlim \varphi_\alpha} \varprojlim B_\alpha \xrightarrow{\varprojlim \psi_\alpha} \varprojlim C_\alpha$$

is exact. In other words, inverse limit is a left exact functor from the category of inverse systems of modules over a fixed directed set to the category of modules.

Example 2.10 *To see that inverse limits are not in general fully exact, consider the following commutative diagram with exact rows:*



Taking inverse limits along the columns, we get

$$0 \to 0 \to \mathbb{Z} \to \widehat{\mathbb{Z}}_p \to 0,$$

which is not exact. (Here $\widehat{\mathbb{Z}}_p$ denotes the p-adic integers.)

2.2 Filtrations and Completions

2.2.1 Topology and Algebraic Structures

Definition A group G is a **topological group** if there exists some topology on G such that the maps:

$$\begin{aligned} G \times G &\to G & \qquad G &\to G \\ (x, y) &\mapsto xy & \qquad x &\mapsto x^{-1} \end{aligned}$$

are both continuous maps.

Definition A ring A is a **topological ring** if there exists some topology on A such that the maps:

$$\begin{aligned} A \times A &\to A & \qquad A \times A &\to A \\ (a, b) &\mapsto a + b & \qquad (a, b) &\mapsto ab \end{aligned}$$

are both continuous maps.

Definition If A is a topological ring, an A-module M is a **topological module** if there exists some topology M such that the maps:

$$\begin{aligned} A \times A &\to A & \qquad A \times M &\to M \\ (x, y) &\mapsto x + y & \qquad (a, x) &\mapsto ax \end{aligned}$$

are both continuous maps.

Exercise 2.11 *Let G be a topological group with identity element e. If (N_α) is a system of basic neighborhoods of e, show that G is Hausdorff if and only if $\{e\} = \bigcap_\alpha N_\alpha$. Hint: A topological space is Hausdorff if and only if the diagonal is closed.*

2.2.2 Filtered Rings and Modules

Definition If A is a ring, we call a descending chain of additive subgroups

$$A = A_0 \supseteq A_1 \supseteq \cdots \supseteq A_n \supseteq \cdots$$

a **filtration** of A if

$$A_i A_j \subseteq A_{i+j}.$$

We say that a ring with a filtration is a **filtered ring**.

Remark Note that from the definition above, the fact that $A_i A_j \subseteq A_{i+j}$ necessitates that each A_i is an ideal of A.

Definition If A is a filtered ring with filtration (A_n) and M is an A-module, then M is a **filtered module** if

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

is a descending chain of subgroups of M such that

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

Remark Note that from the definition above, the fact that $A_i M_j \subseteq M_{i+j}$ necessitates that each M_j is a submodule of M.

Definition Let M be a filtered A-module with filtration (M_n) and let N be a submodule of M. Then setting $N_n = N \cap M_n$ forms a filtration for N. This is called the **induced filtration**.

Definition Let M be a filtered A-module with filtration (M_n) which surjects onto another A-module N via a module homomorphism

$$\varphi : M \twoheadrightarrow N.$$

Setting $N_n = \varphi(M_n)$, we obtain the **image filtration**.

Definition A module homomorphism $\varphi : M \to N$ of filtered modules is called a **filtered map** if

$$\varphi(M_n) \subseteq N_n.$$

Definition Suppose that $\varphi : M \to N$ is a filtered map. Then φ is called **strict** if:

$$\underbrace{\varphi(M_n)}_{\text{image filtration}} = \underbrace{\varphi(M) \cap N_n}_{\text{induced filtration}}$$

2.2.3 The Topology Corresponding to a Filtration

Let M be a filtered A-module—so A and M are both filtered. Treating (M_n) as a fundamental system of open subsets of (0) we can define a topology on M. For any $x \in M$, the fundamental system of neighborhoods around x is $(x + M_n)$.

Exercise 2.12 *Show that the topology defined above makes M a topological module.*

Thus by Exercise 2.11, M is Hausdorff if and only if

$$\bigcap_{n=1}^{\infty} M_n = 0.$$

Definition A function $d : M \times M \to [0, \infty)$ is called a **pseudometric** if:

(1) For all $x, y \in M$, $d(x, y) = d(y, x)$.

(2) For all $x, y, z \in M$, $d(x, y) + d(y, z) \geq d(x, z)$.

If in addition we have that for all $x, y \in M$, $d(x, y) = 0$ if and only if $x = y$, then d is called a **metric**.

If M has a topology defined by a filtration as above, one may define a pseudometric on M as follows: Fix any $c \in (0, 1)$. For any $x, y \in M$ define

$$d(x, y) := c^n,$$

where n is the integer such that $(x - y) \in M_n - M_{n+1}$; if no such integer exists, then set $d(x, y) = 0$. If M is Hausdorff, then we have defined a metric. We will define $\widehat{M}$ to be the completion of M with respect to the metric defined by the topology associated to the filtration. We have two different ways of constructing this completion:

First Construction Recall that a **Cauchy sequence** is a sequence $(x_n) \in M$ such that for all $\varepsilon > 0$ there exists N such that $n, m > N$ implies

$$d(x_n, x_m) < \varepsilon,$$

or in other words, for every N_0 there exists N such that $n, m > N$ implies that $x_n - x_m \in M_{N_0}$. Call a sequences which converges to zero a **null sequence**. Thus in our metric, a null sequence is a sequence (x_n) such that for every L there exists N such that $n > N$ implies that $x_n \in M_L$. We first construct $\widehat{M}$ as follows:

$$\widehat{M} := \{\text{Cauchy sequences in } M\}/\{\text{null sequences in } M\}$$

Second Construction Since M is a filtered module, let each M_n in the filtration be an open neighborhood of 0. Thus each M_n is also closed in M since

$$M - M_n = \bigcup_{x \notin M_n} (x + M_n),$$

which is a union of open sets. Then the quotient topology on M/M_n is the discrete topology since 0, and hence every point, is both open and closed. Thus M/M_n inherits the discrete topology from the quotient topology and is hence complete with respect to the metric associated to the given topology. Since the product of complete spaces is complete, $\prod_{n=0}^{\infty} M/M_n$ is complete under the product topology. Define

$$\begin{aligned}\widehat{M} :=& \varprojlim(M/M_n) = \{\overline{x}_n \in M/M_n : \text{if } n \leq m, \text{ then } \overline{x}_m \mapsto \overline{x}_n\} \\ &\subseteq \prod_{n=0}^{\infty} M/M_n.\end{aligned}$$

$\widehat{M}$ is then a closed subspace of a complete metric space and hence complete.

Exercise 2.13 *Check that the two constructions above for the completion of M are isomorphic as A-modules.*

Recall that for X a metric space and Y a subspace of X then $\widehat{Y} = \overline{\iota(Y)}$ where the bar denotes closure and ι is the inclusion map $\iota : X \to \widehat{X}$.

Exercise 2.14 *If M is a filtered module with filtration (M_n) and N is a submodule of M, then show*

$$\overline{N} = \bigcap_{n=0}^{\infty} (N + M_n)$$

where $\overline{N}$ is the closure of N in the filtered topology.

Exercise 2.15 *Let M be a filtered A-module. Show that the following are equivalent:*

(1) *M is Hausdorff.*

(2) $\bigcap_{n=0}^{\infty} M_n = 0$.

(3) *M is a metric space and not just a pseudometric space.*

Exercise 2.16 *If M is a filtered module with filtration (M_n), show that*

$$\widehat{M_n} = \overline{\iota(M_n)} = \{(\overline{x}_n) : \overline{x}_i = 0 \text{ for } i \leq n \text{ and } x_{n+i} \in M_n \text{ for } i \geq 1\} \subseteq \widehat{M}.$$

Proposition 2.17 *If M is a filtered A-module with filtration (M_n), and $\widehat{M}$ is its completion, then*

$$\widehat{M}/\widehat{M}_n \cong M/M_n$$

as A-modules. Moreover, $\bigcap_{n=0}^{\infty} \widehat{M_n} = 0$, so $\widehat{M}$ is Hausdorff even if M is not.

Proof Let $\pi_n : \prod_{n=0}^{\infty} M/M_n \to M/M_n$ denote the projection map. We leave it to the reader to check that by restricting π_n to $\widehat{M} \subseteq \prod_{n=0}^{\infty} M/M_n$ we have:

$$\mathrm{Ker}(\pi_n) \cong \widehat{M_n} \cong \varprojlim_t \left(\frac{M_n}{M_{n+t}} \right)$$

The second statement then follows easily. ■

Exercise 2.18 *If M is a complete filtered module then the series*

$$\sum_{i=0}^{\infty} x_n$$

converges if and only if $\lim_{n\to\infty}(x_n) = 0$.

Proposition 2.19 *If M is a complete filtered module, and N is a closed submodule of M, then M/N is complete in the quotient topology.*

Proof Let $(\overline{x}_n)$ be a Cauchy sequence in M/N where $\overline{x} = x + N$ for $x \in M$. So there is some increasing integer function $f : \mathbb{N} \to \mathbb{N}$ such that

$$\overline{x}_{n+1} - \overline{x}_n \in \overline{M}_{f(n)} = M_{f(n)} + N/N.$$

Thus $x_{n+1} - x_n = y_n + z_n$ for some $y_n \in N$ and $z_n \in M_{f(n)}$. Consider the sequence:

$$x_1, \quad x_1 + z_1, \quad x_1 + z_1 + z_2, \quad x_1 + z_1 + z_2 + z_3, \quad \dots$$

This is a Cauchy sequence in M. By hypothesis M is complete so the sequence has a limit, say x. Therefore

$$\overline{x} = \lim_{n\to\infty} (\overline{x}_1 + \overline{z}_1 + \cdots + \overline{z}_n) = \lim_{n\to\infty} \overline{x}_{n+1}.$$

■

Exercise 2.20 *Let A be a Noetherian ring. Let $\mathfrak{m}$ be a maximal ideal in A. Give A the $\mathfrak{m}$-adic topology and give $A_{\mathfrak{m}}$ the $\mathfrak{m}A_{\mathfrak{m}}$-adic topology. Show that $\widehat{A} \cong \widehat{A_{\mathfrak{m}}}$.*

2.2.4 Graded Rings and Modules

Definition A ring A is called a **graded ring** if it can be written as a direct sum of subgroups

$$\bigoplus_{n=0}^{\infty} A_n,$$

where $A_i A_j \subseteq A_{i+j}$. Further, elements of A_i are called **homogeneous** elements of degree i. Note also that a graded ring is a filtered ring with filtration (A'_n) where

$$A'_n = \sum_{i=n}^{\infty} A_i.$$

Definition If A is graded ring:

$$A = A_0 \oplus \underbrace{A_1 \oplus \cdots A_n \oplus \cdots}_{A_+}$$

Then A_+ is called the **irrelevant ideal** of A.

Exercise 2.21 *Show that:*

(1) $1_A \in A_0$.

(2) *A_0 is a ring.*

(3) *A is Noetherian if and only if A_0 is Noetherian and A_+ is a finitely generated ideal of A.*

Definition A module M is called a **graded module** if it can be written as a direct sum of subgroups

$$\bigoplus_{n=0}^{\infty} M_n,$$

where $A_i M_j \subseteq M_{i+j}$.

Definition Given a filtered ring A with the filtration (A_n), the **graded ring associated to the filtration** is defined to be

$$\mathrm{Gr}(A) := \bigoplus_{i=0}^{\infty} A_i/A_{i+1}$$

Definition Given a filtered module M with the filtration (M_n), the **graded module associated to the filtration** is defined to be

$$\mathrm{Gr}(M) := \bigoplus_{i=0}^{\infty} M_i/M_{i+1}$$

Remark Since $\widehat{M}/\widehat{M_n} \cong M/M_n$,

$$\mathrm{Gr}(\widehat{A}) \cong \mathrm{Gr}(A),$$
$$\mathrm{Gr}(\widehat{M}) \cong \mathrm{Gr}(M).$$

Exercise 2.22 *Let A be a filtered ring that is Hausdorff under the given filtration. Show that if $\mathrm{Gr}(A)$ is an integral domain, then so is A.*

Example 2.23 *It is possible that A is a domain, while $\mathrm{Gr}(A)$ and $\widehat{A}$ are not. Consider $A = k[x,y]/(y^2 - x^2 - x^3)$. Since $y^2 - x^2 - x^3$ is irreducible, A is a domain. Similarly $A_{\mathfrak{m}}$ is also a domain, where $\mathfrak{m} = (x,y)A$. However, we will see later that $\widehat{A}$ is flat over A and so $\widehat{A} = k[\![x,y]\!]/(y^2 - x^2 - x^3)$.*

Proposition 2.24 *Let A be a filtered ring and M, M', M'' be filtered A-modules. If*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

is exact and f and g are strict, that is,

$$f(M'_n) = f(M') \cap M_n \qquad \text{and} \qquad g(M_n) = g(M) \cap M''_n,$$

then

$$0 \longrightarrow \mathrm{Gr}(M') \xrightarrow{\mathrm{Gr}\, f} \mathrm{Gr}(M) \xrightarrow{\mathrm{Gr}\, g} \mathrm{Gr}(M'') \longrightarrow 0$$

is exact.

Proof Clearly we have $\mathrm{Im}(\mathrm{Gr}\, f) \subseteq \mathrm{Ker}(\mathrm{Gr}\, g)$ since $\mathrm{Im}(f) \subseteq \mathrm{Ker}(g)$.

So let $\overline{x} \in \mathrm{Ker}(\mathrm{Gr}\, g)$. We can assume that $\overline{x} \in M_n/M_{n+1}$ for some n since any $\overline{x}$ is a finite sum of such homogeneous elements. So $g(\overline{x}) \in M'_{n+1} \cap$

$g(M) = g(M_{n+1})$ by the strictness of g. So there exists $x_{n+1} \in M_{n+1}$ such that $g(x) = g(x_{n+1})$. So $g(x - x_{n+1}) = 0$. Since

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

is exact, there exists $y \in M_n$ such that $f(y) = x - x_{n+1} \in f(M_n)$ by the strictness of f. Hence $(\operatorname{Gr} f)(\overline{y}) = \overline{x}$ and so $\operatorname{Ker}(\operatorname{Gr} g) \subseteq \operatorname{Im}(\operatorname{Gr} f)$ also. To see the injection and surjection on the ends, simply repeat the argument modifying it as necessary. ■

Theorem 2.25 *Let M be a complete filtered module and let N be a Hausdorff filtered module. If f is a filtered map and*

$$\operatorname{Gr} f : \operatorname{Gr}(M) \twoheadrightarrow \operatorname{Gr}(N)$$

is surjective, then f is onto and strict. Moreover, N is complete.

Proof Let $y \in N$. Since N is Hausdorff, there is a $n \in \mathbb{N}$ such that $y \in N_n - N_{n+1}$. By assumption $f_n : M_n/M_{n+1} \to N_n/N_{n+1}$ is onto for all n. So there exists $x_n \in M_n$ such that $\overline{f(x_n)} = \overline{y}$ in N_n/N_{n+1}, that is there exists $y_{n+1} \in N_{n+1}$ with $y_{n+1} = y - f(x_n)$. We may apply the same argument to y_{n+1} to get $x_{n+1} \in M_{n+1}$ such that $\overline{f(x_{n+1})} = \overline{y_{n+1}}$ in N_{n+1}/N_{n+2}. Continuing in this way we obtain a sequence $(x_i)_{i \geq 0}$ with $x_i \in M_{n+i}$ such that

$$y - f(x_n) - f(x_{n+1}) - \cdots - f(x_{n+i}) \in N_{n+i+1}$$

for all i. Since $\lim_{n\to\infty}(x_n) = 0$, the following sum

$$x = \sum_{i=0}^{\infty} x_{n+i}$$

converges. We leave it to the reader to check that $x \in M_n$ and $f(x) = y$. Thus f is onto, N is complete, and $f(M_n) = N_n$ so f is strict. ■

Corollary 2.26 *Suppose A is complete, and M is a Hausdorff filtered A-module. Suppose further that $\operatorname{Gr}(M)$ is a finitely generated $\operatorname{Gr}(A)$-module. Let $x_1, \ldots, x_d$ be elements of M such that their images generate $\operatorname{Gr}(M)$. Then M is generated by $x_1, \ldots, x_d$ and M is complete.*

Proof Because we can find homogeneous generators of a graded module over a graded ring, let $x_1, \ldots, x_d \in M$ such that $x_i \in M_{n_i} - M_{n_{i+1}}$ and such that $x_1, \ldots, x_d$ generate $\operatorname{Gr}(M)$ over $\operatorname{Gr}(A)$. So we have an onto map

$$\begin{aligned} f : A^d &\twoheadrightarrow M \\ e_i &\mapsto x_i \end{aligned}$$

We can define a filtration on A^d by setting

$$(Ae_i)_j = \begin{cases} Ae_i & \text{if } j \leq n_i \\ A_{j-n_i} e_i & \text{if } j > n_i. \end{cases}$$

This filtration guarantees that f is a filtered map. Since $\mathrm{Gr}(f)$ is onto by construction, the previous theorem tells us that f is onto and that M is complete. Moreover, M is generated by $x_1, \ldots, x_d$ over A. ■

Corollary 2.27 *Let A be complete and M be Hausdorff. If $\mathrm{Gr}(M)$ is Noetherian, then so is M.*

Proof Take $N \subseteq M$ to be any submodule. Set $N_n = N \cap M_n$. Then the map

$$\mathrm{Gr}(N) \to \mathrm{Gr}(M)$$

is injective by Proposition 2.24. Since $\mathrm{Gr}(M)$ is Noetherian, $\mathrm{Gr}(N)$ is finitely generated. By the previous corollary, N is finitely generated. ■

Corollary 2.28 *Let A be complete and M be Hausdorff. If $\mathrm{Gr}(M)$ is Noetherian, then every submodule of M is closed in M.*

Proof By the previous corollary, every submodule of M is finitely generated and complete. Since every complete subspace of a Hausdorff space is complete, we are done by Corollary 2.26. ■

2.3 Adic Completions and Local Rings

One of the most useful filtrations is the I-adic filtration.

Definition If M is an A-module and I is an ideal of A, then the ***I*-adic filtration** is the filtration:

$$M \supseteq IM \supseteq I^2M \supseteq \cdots \supseteq I^nM \supseteq \cdots$$

In other words, the filtration (M_n) is given by $M_n = I^nM$.

Definition If I is an ideal of A, then we denote the associated graded ring by

$$\mathrm{Gr}_I(A) := \bigoplus_{i=0}^{\infty} I^i/I^{i+1}.$$

Similarly, given an A-module M, we have the associated graded module

$$\mathrm{Gr}_I(M) := \bigoplus_{i=0}^{\infty} I^iM/I^{i+1}M.$$

Definition If M is complete with respect to the metric defined by the I-adic filtration, then we say that M is ***I*-adically complete**.

Definition If M is an A-module, the ***I*-adic completion** is given by

$$\widehat{M} := \varprojlim (M/I^nM).$$

If $(A, \mathfrak{m})$ is a local ring and M is an A-module, then by the **completion** of M, denoted $\widehat{M}$, we mean the $\mathfrak{m}$-adic completion of M.

Exercise 2.29 *If $B = A[X_1, \ldots, X_n]$ and $I = (X_1, \ldots, X_n)$, show that the I-adic completion of B is*

$$\widehat{B} = \varprojlim(B/I^n) \cong A[\![X_1, \ldots, X_n]\!].$$

Exercise 2.30 *If p is a prime in $\mathbb{Z}$, show that the p-adic integers are:*

$$\widehat{\mathbb{Z}}_p \cong \varprojlim(\mathbb{Z}/p^n\mathbb{Z})$$

Exercise 2.31 *To further understand what is going on, show that:*

$$\mathbb{C}[X] \subseteq \mathbb{C}[X]_{(X)} \subseteq \mathbb{C}\{X\} \subseteq \mathbb{C}[\![X]\!] = \widehat{\mathbb{C}[X]}$$

where $\mathbb{C}\{X\}$ is the set of all convergent power series with respect to the (X)-adic metric.

As an additional corollary to Theorem 2.25 we have:

Corollary 2.32 *If A is a ring with a finitely generated ideal I such that:*

(1) *A is I-adically complete and Hausdorff, and*

(2) *A/I is Noetherian.*

Then A is Noetherian.

Proof If I is generated by $x_1, \ldots, x_d$, then $\mathrm{Gr}_I(A)$ is a quotient of the polynomial ring $(A/I)[X_1, \ldots, X_d]$, and hence Noetherian. Thus A is Noetherian by Corollary 2.26. ■

While many of the following theorems will be stated for nonlocal rings, and I-adic completions, the reader should be aware that the case of a local ring with the $\mathfrak{m}$-adic completion is often most important.

Lemma 2.33 (Artin-Rees) *If A is Noetherian with an ideal I, and M is a finitely generated A-module with submodule N, then there exists $m \geq 0$ such that*

$$N \cap I^{m+n}M = I^n(N \cap I^m M)$$

for all $n \geq 0$.

Proof Note in the above theorem it is always true that

$$N \cap I^{m+n}M \supseteq I^n(N \cap I^m M).$$

For the other containment, set

$$\widetilde{A} = A \oplus I \oplus I^2 \oplus \cdots,$$

$$\widetilde{M} = M \oplus IM \oplus I^2M \oplus \cdots,$$

and

$$\widetilde{N} = N \oplus N \cap IM \oplus N \cap I^2M \oplus \cdots .$$

Since A is Noetherian, I is finitely generated and hence $\widetilde{A}$ is Noetherian as we can surject $A[X]$ onto $\widetilde{A}$. Since M is finitely generated over A, $\widetilde{M}$ is finitely generated over $\widetilde{A}$, and hence is also Noetherian. Thus $\widetilde{N}$ is finitely generated over $\widetilde{A}$. We may choose generators of $\widetilde{N}$, $\eta_1, \ldots, \eta_k$, such that each is of homogeneous degree $d_1, \ldots, d_k$ respectively, that is to say, $\eta_i \in N \cap I^{d_i}M$. Set

$$m = \max\{d_1, \ldots, d_k\}.$$

Suppose $x \in N \cap I^{m+n}M$ for $n \geq 0$. Then we may write

$$x = a_1\eta_1 + a_2\eta_2 + \cdots + a_k\eta_k$$

where $\deg(a_i) = m + n - d_i \geq n$. Thus $a_i \in I^n$. So we can write

$$x = b(a_1'\eta_1 + \cdots + a_k'\eta_k)$$

where $b \in I^n$ and $a_i = ba_i'$. Therefore $N \cap I^{m+n}M \subseteq I^n(N \cap I^mM)$. ■

Definition Let A be a ring and M be an A-module with filtration (M_n). We say the filtration (M_n) is ***I*-good** if there exists an integer j such that for all $i \geq 0$:

$$M_{i+j} = I^iM_j$$

Remark The Artin-Rees Lemma implies that if $N \subseteq M$, and M is I-adically filtered, then the induced filtration on N, $(N \cap I^nM)$, is I-good. Thus (I^nN) and $(N \cap I^nM)$ define the same topology on N and hence the completion of N with respect to the two topologies are identical.

Exercise 2.34 *Show that if A is I-adically complete, then $I \subseteq \mathfrak{J}(A)$.*

Corollary 2.35 *Let $(A, \mathfrak{m}, k)$ be a local ring. If M is a finitely generated A-module, then*

$$\begin{aligned}\boldsymbol{\mu}(M) :=& \{\textit{the minimal number of generators of } M\} \\ =& \operatorname{rank}_k(M/\mathfrak{m}M).\end{aligned}$$

Proof Consider a k-basis $\{\overline{b}_1, \ldots, \overline{b}_n\}$ of $M \otimes_A k$. We claim that $\{b_1, \ldots, b_n\}$ is a minimal set of generators for M. Write

$$M = \sum_{i=1}^{n} b_iA + \mathfrak{m}M$$

Setting $\overline{M} = M/\sum_{i=1}^{n} b_iA$ we then have $\overline{M} = \mathfrak{m}\overline{M}$, and so by Corollary 0.29, Nakayama's Lemma, we see that $M = \sum_{i=1}^{n} b_iA$. To see that this is minimal, suppose that it is not, then we have $\sum_{i=1}^{n-1} c_iA = M$. But now $\{\overline{c}_1, \ldots, \overline{c}_{n-1}\}$ form a basis for $M \otimes_A k$, a contradiction as $M \otimes_A k$ is a free module of rank n. ■

Compare Corollary 2.35 with the following exercise:

Exercise 2.36 *Let $(A, \mathfrak{m}, k)$ be a complete local ring and let M be a Hausdorff A-module. Suppose there exist $x_1, \ldots, x_n \in M$ such that $\overline{x}_1, \ldots, \overline{x}_n$ generate $M/\mathfrak{m}M$ over $A/\mathfrak{m}$. Then $x_1, \ldots, x_n$ generate M over A. In particular if $\operatorname{rank}_k(M/\mathfrak{m}M) < \infty$, then M is finitely generated over A. Hint: Consider Corollary 2.26.*

To see how the Krull Intersection Theorem gets its namesake read the following corollaries:

Corollary 2.37 *Let A be a Noetherian ring and $I \subseteq \mathfrak{J}(A)$. If M is finitely generated, then*

$$\bigcap_{n=1}^{\infty} I^n M = 0.$$

Proof Let $N = \bigcap_{i=1}^{\infty} I^n M$. By the Artin-Rees Lemma, Lemma 2.33, there exists $k > 0$ such that for all n we have

$$N = N \cap I^{n+k} M = I^n (N \cap I^k M) = I^n N.$$

Thus by Nakayama's Lemma, $N = 0$. ■

Corollary 2.38 *Let A be a domain. If I is a proper ideal of A, then*

$$\bigcap_{n=1}^{\infty} I^n = 0.$$

Proof Let $J = \bigcap I^n$. Then we have $J = IJ$. By Krull's Intersection Theorem, Theorem 0.28, there exists $a \in I$ such that $(1 - a)J = 0$. Since A is a domain and since I is proper we must have that $J = 0$. ■

Exercise 2.39 *Let A be a Noetherian ring and let $I \subseteq J$ be two ideals of A. Suppose that A is J-adically complete. Show that A is also I-adically complete.*

Lemma 2.40 *If A is Noetherian with an ideal I and*

$$0 \to N \to M \to T \to 0$$

is an exact sequence of finitely generated A-modules, then

$$0 \to \widehat{N} \to \widehat{M} \to \widehat{T} \to 0$$

is exact, where $\widehat{(-)}$ denotes I-adic completion.

Proof By the Artin-Rees Lemma, Lemma 2.33, $(I^n N)$ and $(N \cap I^n M)$ define the same topology on N. Hence the completions are identical. For all n we have the following exact sequence

$$0 \longrightarrow N/(N \cap I^n M) \xrightarrow{f_n} M/I^n M \xrightarrow{g_n} T/I^n T \longrightarrow 0.$$

Since by Exercise 2.9, taking the inverse limit of an inverse system of exact sequences is left exact, we get the following exact sequence by Proposition 2.24:

$$0 \longrightarrow \varprojlim N/(N \cap I^n M) \xrightarrow{f} \varprojlim M/I^n M \xrightarrow{g} \varprojlim T/I^n T.$$

This can also be checked directly and in fact, the last map is onto. To see this take $(x_n) \in \varprojlim T/I^n T$. We build a preimage of (x_n) by induction. Suppose we have $(y_i)_{1 \leq i \leq n}$ where $y_i \in M/I^n M$ and such that $g_n(y_i) = x_i$. By the above remarks we have the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N/N \cap I^{n+1}M & \xrightarrow{f_{n+1}} & M/I^{n+1}M & \xrightarrow{g_{n+1}} & T/I^{n+1}T & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \varphi} & & \downarrow & & \\ 0 & \longrightarrow & N/N \cap I^{n}M & \xrightarrow{f_{n}} & M/I^{n}M & \xrightarrow{g_{n}} & T/I^{n}T & \longrightarrow & 0. \end{array}$$

Note that the vertical maps are all surjective. Using this fact, a simple diagram chasing argument produces $y_{n+1} \in M/I^{n+1}M$ such that $\varphi(y_{n+1}) = y_n$ and $g_{n+1}(y_{n+1}) = x_{n+1}$. So by induction we get $(y_n) \in \varprojlim M/I^n M$ that maps to (x_n) via g. ■

WARNING 2.41 *If A is not Noetherian and I is an ideal in A, then the I-adic completion is in general neither left nor right exact.*

Corollary 2.42 *If A is Noetherian with A-modules M and N, and I is an ideal of A, then*

$$\widehat{M}/\widehat{N} \cong \widehat{M/N},$$

where $\widehat{(-)}$ denotes I-adic completion.

Proof This follows from Lemma 2.40. ■

Proposition 2.43 *Let A be a Noetherian ring and I is an ideal of A. If M is a finitely generated A-module and $\widehat{A}$ and $\widehat{M}$ denote the I-adic completion, then*

$$\widehat{M} \cong M \otimes_A \widehat{A}.$$

Proof Consider the map

$$\begin{aligned} \varphi : M \otimes_A \widehat{A} &\to \widehat{M}, \\ x \otimes (a_n) &\mapsto (a_n x). \end{aligned}$$

Note that using the properties of direct sums and inverse limits we get that $\bigoplus_{i=1}^n \widehat{A} \cong \widehat{(\bigoplus_{i=1}^n A)}$. Suppose M is generated by d elements. Then there is an exact sequence of the form

$$A^s \to A^d \to M \to 0.$$

Then we have the following commutative diagram with exact rows

$$\begin{array}{ccccccc} A^s \otimes_A \widehat{A} & \longrightarrow & A^r \otimes_A \widehat{A} & \longrightarrow & M \otimes_A \widehat{A} & \longrightarrow & 0 \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \theta} & & \\ \widehat{A^s} & \longrightarrow & \widehat{A^r} & \longrightarrow & \widehat{M} & \longrightarrow & 0. \end{array}$$

The exactness of the first row follows from the fact that $- \otimes_A \widehat{A}$ is a right exact functor. The exactness of the second row follows from Lemma 2.40. Since φ and ψ are isomorphisms, θ is also an isomorphism by the Five Lemma. ■

Theorem 2.44 *Let A be Noetherian and I an ideal of A. If $\widehat{A}$ is the I-adic completion of A, then*

$$A \to \widehat{A}$$

is flat. That is, $\widehat{A}$ is a flat A-module.

Proof This is clear in light of the previous propositions. ■

Corollary 2.45 *Let M be a finitely generated A-module and let $N_1, N_2 \subseteq M$ be submodules. Then*

(1) $\widehat{N_1 \cap N_2} = \widehat{N_1} \cap \widehat{N_2}$

(2) $\widehat{N_1 + N_2} = \widehat{N_1} + \widehat{N_2}$

Exercise 2.46 *Let $\widehat{A}$ be the I-adic completion of A for I a proper ideal of A. Then*

(1) *For any ideal J of A, $\widehat{J} \cong J\widehat{A}$.*

(2) $\widehat{I} \subseteq \mathfrak{J}(\widehat{A})$.

(3) *The maximal ideals of $\widehat{A}$ are in bijective correspondence with the maximal ideals of A that contain I. Further, if $\mathfrak{m}$ is a maximal ideal with $I \not\subseteq \mathfrak{m}$. Then $\widehat{\mathfrak{m}} = \widehat{A}$.*

2.4 Faithfully Flat Modules

Definition If A is a ring and M is an A-module we call M **faithfully flat** if it satisfies any of the equivalent conditions of the following theorem.

Theorem 2.47 *If A is a ring and M is an A-module then the following are equivalent:*

(1) *The sequence of A-modules*

$$N' \to N \to N''$$

is exact if and only if

$$M \otimes_A N' \to M \otimes_A N \to M \otimes_A N''$$

is exact.

(2) *The sequence of A-modules*

$$0 \to N' \to N \to N'' \to 0$$

is exact if and only if

$$0 \to M \otimes_A N' \to M \otimes_A N \to M \otimes_A N'' \to 0$$

is exact.

(3) *M is A-flat and for all A-modules N,*

$$M \otimes_A N = 0 \qquad \Rightarrow \qquad N = 0.$$

(4) *M is A-flat and for all ideals I of A,*

$$M \otimes_A A/I = 0 \qquad \Rightarrow \qquad A = I.$$

(5) *M is A-flat and for all maximal ideals $\mathfrak{m}$ of A,*

$$\mathfrak{m}M \subsetneq M.$$

Proof (1) $\Rightarrow$ (2) Obvious.

(2) $\Rightarrow$ (3) Clearly condition (2) implies that M is A-flat. Consider the sequence of A-modules $0 \to N \to 0$. Then

$$\begin{aligned} N = 0 &\Leftrightarrow 0 \to N \to 0 \text{ is exact,} \\ &\Leftrightarrow 0 \to N \otimes_A M \to 0 \text{ is exact,} \\ &\Leftrightarrow M \otimes_A N = 0. \end{aligned}$$

(3) $\Rightarrow$ (4) Take $N = A/I$.

(4) $\Rightarrow$ (5) Let $\mathfrak{m}$ be a maximal ideal. Since $\mathfrak{m} \subsetneq A$ we must have that $M/\mathfrak{m} \cong M \otimes_A A/\mathfrak{m} \neq 0$. Thus $\mathfrak{m}M \subsetneq M$.

(5) $\Rightarrow$ (3) Let N be a nonzero A-module. We must show that $M \otimes_A N \neq 0$. Let $0 \neq x \in N$ and define

$$\begin{aligned} \varphi : A &\to N, \\ a &\mapsto a \cdot x. \end{aligned}$$

Let $I = \mathrm{Ker}(\varphi)$. If I is a proper ideal we can find a maximal ideal $\mathfrak{m}$ containing I. Then

$$IM \subseteq \mathfrak{m}M \subsetneq M.$$

Thus $M/IM \neq 0$ and we have an injection $A/I \hookrightarrow N$. Since M is flat, $M/IM \hookrightarrow M \otimes_A N$. Therefore $M \otimes_A N \neq 0$.

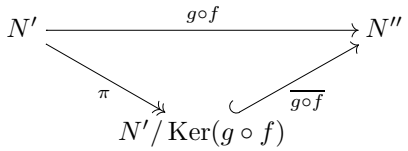
(3) $\Rightarrow$ (1) Now suppose that we have a sequence of modules

$$N' \xrightarrow{f} N \xrightarrow{g} N''$$

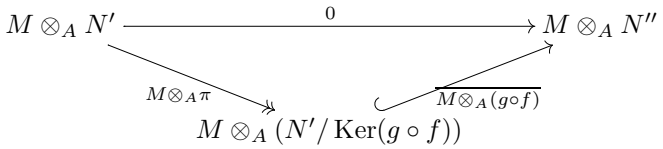
and that

$$M \otimes_A N' \xrightarrow{M\otimes_A f} M \otimes_A N \xrightarrow{M\otimes_A g} M \otimes_A N''$$

is exact. We have the following commutative diagram:

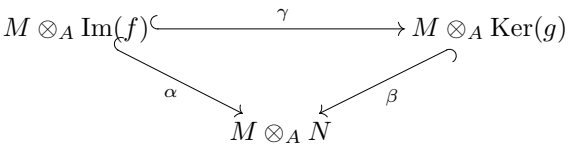


Since M is flat and since $M \otimes_A (g \circ f) = 0$ we get the following commutative diagram after applying $M \otimes_A -$:



Therefore $M \otimes_A (N'/\operatorname{Ker}(g \circ f)) = 0$. By assumption then $N/\operatorname{Ker}(g \circ f) = 0$. So $\operatorname{Ker}(g \circ f) = N$ and thus $g \circ f = 0$.

Now set $X = \operatorname{Im}(M \otimes_A f) = \operatorname{Ker}(M \otimes_A g)$. Since $\operatorname{Im}(f) \subseteq \operatorname{Ker}(g) \subseteq N$ and since M is flat we have the following commutative diagram



In $M \otimes_A N$ we have then

$$X \subseteq \operatorname{Im}(\alpha) \subseteq \operatorname{Im}(\beta) \subseteq X.$$

Therefore $\operatorname{Im}(\alpha) = \operatorname{Im}(\beta)$ and so

$$0 \to M \otimes_A \operatorname{Im}(f) \to M \otimes_A \operatorname{Ker}(g) \to 0$$

is an exact sequence. Therefore so is

$$0 \to \operatorname{Im}(f) \to \operatorname{Ker}(g) \to 0.$$

Therefore $\operatorname{Im}(f) = \operatorname{Ker}(g)$, and original sequence is exact. ■

Example 2.48 *If F is a free A-module, then F is faithfully flat. To see this note*

$$F = \bigoplus_{\alpha \in \mathcal{I}} A_\alpha$$

and so if

$$0 = F \otimes_A N = \bigoplus_{\alpha \in \mathcal{I}} N$$

we see that $N = 0$. In particular, this means that polynomials rings over A are faithfully flat.

WARNING 2.49 *Recall that a module M is called* ***faithful*** *if*

$$\mathrm{Ann}_A(M) = 0.$$

It should be easy to see that if an A-module is faithfully flat, then it is both faithful and flat over A. However, the converse is ***not*** *true! Consider $\mathbb{Q}$ as a $\mathbb{Z}$-module. We know that $\mathbb{Q}$ is $\mathbb{Z}$-flat, and $\mathrm{Ann}_{\mathbb{Z}}(\mathbb{Q}) = 0$ so $\mathbb{Q}$ is faithful, however*

$$\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0 \qquad \textit{but} \qquad \mathbb{Z}/3\mathbb{Z} \neq 0.$$

Hence $\mathbb{Q}$ is not faithfully flat over $\mathbb{Z}$.

Lemma 2.50 *If*

$$0 \to M \to N \to P \to 0$$

is an exact sequence of A-modules and if P is flat, then for any module T

$$0 \to T \otimes_A M \to T \otimes_A N \to T \otimes_A P \to 0$$

is exact.

Proof Let T be any A-module. Let F be a free module that maps surjectively onto T so that we have the exact sequence

$$0 \to K \to F \to T \to 0.$$

Then we have the following commutative diagram

$$\begin{array}{ccccccccc}
 & & & & 0 & & & & \\
 & & & & \downarrow & & & & \\
 & & K \otimes_A M & \longrightarrow & K \otimes_A N & \longrightarrow & K \otimes_A P & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & F \otimes_A M & \longrightarrow & F \otimes_A N & \longrightarrow & F \otimes_A P & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & T \otimes_A M & \longrightarrow & T \otimes_A N & \longrightarrow & T \otimes_A P & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

The first two columns are clearly exact and last column is exact because P is flat. Free modules are flat, so the middle row is exact. Clearly the first row is exact also. It remains to check that the bottom row is exact (and not just right exact). Since $K \otimes_A P \to F \otimes_A P$ is injective, one can check by a diagram chasing argument that $T \otimes_A M \to T \otimes_A N$ is injective. ■

Theorem 2.51 *If $f : A \to B$ is a homomorphism of rings, then the following are equivalent:*

(1) *$A \to B$ is faithfully flat.*

(2) *B is A-flat and for every ideal I of A, $f^{-1}(IB) = I$.*

(3) *B is A-flat and for every A-module M, the map*

$$\begin{aligned} M &\to M \otimes_A B, \\ x &\mapsto x \otimes 1, \end{aligned}$$

is injective.

(4) *f is injective and $B/\operatorname{Im}(f)$ is A-flat.*

Proof (1) $\Rightarrow$ (2) By assumption B is A-flat. So let I be an ideal of A. Set $J = f^{-1}(IB)$ so that $JB = IB$. Since $I \subseteq J$ we have the exact sequence

$$0 \to I \to J \to J/I \to 0.$$

Since B is A-flat, the sequence

$$0 \to I \otimes_A B \to J \otimes_A B \to J/I \otimes_A B \to 0$$

is also exact. Thus

$$\begin{aligned} J/I \otimes_A B &= JB/IB \\ &= 0. \end{aligned}$$

Since B is faithfully flat, we get by Theorem 2.47 that $J/I = 0$ and so $J = I$.

(2) $\Rightarrow$ (3) Consider the map

$$\begin{aligned} \widetilde{f} : M &\to M \otimes_A B, \\ x &\mapsto x \otimes_A 1. \end{aligned}$$

Let $m \in \operatorname{Ker}(\widetilde{f})$ and consider the map

$$\begin{aligned} \varphi : A &\to Am, \\ 1 &\mapsto m. \end{aligned}$$

Now let $I = \mathrm{Ker}(\varphi)$ so that $A/I \cong Am$. Then since B is A-flat we have the following commutative diagram:

$$\begin{array}{ccc} A/I \otimes_A A \cong A/I \cong Am & \xhookrightarrow{\varphi} & M \\ \downarrow{\scriptstyle \mathbb{1}_{A/I} \otimes_A f} & \searrow^{0} & \downarrow{\scriptstyle \widetilde{f}} \\ A/I \otimes_A B & \xhookrightarrow{\varphi \otimes_A \mathbb{1}_B} & M \otimes_A B \end{array}$$

Since $f^{-1}(IB) = I$, we get that the map $\mathbb{1}_{A/I} \otimes_A f$ on the left must be injective. This contradicts that $\widetilde{f} \circ \varphi = 0$. Therefore $\widetilde{f}$ must be injective.

(3) $\Rightarrow$ (4) By (3) the map $A \to A \otimes_A B$ sending $a \mapsto a \otimes 1$ is injective. So let

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

be an exact sequence of A-modules. Then we have the following commutative diagram

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M' \otimes_A B & \longrightarrow & M \otimes_A B & \longrightarrow & M'' \otimes_A B & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M' \otimes_A B/A & \longrightarrow & M \otimes_A B/A & \longrightarrow & M'' \otimes_A B/A & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

where all columns are exact by assumption and the first two rows are exact by assumption and by the flatness of B. The last row is also right exact by the right exactness of $- \otimes_A B/A$. A simple diagram chasing argument shows that the last row is indeed exact and hence that B/A is A-flat. (We leave this to the reader to check, this diagram chase is sometimes called the Nine Lemma.)

(4) $\Rightarrow$ (1) Let

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

be an exact sequence. We then have the same commutative diagram as in the proof of (3) $\Rightarrow$ (4). Now we have that the columns are exact by Lemma 2.50, the first row is exact by assumption, and the last row is exact since B/A is A-flat. A diagram chasing argument shows that the middle row is exact and hence B is A-flat.

We now show that for any A-module M, if $M \otimes_A B = 0$ then $M = 0$ from which it follows from Theorem 2.47 that B is faithfully flat over A. Consider

the exact sequence

$$0 \to A \to B \to B/A \to 0.$$

Let M be an A-module. Since B/A is A-flat, the sequence

$$0 \to M \to M \otimes_A B \to M \otimes_A B/A \to 0$$

is exact again by Lemma 2.50. Thus if $M \otimes_A B = 0$ then $M = 0$. ■

Theorem 2.52 *If A is a Noetherian ring with an ideal I, and $\widehat{A}$ denotes the I-adic completion of A, then the following are equivalent:*

(1) *$A \to \widehat{A}$ is faithfully flat.*

(2) *$I \subseteq \mathfrak{J}(A)$ where $\mathfrak{J}(A)$ is the Jacobson radical of A.*

Proof (1) $\Rightarrow$ (2) Suppose $A \to \widehat{A}$ is faithfully flat. Take any maximal ideal $\mathfrak{m}$ of A. Then $\mathfrak{m}\widehat{A} \neq \widehat{A}$ by the previous theorem. Suppose $\mathfrak{m} \not\supseteq I$. Then $\mathfrak{m} + I = A$, so we can write $1 = x + y$ with $x \in \mathfrak{m}$ and $y \in I$. Since $y \in I$, the element $u = \sum_{i=0}^{\infty} y^i$ is a convergent, well-defined element of $\widehat{A}$. But then

$$xu = (1 - y)\sum_{i=0}^{\infty} y^i = 1.$$

Thus x is a unit in $\widehat{A}$. But $x \in \widehat{\mathfrak{m}} = \mathfrak{m}\widehat{A} \subsetneq \widehat{A}$, a contradiction. We conclude $\mathfrak{m} \supseteq I$. So $I \subseteq \bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m} = \mathfrak{J}(A)$.

(2) $\Rightarrow$ (1) Suppose now that $I \subseteq \mathfrak{J}(A)$. Then for every finitely generated A-module M we have $\bigcap I^n M = 0$ by Corollary 2.37. So the I-adic topology on M is Hausdorff. Therefore $M \to \widehat{M}$ is injective. Since M is finitely generated, $\widehat{M} \cong M \otimes_A \widehat{A}$. So $M \to M \otimes_A \widehat{A}$ is injective for all finitely generated A-modules M. Thus $M \otimes_A \widehat{A} \neq 0$. It remains then to show this for an arbitrary A-module M.

Let M now be any A-module. We can write M as a direct limit of its finitely generated submodules, $M = \varinjlim M_i$. Since each $x \in M$ is contained in M_i for some i, and since $M_i \to M_i \otimes_A \widehat{A}$ is injective for all i, $M \to M \otimes_A \widehat{A}$ is injective. ■

Corollary 2.53 *If A is a local ring and $\widehat{A}$ is the $\mathfrak{m}$-adic completion then $A \to \widehat{A}$ is a faithfully flat extension.*

Definition If $(A, \mathfrak{m})$ and $(B, \mathfrak{n})$ are local rings, a homomorphism $\varphi : A \to B$ is called **local** if $\varphi(\mathfrak{m}) \subseteq \mathfrak{n}$.

Exercise 2.54 *If $f : A \to B$ is a local homomorphism of local rings, f is flat if and only if f is faithfully flat.*

Example 2.55 *If $A = \mathbb{C}[X_1, \ldots, X_n]$ and $I = (X_1, \ldots, X_n)$, then the I-adic completion of A is $\mathbb{C}[\![X_1, \ldots, X_n]\!]$. Is*

$$\mathbb{C}[\mathbf{X}] \hookrightarrow \mathbb{C}[\![\mathbf{X}]\!]$$

faithfully flat? To answer this we should ask ourselves, is $I \subseteq \mathfrak{J}(\mathbb{C}[\mathbf{X}])$? The answer to this question is "No!" Thus, $\mathbb{C}[\mathbf{X}] \hookrightarrow \mathbb{C}[\![\mathbf{X}]\!]$ is flat but not faithfully flat. However, the canonical injection (show that this is an injection)

$$\mathbb{C}[\mathbf{X}]_{(\mathbf{X})} \hookrightarrow \mathbb{C}[\![\mathbf{X}]\!]$$

is in fact faithfully flat by the above exercise.

As a final remark on completions, we note the Cohen Structure Theorem guarantees that every complete, Noetherian local ring is a quotient of $V[\![x_1, \ldots, x_n]\!]$, where V is a field or a complete discrete valuation ring. In particular, this means that every complete local ring R is **catenary**, that is, given any two saturated chains of prime ideals $\mathfrak{q} = \mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n = \mathfrak{q}'$ and $\mathfrak{q} = \mathfrak{p}'_0 \subseteq \mathfrak{p}'_1 \subseteq \cdots \subseteq \mathfrak{p}'_{m-1} \subseteq \mathfrak{p}'_m = \mathfrak{q}'$ of R we have $m = n$. This can fail for arbitrary Noetherian local rings, although the construction of non-catenary rings is rather involved.

Chapter 3

Dimension Theory

In this chapter, we will develop the notion of the dimension of a module three different ways. The Dimension Theorem will then show that over a local ring, the three notions are actually equivalent.

3.1 The Graded Case

Definition If $f : \mathbb{Z} \to \mathbb{Z}$ is a function, we say that f is **essentially polynomial** or **polynomial-like** if there exists $P \in \mathbb{Q}[x]$ such that $f(n) = P(n)$ for sufficiently large n.

Note that it is an easy exercise to see that such a P as in the above definition is unique. Moreover, we define the **degree** of f to be the degree of the polynomial P. If $P = 0$, then we say f has degree -1.

Definition Given the function $f : \mathbb{Z} \to \mathbb{Z}$, define the **standard difference operator** Δ to be

$$\Delta f(n) := f(n+1) - f(n).$$

Definition We denote by $B_k(x) : \mathbb{Z} \to \mathbb{Z}$ for $k \geq 0$ the kth **binomial polynomial** function defined by

$$B_0(x) = 1$$
$$B_k(x) = \binom{x}{k} := \frac{x!}{k!(x-k)!} = \frac{(x)(x-1)\cdots(x-k+1)}{k!}.$$

Note that

$$\begin{aligned}\Delta B_k(n) &= B_k(n+1) - B_k(n) \\ &= \frac{(n+1)!}{k!(n-k+1)!} - \frac{n!}{k!(n-k)!} \\ &= \frac{(n+1)n!}{k!(n-k+1)!} - \frac{(n-k+1)n!}{k!(n-k+1)!} \\ &= \frac{(k)n!}{k!(n-k+1)!} \\ &= \frac{n!}{(k-1)!(n-(k-1))!} \\ &= B_{k-1}(n),\end{aligned}$$

for $k > 1$, and for any function $f : \mathbb{Z} \to \mathbb{Z}$ we have

$$\begin{aligned}f(n) &= \Delta f(n+1) + f(n-1) \\ &= \left(\sum_{i=1}^{n} \Delta f(i+1)\right) + f(0).\end{aligned}$$

Thus if $\Delta f(x) = \Delta g(x)$, then $f(x) = g(x) + C$ for some integer C.

Proposition 3.1 *Let $f \in \mathbb{Q}[X]$. Then the following are equivalent:*

(1) *$f(x)$ is a $\mathbb{Z}$-linear combination of the $B_k(x)$.*

(2) *$f(n) \in \mathbb{Z}$ for all $n \geq 0$.*

(3) *$f(n) \in \mathbb{Z}$ for n sufficiently large.*

(4) *$\Delta f(x)$ is a $\mathbb{Z}$-linear combination of the $B_k(x)$.*

Proof The implications (1) $\Rightarrow$ (2) $\Rightarrow$ (3) and (1) $\Rightarrow$ (4) are clear. We prove (4) $\Rightarrow$ (1) and (3) $\Rightarrow$ (1).
For (4) $\Rightarrow$ (1), suppose $\Delta f(x) = \sum_k m_k B_k(x)$ for some $m_k \in \mathbb{Z}$. Then $\Delta f(x) = \sum_k B_k(x) \sum_k m_k \Delta B_{k+1}(x) = \Delta \sum_k m_k B_{k+1}(x)$. By the remark above, $f(n) = (\sum_k m_k B_{k+1}(n)) + C \cdot B_0(n)$ for some integer C, as required.
For (3) $\Rightarrow$ (1), suppose $f(n) \in \mathbb{Z}$ for all $n \gg 0$. We proceed by induction on $\deg(f)$. Since $\Delta f(n) \in \mathbb{Z}$ for all $n \gg 0$, by induction we have that $\Delta f(x)$ is a $\mathbb{Z}$-linear combination of the $B_k(x)$. As (4) $\Rightarrow$ (1), we have that $f(x)$ is a $\mathbb{Z}$-linear combination of the $B_k(x)$.

■

Lemma 3.2 *Let $\mathcal{P}$ be the set of essentially polynomial functions and let $f : \mathbb{Z} \to \mathbb{Z}$. The following are equivalent:*

(1) *$f \in \mathcal{P}$.*

(2) *$\Delta f \in \mathcal{P}$.*

(3) $\Delta^r f = 0$ *for some* $r > 0$.

Proof (1) $\Rightarrow$ (2) $\Rightarrow$ (3) These are clear from the definitions.

(2) $\Rightarrow$ (1) First note that if $\Delta f(n) = 0$ for sufficiently large n, we have that $f(n+1) - f(n) = 0$, which implies that $f(n+1) = f(n)$ for sufficiently large n. Because $f : \mathbb{Z} \to \mathbb{Z}$, we see that f must be constant for large n, showing $f \in \mathcal{P}$.

Now suppose that $\Delta f(n) = P(n)$ for n sufficiently large, where $P(x) \in \mathbb{Q}[x]$. By the previous proposition,

$$P(n) = \sum_{i=0}^{t} a_i B_k(n) = \sum_{i=0}^{t} a_i \Delta B_{k+1}(n) = \Delta \left(\sum_{i=0}^{t} a_i B_{k+1}(n) \right),$$

where $a_0, \ldots, a_t \in \mathbb{Z}$. Let $Q(x) = \sum_{i=0}^{t} a_i B_{k+1}(x)$. Then if we set $g(n) = f(n) - Q(n)$ then for n sufficiently large, we have that

$$\Delta g(n) = \Delta f(n) - \Delta Q(n) = P(n) - P(n) = 0.$$

Hence $f(n) = Q(n) + c$ for n sufficiently large and for some constant c. Therefore $f \in \mathcal{P}$.

(3) $\Rightarrow$ (1) This follows from (2) $\Rightarrow$ (1) applied r times. ■

3.1.1 The Hilbert Polynomial

Theorem 3.3 (Hilbert-Serre) *Let A_0 be an Artinian ring and A be the graded ring*

$$A = A_0 \oplus \underbrace{A_1 \oplus \cdots A_n \oplus \cdots}_{A_+}$$

where A_+ is generated by $x_1, \ldots, x_r \in A_1$. We see that we may think of A as the algebra $A = A_0[x_1, \ldots, x_r]$. Let M be a finitely generated graded A-module,

$$M = M_0 \oplus M_1 \oplus \cdots \oplus M_n \oplus \cdots,$$

where each M_n is a finitely generated A_0-module. The following are true:

(1) $\lambda_{A_0}(M_n) < \infty$ *for all* $n \geq 0$.

(2) *Define the* ***Hilbert function*** $\mathrm{Hilb}_M(n) := \lambda_{A_0}(M_n)$. *Then* $\mathrm{Hilb}_M(n)$ *is essentially polynomial of degree at most* $r - 1$.

(3) *Suppose that M_0 generates M over A. Then*

$$\Delta^{r-1}\mathrm{Hilb}_M(n) \leq \lambda_{A_0}(M_0)$$

with equality holding if and only if

$$\begin{aligned} \psi : M_0 \otimes_{A_0} A_0[X_1, \ldots, X_r] &\to M \\ m_0 \otimes a X_1^{i_1} \cdots X_r^{i_r} &\mapsto a \cdot x_1^{i_1} \cdots x_r^{i_r} \cdot m_0 \end{aligned}$$

is an isomorphism where the X_i's are indeterminates.

Proof We will show this in several parts:

(1) To show $\lambda_{A_0}(M_n) < \infty$, it is enough to show that each M_n is finitely generated over A_0, as A_0 is both Artinian and Noetherian. Take any M_n and suppose that $m_1, \ldots, m_s$ generate M over A with each m_i homogeneous of degree d_i. Each element in M_n is then a sum of elements of the form

$$ax_1^{i_1} \cdots x_r^{i_r} m_j$$

where $a \in A_0$ and $\sum_{t=1}^{r} i_t + d_j = n$. Given n and d_j only finitely many i_t's can be found, so M_n is finitely generated over A_0.

(2) Proceed by induction on r. If $r = 0$, then we have $A = A_0$ and since M is finitely generated over A this implies that $M_n = 0$ for n sufficiently large. Thus $\mathrm{Hilb}_M(n) = 0$ for n sufficiently large and we have that the degree of $\mathrm{Hilb}_M(n) = -1$.

Now suppose our statement is true up through $r - 1$. Consider the exact sequence

$$0 \longrightarrow N \longrightarrow M \xrightarrow{x_r} M \longrightarrow L \longrightarrow 0$$

where $N = (0 :_M x_r)$ and $L = M/x_r M$. So both N and L are killed by x_r and hence are both graded modules over

$$\overline{A} = A_0[\mathbf{x}]/_r A_0[\mathbf{x}] = A/x_r A,$$

a graded ring with $\overline{A}_+$ generated by $r - 1$ elements over $\overline{A}_0$.

Now for each n we have an exact sequence

$$0 \longrightarrow N_n \longrightarrow M_n \xrightarrow{x_r} M_{n+1} \longrightarrow L_{n+1} \longrightarrow 0.$$

Since length is additive we get

$$\lambda_{A_0}(L_{n+1}) - \lambda_{A_0}(M_{n+1}) + \lambda_{A_0}(M_n) - \lambda_{A_0}(N_n) = 0.$$

And so we see that

$$\lambda_{A_0}(M_{n+1}) - \lambda_{A_0}(M_n) = \lambda_{A_0}(L_{n+1}) - \lambda_{A_0}(N_n),$$

which shows us

$$\Delta\mathrm{Hilb}_M(n) = \mathrm{Hilb}_L(n+1) - \mathrm{Hilb}_N(n).$$

By the inductive hypothesis, the right-hand side is essentially polynomial of degree at most $r - 2$. Thus $\Delta\mathrm{Hilb}_M(n)$ is essentially polynomial of degree at most $r - 2$. By Lemma 3.2, we have the degree of $\mathrm{Hilb}_M(n)$ is essentially polynomial of degree at most $r - 1$. So by induction, we have proved (2).

(3) ($\Rightarrow$) Suppose that M_0 generates M over A. That is $\alpha_1, \ldots, \alpha_s$ generate M over A and each of the α_i's have degree 0. Consider the map

$$\begin{aligned}\psi : M_0 \otimes_{A_0} A_0[X_1, \ldots, X_r] &\to M \\ m \otimes a X_1^{i_1} \cdots X_r^{i_r} &\mapsto m \cdot a \cdot x_1^{i_1} \cdots x_r^{i_r}.\end{aligned}$$

Then ψ is a graded map of degree 0. ψ is onto as M is generated by M_0. Hence if F_n is the free A_0-module generated by monomials $X_1^{i_1} \cdots X_r^{i_r}$ such that $\sum i_j = n$,

$$\psi_n : M_0 \otimes_{A_0} F_n \to M_n$$

is onto. So we have

$$\begin{aligned}\lambda_{A_0}(M_n) &\leq \lambda_{A_0}(M_0 \otimes_{A_0} F_n) \\ &\leq \lambda_{A_0}(M_0) \cdot N,\end{aligned}$$

where N is the number of monomials $X_1^{i_1} \cdots X_r^{i_r}$ of degree n. But what is this value N? Well whatever it is, it is the same as the number of monomials $X_1^{i_1} \cdots X_r^{i_r}$ of degree n in the expression

$$\begin{aligned}(1 + X_1 + X_1^2 + \cdots)(1 + X_2 + X_2^2 + \cdots) \cdots (1 + X_r + X_r^2 + \cdots) \\ = \frac{1}{1 - X_1} \cdot \frac{1}{1 - X_2} \cdot \cdots \cdot \frac{1}{1 - X_r}.\end{aligned}$$

But this is nothing more than the coefficient of X^n in

$$\frac{1}{(1 - X)^r} \qquad \text{where} \qquad X = X_1 = X_2 = \cdots = X_r.$$

So we see that

$$N = \binom{n + r - 1}{r - 1}.$$

Alternatively one can realize that the above formula is the one for choosing with replacement n items from r types of item. Now by (1) we know that $\mathrm{Hilb}_M(n)$ is essentially polynomial of degree at most $r - 1$. So by $\mathrm{Hilb}_M(n)$ we shall instead now mean the polynomial equal to $\mathrm{Hilb}_M(n)$ for large n. Thus for n sufficiently large,

$$\mathrm{Hilb}_M(n) = \lambda_{A_0}(M_n) \leq \lambda_{A_0}(M_0) \cdot N = \lambda_{A_0}(M_0) \cdot \frac{(n + r - 1)!}{(r - 1)! n!}$$

So we see that

$$\mathrm{Hilb}_M(n) \leq \lambda_{A_0}(M_0) \cdot \frac{(n + r - 1)!}{(r - 1)! n!}$$

and so

$$(r - 1)! \cdot \mathrm{Hilb}_M(n) \leq \lambda_{A_0}(M_0) \cdot \frac{(n + r - 1)!}{n!}.$$

Taking the limit as n goes to infinity of both sides, we get

$$\Delta^{r-1}\text{Hilb}_M(n) \leq \lambda_{A_0}(M_0).$$

Now if ψ as described above is an isomorphism it is clear that

$$\Delta^{r-1}\text{Hilb}_M(n) = \lambda_{A_0}(M_0).$$

($\Leftarrow$) Conversely, suppose that $\Delta^{r-1}\text{Hilb}_M(n) = \lambda_{A_0}(M_0)$. We will show that ψ as described above is an isomorphism. Proceed by induction on $\lambda_{A_0}(M_0)$. Suppose that $\lambda_{A_0}(M_0) = 1$ and so $M_0 = A_0/\mathfrak{m}_0 = k$, where $\mathfrak{m}_0$ is some maximal ideal of A_0. Consider the exact sequence

$$0 \longrightarrow L \longrightarrow k[X_1, \ldots, X_r] \xrightarrow{\psi} M \longrightarrow 0,$$

where L is an ideal of $k[\mathbf{X}]$. Likewise we have an exact sequence

$$0 \to L_n \to k[X_1, \ldots, X_r]_n \to M_n \to 0.$$

Now we have

$$\lambda_{A_0}(k[\mathbf{X}]_n) = \lambda_{A_0}(L_n) + \lambda_{A_0}(M_n)$$

and so

$$\text{Hilb}_{k[\mathbf{X}]}(n) = \text{Hilb}_L(n) + \text{Hilb}_M(n).$$

From here we see

$$\Delta^{r-1}\text{Hilb}_{k[\mathbf{X}]}(n) = \Delta^{r-1}\text{Hilb}_L(n) + \Delta^{r-1}\text{Hilb}_M(n).$$

However, by (2) we see that $\Delta^{r-1}\text{Hilb}_{k[\mathbf{X}]}(n)$ and $\Delta^{r-1}\text{Hilb}_M(n)$ are both of degree zero, and since $\lambda_{A_0}(M_0) = 1$, we have that they are both 1. Thus

$$\Delta^{r-1}\text{Hilb}_L(n) = 0$$

We claim that if $L \neq (0)$, then $\Delta^{r-1}\text{Hilb}_L(n) > 0$. Suppose there exists nonzero $f \in L$ and set $d = \deg(f)$. Since L is an ideal of $k[\mathbf{X}]_n$, we have that $f \cdot k[\mathbf{X}]_n \subseteq L$. Thus

$$\lambda_{A_0}(L_n) \geq \lambda_{A_0}((k[\mathbf{X}]f)_n).$$

Since $k[\mathbf{X}]$ is a domain, multiplication by f is injective. Therefore, $f \cdot k[\mathbf{X}] \cong k[\mathbf{X}]$ as k-modules. Thus

$$\lambda_{A_0}((k[\mathbf{X}]f)_n) = \lambda_{A_0}(k[\mathbf{X}]_{n-d}) = \binom{n-d+r-1}{r-1}.$$

and so $\Delta^{r-1}\text{Hilb}_L(n) > 0$.

Now suppose that $\lambda_{A_0}(M_0) > 1$ and look at

$$0 \longrightarrow L \longrightarrow M_0[\mathbf{X}] \xrightarrow{\psi} M \longrightarrow 0$$

where $L = \mathrm{Ker}(M)$. So we need to show that $L = (0)$. Supposing $L \neq (0)$, we then have

$$\mathrm{Hilb}_{M_0[\mathbf{X}]}(n) = \mathrm{Hilb}_L(n) + \mathrm{Hilb}_M(n),$$

and so

$$\Delta^{r-1}\mathrm{Hilb}_{M_0[\mathbf{X}]}(n) = \Delta^{r-1}\mathrm{Hilb}_L(n) + \Delta^{r-1}\mathrm{Hilb}_M(n).$$

But $\Delta^{r-1}\mathrm{Hilb}_{M_0[\mathbf{X}]}(n) = \lambda_{A_0}(M_0) = \Delta^{r-1}\mathrm{Hilb}_M(n)$. Hence $\Delta^{r-1}\mathrm{Hilb}_L(n) = 0$. We claim that this shows that $L = (0)$. Suppose that $L \neq (0)$. Consider a Jordan-Hölder chain, that is

$$M_0 \supsetneq M_0^1 \supsetneq \cdots \supsetneq M_0^s = (0)$$

such that $M_0^i/M_0^{i+1} \cong A_0/\mathfrak{m}_i \cong k_i$ where k_i is a field. Now we have the exact sequence:

$$0 \to M_0^{i+1} \to M_0^i \to k_i \to 0$$

Applying $- \otimes_{A_0} A_0[X_1, \ldots, X_r]$ we obtain the exact sequence

$$0 \to M_0^{i+1}[\mathbf{X}] \to M_0^i[\mathbf{X}] \to k_i[\mathbf{X}] \to 0 \qquad (\bigstar)$$

as $A_0[X_1, \ldots, X_r]$ is a free, hence flat, A_0-module. Since $L \neq (0)$, there exists i such that $L \subseteq M_0^i[\mathbf{X}]$ but $L \not\subseteq M_0^{i+1}[\mathbf{X}]$. By $(\bigstar)$, the image of L in $k_i[\mathbf{X}]$ is nonzero, call it L_i. Now we have the surjection $L \twoheadrightarrow L_i$ and hence we have

$$\mathrm{Hilb}_{L_i}(n) \leq \mathrm{Hilb}_L(n)$$
$$\Delta^{r-1}\mathrm{Hilb}_{L_i}(n) \leq \Delta^{r-1}\mathrm{Hilb}_L(n),$$

but by an argument similar to the one above we see that $\Delta^{r-1}\mathrm{Hilb}_{L_i}(n) > 0$ and hence that $\Delta^{r-1}\mathrm{Hilb}_L(n) > 0$. So we see that $L = 0$ and hence our map ψ is an isomorphism. ■

Definition The polynomial representative of the Hilbert function $\mathrm{Hilb}_M(n) = \lambda_{A_0}(M_n)$ is called the **Hilbert polynomial** of M. We will abuse notation and simply denote this polynomial by $\mathrm{Hilb}_M(n)$.

Remark The previous theorem is saying that if $A = k[x_1, \ldots, x_n]$ and if M is defined as above, then:

(1) Each M_i is a finite dimensional vector space since $\lambda_k(M_n) = \dim_k(M_n) < \infty$.

(2) The dimensions of the vector spaces M_i exhibit polynomial growth.

Definition If $\mathrm{Hilb}_M(n)$ is of degree d, then the **Hilbert multiplicity** of M is

$$e(M) := \begin{cases} \Delta^d\mathrm{Hilb}_M(n) = d!\, a_d & \text{if } d > 0 \\ \lambda_{A_0}(M) & \text{if } d = 0 \end{cases}$$

where $\mathrm{Hilb}_M(n) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$.

Definition With notation as above, we define the **Hilbert series** of M to be

$$HS_M(t) := \sum_{i \geq 0} \mathrm{Hilb}_M(i) t^i = \sum_{i \geq 0} \lambda_{A_0}(M_i) t^i.$$

Because $\mathrm{Hilb}_M(n)$ is eventually polynomial, it follows that the Hilbert Series is a rational function $HS_M(t) = \frac{g(t)}{(1-t)^r}$, where r is the number of generators of A_+. After reducing the rational function representation so that the numerator is not divisible by $1-t$, we can write $HS_M(t) = \frac{h(t)}{(1-t)^m}$ for some nonnegative integer m so that $h(1) \neq 0$.

Example 3.4 *Let $S = K[x,y,z]$, where S is a field and consider the graded ideal (x^2, yz). One checks that*

$$\begin{aligned}
S_0 &= K \\
S_1 &= Kx + Ky + Kz \\
S_2 &= Kxy + Kxz + Ky^2 + Kz^2 \\
S_3 &= Kxy^2 + Kxz^2 + Ky^3 + Kz^3 \\
S_4 &= Kxy^3 + Kxz^3 + Ky^4 + Kz^4 \\
&\vdots \quad \vdots \\
S_d &= Kxy^{d-1} + Kxz^{d-1} + Ky^3 + Kz^d
\end{aligned}$$

Thus the first few values of the Hilbert function of S/I are: $1,3,4,4,4,\ldots$ and $\mathrm{Hilb}_{S/I}(n) = 4$ for all $n \geq 2$. Thus the Hilbert polynomial of S/I is 4 and the Hilbert multiplicity of M is 4. The Hilbert Series of M is then

$$HS_M(t) = 1 + 3t + 4t^2 + 4t^3 + 4t^4 + \cdots = \frac{1 + 2t + t^2}{1 - t}.$$

Exercise 3.5 *Let $S = K[x_1, \ldots, x_n]$ be a standard graded (i.e. $\deg(x_i) = 1$ for all i) polynomial ring over a field. Show that*

$$HS_S(t) = \frac{1}{(1-t)^n}.$$

Exercise 3.6 *Let $S = K[x_1, \ldots, x_n$ and let M be a finitely generated graded S-module. Suppose that*

$$HS_M(t) = \frac{h(t)}{(1-t)^m},$$

where $h(1) \neq 0$. Show that $e(M) = h(1)$.

3.2 The Hilbert-Samuel Polynomial

Lemma 3.7 *If A is a quasi-local ring with maximal ideal $\mathfrak{m}$, and M, N, are nonzero finitely generated A-modules, then $M \otimes_A N \neq 0$.*

Proof Arguing by contradiction, suppose $M \neq 0$, $N \neq 0$, and $M \otimes_A N = 0$. Then

$$\begin{aligned} 0 = (M \otimes_A N) \otimes_A A/\mathfrak{m} &= M \otimes_A (N \otimes_A A/\mathfrak{m}) \\ &= M \otimes_A N/\mathfrak{m}N \\ &= M \otimes_A A/\mathfrak{m} \otimes_{A/\mathfrak{m}} N/\mathfrak{m}N \\ &= M/\mathfrak{m}M \otimes_{A/\mathfrak{m}} N/\mathfrak{m}N. \end{aligned}$$

At this point note that $M/\mathfrak{m}M$ is a finite dimensional vector space over $A/\mathfrak{m}$. We claim that $M \neq 0$ implies that $M/\mathfrak{m}M \neq 0$, for if $M/\mathfrak{m}M = 0$, then $M = \mathfrak{m}M$, and hence by Nakayama's Lemma, Corollary 0.29, $M = 0$. Since $M/\mathfrak{m}M \neq 0$ as a finite dimensional vector space over $A/\mathfrak{m}$ and since $N/\mathfrak{m}N \neq 0$ as a finite dimensional vector space over $A/\mathfrak{m}$, we see that $M/\mathfrak{m}M \otimes_{A/\mathfrak{m}} N/\mathfrak{m}N \neq 0$, a contradiction. ■

Lemma 3.8 *If A is Noetherian and M, N are finitely generated A-modules, then*

$$\operatorname{Supp}(M \otimes_A N) = \operatorname{Supp}(M) \cap \operatorname{Supp}(N)$$

Proof ($\subseteq$) Suppose that $\mathfrak{p} \in \operatorname{Supp}(M \otimes_A N)$. Write

$$\begin{aligned} 0 \neq (M \otimes_A N)_\mathfrak{p} &\cong M \otimes_A N \otimes_A \otimes A_\mathfrak{p} \\ &\cong M \otimes_A N_p \\ &\cong M \otimes_A A_\mathfrak{p} \otimes_{A_\mathfrak{p}} N_p \\ &\cong M_\mathfrak{p} \otimes_{A_\mathfrak{p}} N_\mathfrak{p}. \end{aligned}$$

This shows us that $M_\mathfrak{p} \neq (0)$ and that $N_\mathfrak{p} \neq (0)$.

($\supseteq$) If $\mathfrak{p} \in \operatorname{Supp}(M) \cap \operatorname{Supp}(N)$, $M_\mathfrak{p} \neq 0$ and $N_\mathfrak{p} \neq 0$ we see by Lemma 3.7 that $M_\mathfrak{p} \otimes_{A_\mathfrak{p}} N_\mathfrak{p} \neq 0$. This shows us that $(M \otimes_A N)_\mathfrak{p} \neq 0$ and so we see that $\mathfrak{p} \in \operatorname{Supp}(M \otimes_A N)$. ■

Lemma 3.9 *Let A be a Noetherian ring and M a finitely generated A-module such that for some ideal $\mathfrak{a}$ of A, $\lambda(M/\mathfrak{a}M) < \infty$. Suppose (M_i) is a filtration of M with respect to $\mathfrak{a}$, that is $\mathfrak{a}^n M \subseteq M_n$ for each n. Then we have the following:*

(1) *$\lambda(M/M_n) < \infty$.*

(2) *If $N \hookrightarrow M$, then $\lambda(N/\mathfrak{a}N) < \infty$.*

Proof (1) First note that $\lambda(M/\mathfrak{a}M) < \infty$ if and only if $\operatorname{Supp}(M/\mathfrak{a}M)$ consists entirely of maximal ideals. Write

$$\operatorname{Supp}(M/\mathfrak{a}M) = \operatorname{Supp}(M \otimes_A A/\mathfrak{a}) = \operatorname{Supp}(M) \cap \operatorname{Supp}(A/\mathfrak{a}),$$

and

$$\operatorname{Supp}(M/\mathfrak{a}^n M) = \operatorname{Supp}(M \otimes_A A/\mathfrak{a}^n) = \operatorname{Supp}(M) \cap \operatorname{Supp}(A/\mathfrak{a}^n).$$

But $\operatorname{Supp}(A/\mathfrak{a}) = \operatorname{Supp}(A/\mathfrak{a}^n)$. Thus, $\lambda(M/\mathfrak{a}^n M) < \infty$ for each n if and only if $\lambda(M/\mathfrak{a}M) < \infty$. By construction we have the following exact sequence

$$M/\mathfrak{a}^n M \to M/M_n \to 0.$$

Hence $\lambda(M/M_n) < \infty$ for all $n > 0$.

(2) Now if $N \hookrightarrow M$,

$$\operatorname{Supp}(N/\mathfrak{a}N) = \operatorname{Supp}(N) \cap \operatorname{Supp}(A/\mathfrak{a}) \subseteq \operatorname{Supp}(M) \cap \operatorname{Supp}(A/\mathfrak{a}).$$

But $\operatorname{Supp}(M) \cap \operatorname{Supp}(A/\mathfrak{a}) = \operatorname{Supp}(M/\mathfrak{a}M)$, hence $\operatorname{Supp}(N/\mathfrak{a}N)$ consists only of maximal ideals and we see that $\lambda(N/\mathfrak{a}N) < \infty$. ■

Proposition 3.10 *Let A be Noetherian, M finitely generated with $\mathfrak{a}$ an ideal of A such that $\lambda(M/\mathfrak{a}M) < \infty$. Let (M_i) be an $\mathfrak{a}$-good filtration of M. Then*

$$P((M_i), n) := \lambda(M/M_n)$$

is essentially polynomial.

Proof Write

$$\Delta P((M_i), n) = P((M_i), n+1) - P((M_i), n) = \lambda(M/M_{n+1}) - \lambda(M/M_n).$$

Since length is additive, we see that the right-hand side is $\lambda(M_n/M_{n+1})$ by looking at the exact sequence

$$0 \to M_n/M_{n+1} \to M/M_{n+1} \to M/M_n \to 0.$$

Now

$$\begin{aligned} \operatorname{Gr}(M) &= M/M_1 \oplus M_1/M_2 \oplus \cdots \oplus M_n/M_{n+1} \oplus \cdots, \\ \operatorname{Gr}_{\mathfrak{a}}(A) &= A/\mathfrak{a} \oplus \mathfrak{a}/\mathfrak{a}^2 \oplus \cdots \oplus \mathfrak{a}^n/\mathfrak{a}^{n+1} \oplus \cdots. \end{aligned}$$

Note that while $\operatorname{Gr}_{\mathfrak{a}}(A)$ is Noetherian, and is generated by elements of $\mathfrak{a}/\mathfrak{a}^2$, $A/\mathfrak{a}$ is not necessarily Artinian, and hence we cannot use the Hilbert-Serre Theorem, Theorem 3.3. By assumption we have $\lambda(M/\mathfrak{a}M) < \infty$. Hence

$$\begin{aligned} \operatorname{Supp}(M/\mathfrak{a}M) &= \operatorname{Supp}(M) \cap \operatorname{Supp}(A/\mathfrak{a}) \\ &= \operatorname{Supp}(A/\operatorname{Ann}(M)) \cap \operatorname{Supp}(A/\mathfrak{a}) \\ &= \operatorname{Supp}(A/\operatorname{Ann}(M) \otimes_A A/\mathfrak{a}) \\ &= \operatorname{Supp}(A/(\operatorname{Ann}(M) + \mathfrak{a})), \end{aligned}$$

and so we see $\lambda(A/(\operatorname{Ann}(M)+\mathfrak{a})) < \infty$. But this shows us that $A/(\operatorname{Ann}(M)+\mathfrak{a})$ is Artinian. Now take $B = A/\operatorname{Ann}(M)$ and $\mathfrak{b} = (\mathfrak{a} + \operatorname{Ann}(M))/\operatorname{Ann}(M)$. Each M_n/M_{n+1} is a $B/\mathfrak{b}$-module. Now

$$\operatorname{Gr}_{\mathfrak{b}}(B) = B/\mathfrak{b} \oplus \mathfrak{b}/\mathfrak{b}^2 \oplus \cdots \oplus \mathfrak{b}^n/\mathfrak{b}^{n+1} \oplus \cdots$$

is a graded ring which is a finitely generated $B/\mathfrak{b}$-algebra by elements of $\mathfrak{b}/\mathfrak{b}^2$ and $B/\mathfrak{b}$ is Artinian. Moreover, $\mathrm{Gr}(M)$ is a finitely generated $\mathrm{Gr}_{\mathfrak{b}}(B)$-module and $\lambda_A(M_n) = \lambda_B(M_n)$. Hence by the Hilbert-Serre Theorem, Theorem 3.3, $\mathrm{Hilb}_{\mathrm{Gr}(M)}(n) = \lambda(M_n/M_{n+1})$ is essentially polynomial and hence $\Delta P((M_i), n)$ is essentially polynomial, which shows us that $P((M_i), n)$ is essentially polynomial. ■

Theorem 3.11 (Samuel) *If A is Noetherian, M is a finitely generated A-module, $\mathfrak{a}$ is an ideal of A such that $\lambda(M/\mathfrak{a}M) < \infty$, and (M_i) is a filtration of M such that $\mathfrak{a}^n M \subseteq M_n$, then define*

$$P_{\mathfrak{a}}(M, n) := \lambda(M/\mathfrak{a}^n M).$$

The following are true:

(1) $P_{\mathfrak{a}}(M, n) \geq P((M_i), n)$.

(2) *Suppose that (M_i) is $\mathfrak{a}$-good. Then*

$$P_{\mathfrak{a}}(M, n) = P((M_i), n) + R(n)$$

where the degree of $R(n)$ is strictly less than the degree of $P_{\mathfrak{a}}((M_i), n)$. In particular, $P_{\mathfrak{a}}(M, n)$ and $P((M_i), n)$ have the same degree and same leading coefficient. Moreover the leading coefficient of $R(n)$ is nonnegative.

Proof First we will prove (1). Since $\mathfrak{a}^n M \subseteq M_n$ we have the exact sequence:

$$0 \to M_n/\mathfrak{a}^n M \to M/\mathfrak{a}^n M \to M/M_n \to 0$$

Thus

$$\lambda(M/\mathfrak{a}^n M) \geq \lambda(M/M_n) \qquad (\bigstar)$$

and so by definition $P_{\mathfrak{a}}(M, n) \geq P_{\mathfrak{a}}((M_i), n)$.

Now for (2) we will start by defining

$$R(n) = \lambda(M/\mathfrak{a}^n M) - \lambda(M/M_n) = \lambda(M_n/\mathfrak{a}^n M).$$

Since (M_i) is $\mathfrak{a}$-good, we see that there exists $m > 0$ such that

$$\mathfrak{a}^{n+m} M \subseteq M_{n+m} = \mathfrak{a}^n M_m \subseteq \mathfrak{a}^n M$$

for some large n. Thus we have the exact sequence

$$0 \to M_{n+m}/\mathfrak{a}^{n+m} M \to M/\mathfrak{a}^{n+m} M \to M/M_{n+m} \to 0.$$

and so $\lambda(M/\mathfrak{a}^{n+m} M) \geq \lambda(M/M_{n+m})$. By $(\bigstar)$ we see that

$$P_{\mathfrak{a}}(M, n+m) \geq P((M_i), n+m) \geq P_{\mathfrak{a}}(M, n) \geq P((M_i), n)$$

for large n. Hence $P_{\mathfrak{a}}(M, n)$ has the same degree as $P_{\mathfrak{a}}((M_i), n)$ with the same leading coefficient. So $\deg(R(n))$ is strictly less than that of $P_{\mathfrak{a}}(M, n)$. Since $R(n) \geq 0$ for every n, we see that the leading coefficient of $R(n)$ must be nonnegative. ■

Definition If A is Noetherian, M is a finitely generated A-module, $\mathfrak{a}$ is an ideal of A such that $\lambda(M/\mathfrak{a}M) < \infty$, then the polynomial $P_{\mathfrak{a}}(M,n)$ as defined above by

$$P_{\mathfrak{a}}(M,n) := \lambda(M/\mathfrak{a}^n M) \text{ for } n \gg 0$$

is called the **Hilbert-Samuel polynomial** of M with respect to $\mathfrak{a}$.

Definition (First Notion of Dimension) If $(A,\mathfrak{m})$ is a local ring and M is a finitely generated A-module denote

$$\dim_{HS}(M) := \deg(P_{\mathfrak{m}}(M,n)).$$

Corollary 3.12 *Properties of the Hilbert-Samuel polynomial $P_{\mathfrak{a}}(M,n)$:*

(1) $\deg(P_{\mathfrak{a}}(M,n)) \leq m$ *where m is the minimal number of generators of* $(\mathfrak{a} + \operatorname{Ann}(M))/\operatorname{Ann}(M)$.

(2) *Suppose r is the minimal number of generators of $\mathfrak{a}$. Then*

$$\Delta^r P_{\mathfrak{a}}(M,n) \leq \lambda(M/\mathfrak{a}M).$$

Moreover, equality holds if and only if the canonical homomorphism

$$M/\mathfrak{a}M[X_1,\ldots,X_r] \to \bigoplus_{n=0}^{\infty} \frac{\mathfrak{a}^n M}{\mathfrak{a}^{n+1}M}$$

is an isomorphism.

Proof Follows from the Hilbert-Serre Theorem, Theorem 3.3. ■

Proposition 3.13 *If A is Noetherian, and $\mathfrak{a}$ is an ideal of A let*

$$0 \to L \to M \to N \to 0$$

be an exact sequence of finitely generated A-modules such that $\lambda(M/\mathfrak{a}M) < \infty$. Then

$$P_{\mathfrak{a}}(M,n) = P_{\mathfrak{a}}(L,n) + P_{\mathfrak{a}}(N,n) - R(n)$$

where $\deg(R(n)) < \deg(P_{\mathfrak{a}}(L,n))$.

Proof Since $\lambda(M/\mathfrak{a}M) < \infty$, we know that $L/\mathfrak{a}L$ and $N/\mathfrak{a}N$ both have finite length, hence the equation we wish to show is well-defined. We have an exact sequence:

$$0 \to \frac{L}{L \cap \mathfrak{a}^n M} \to \frac{M}{\mathfrak{a}^n M} \to \frac{N}{\mathfrak{a}^n N} \to 0$$

Write $L_n = L \cap \mathfrak{a}^n M$. By the Artin-Rees Lemma, Lemma 2.33, (L_i) is $\mathfrak{a}$-good. Thus $\lambda(M\mathfrak{a}^n M) = \lambda(N/\mathfrak{a}^n N) + \lambda(L/L \cap a^n M)$ and so

$$\begin{aligned} P_{\mathfrak{a}}(M,n) &= P_{\mathfrak{a}}(N,n) + P((L_i),n) \\ &= P_{\mathfrak{a}}(N,n) + P_{\mathfrak{a}}(L,n) - R(n), \end{aligned}$$

by the previous theorem. ■

Corollary 3.14 *If $(A, \mathfrak{m})$ is local, let*

$$0 \to L \to M \to N \to 0$$

be an exact sequence of finitely generated A-modules such that $\lambda(M/\mathfrak{m}M) < \infty$. Then

$$\dim_{HS}(M) = \max\{\dim_{HS}(L), \dim_{HS}(N)\}.$$

Proposition 3.15 *Let A be Noetherian, M finitely generated, $\mathfrak{a}$ an ideal of A, and $\lambda(M/\mathfrak{a}M) < \infty$. Then the degree of $P_{\mathfrak{a}}(M, n)$ depends only on M and $\mathrm{Supp}(M/\mathfrak{a}M)$.*

Proof Let $\mathfrak{a}'$ be an ideal such that $\mathrm{Supp}(M/\mathfrak{a}M) = \mathrm{Supp}(M/\mathfrak{a}'M)$. We will show that $\deg(P_{\mathfrak{a}}(M, n)) = \deg(P_{\mathfrak{a}'}(M, n))$. Note that

$$\mathrm{Supp}(M/\mathfrak{a}M) = \mathrm{Supp}(A/(\mathrm{Ann}(M) + \mathfrak{a}))$$

and that

$$\mathrm{Supp}(M/\mathfrak{a}'M) = \mathrm{Supp}(A/(\mathrm{Ann}(M) + \mathfrak{a}')).$$

Moreover note that we have that

$$\sqrt{\mathrm{Ann}(M) + \mathfrak{a}} = \bigcap_{\mathfrak{p} \supseteq (\mathrm{Ann}(M)+\mathfrak{a})} \mathfrak{p} = \bigcap_{\mathfrak{p} \supseteq (\mathrm{Ann}(M)+\mathfrak{a}')} \mathfrak{p} = \sqrt{\mathrm{Ann}(M) + \mathfrak{a}'}.$$

Since A is Noetherian, and so $\mathrm{Ann}(M) + \mathfrak{a}$ and $\mathrm{Ann}(M) + \mathfrak{a}'$ are both finitely generated ideals show us that there exists m and m' greater than zero such that:

$$(\mathrm{Ann}(M) + \mathfrak{a}')^m \subseteq \mathrm{Ann}(M) + \mathfrak{a}$$
$$(\mathrm{Ann}(M) + \mathfrak{a})^{m'} \subseteq \mathrm{Ann}(M) + \mathfrak{a}'.$$

We leave it as an exercise to now check that:

$$\begin{aligned} \deg(P_{\mathfrak{a}}(M, n)) &= \deg(P_{(\mathrm{Ann}(M)+\mathfrak{a})}(A, n)) \\ &= \deg(P_{(\mathrm{Ann}(M)+\mathfrak{a}')}(A, n)) \\ &= \deg(P_{\mathfrak{a}'}(M, n)) \end{aligned}$$

■

Definition We define the **Hilbert-Samuel multiplicity** of a module M with respect to $\mathfrak{a}$ by

$$e_{\mathfrak{a}}(M) := \Delta^d P_{\mathfrak{a}}(M, n),$$

where $d > 0$ is the degree of the Hilbert-Samuel polynomial $P_{\mathfrak{a}}(M, n)$.

Corollary 3.16 *If A is Noetherian, and $\mathfrak{a}$ is an ideal of A let*

$$0 \to L \to M \to N \to 0$$

be an exact sequence of finitely generated A-modules such that $\lambda(M/\mathfrak{a}M) < \infty$. Then

$$e_{\mathfrak{a}}(M) = e_{\mathfrak{a}}(L) + e_{\mathfrak{a}}(N).$$

Proof This follows from Proposition 3.13. ■

Proposition 3.17 *If A is Noetherian, M is a finitely generated with $\lambda(M/\mathfrak{a}M) < \infty$ where $\mathfrak{a}$ is an ideal of A, and $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ are the maximal ideals containing $\operatorname{Ann}(M) + \mathfrak{a}$ in A, then setting $\mathfrak{a}_i = \mathfrak{a}A_{\mathfrak{m}_i}$ we have*

$$P_{\mathfrak{a}}(M, n) = \sum_{i=1}^{r} P_{\mathfrak{a}_i}(M_{\mathfrak{m}_i}, n).$$

In other words, to study the Hilbert-Samuel polynomial, it suffices to work over local rings.

Proof To start, note that since $P_{\mathfrak{a}}(M, n) = P_{\operatorname{Ann}(M)+\mathfrak{a}}(M, n)$, we may assume that M is an $A/\operatorname{Ann}(M)$-module. Thus we will assume that $\operatorname{Ann}_A(M) = 0$, and that $\lambda(A/\mathfrak{a}) < \infty$. Hence

$$\operatorname{Ass}_A(A/\mathfrak{q}) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$$

is a set containing only maximal ideals. Now use the Primary Decomposition Theorem, Theorem 1.16, to write

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$$

where each $\mathfrak{q}_i$ is $\mathfrak{m}_i$-primary. Since A is Noetherian, for each i there exists t_i such that $\mathfrak{m}_i^{t_i} \subseteq \mathfrak{q}_i$ and so the $\mathfrak{q}_i$'s are pairwise comaximal. Thus

$$\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_r \quad \text{and so} \quad \mathfrak{a}^n = \mathfrak{q}_1^n \cdots \mathfrak{q}_r^n.$$

Thus by the Chinese Remainder Theorem,

$$A/\mathfrak{a}^n \cong A/\mathfrak{q}_1^n \oplus \cdots \oplus A/\mathfrak{q}_r^n.$$

Now apply $- \otimes_A M$ to obtain

$$M/\mathfrak{a}^n M \cong M/\mathfrak{q}_1^n \oplus \cdots \oplus M/\mathfrak{q}_r^n \qquad (\bigstar)$$

and define

$$\mathfrak{a}_i := \mathfrak{a}A_{\mathfrak{m}_i} = \mathfrak{q}_i A_{\mathfrak{m}_i}.$$

Since $A/\mathfrak{q}_i$ is a local ring with maximal ideal $\mathfrak{m}_i$, we see that

$$A/\mathfrak{q}_i \cong A_{\mathfrak{m}_i}/\mathfrak{q}_i A_{\mathfrak{m}_i} = A_{\mathfrak{m}_i}/\mathfrak{a}_i.$$

Similarly we see that $A/\mathfrak{q}_i^n \cong A_{\mathfrak{m}_i}/\mathfrak{a}_i^n$. Applying $- \otimes_A M$ we see that

$$M/\mathfrak{q}_i^n M \cong M_{\mathfrak{m}_i}/\mathfrak{a}_i^n M_{\mathfrak{m}_i}$$

and so by $(\bigstar)$ we obtain

$$M/\mathfrak{a}^n M \cong \bigoplus_{i=1}^{r} M_{\mathfrak{m}_i}/\mathfrak{a}_i^n M_{\mathfrak{m}_i}.$$

Thus $P_{\mathfrak{a}}(M, n) = \sum_{i=1}^{r} P_{\mathfrak{a}_i}(M_{\mathfrak{m}_i}, n)$. ■

The previous theorem shows us that the degree of $P_{\mathfrak{a}}(M, n)$ is a local property and thus when $\lambda(M/\mathfrak{a}M) < \infty$, so is the Hilbert-Samuel multiplicity of M with respect to $\mathfrak{a}$.

3.3 The Topological Approach

3.3.1 Basic Definitions

We will first recall some basic definitions from topology.

Definition If X is a set, a **topology** on X is a collection of subsets of X such that:

(1) The union of any number of the sets in the collection is again in the collection.

(2) The intersection of any two of the sets in the collection is again in the collection.

(3) X is in the collection.

(4) The empty set is in the collection.

Definition A **topological space** is a set X equipped with a topology.

Definition A set Y is **open** in a topological space X if it one of the sets of the topology of X.

Definition A set Y is **closed** in a topological space X if it is the complement of an open set in X.

Definition Let X be a topological space, $Y \subseteq X$ is called **irreducible** if $Y \neq Y_1 \cup Y_2$, where Y_1, Y_2 are two proper closed subsets of Y and $Y \neq \varnothing$.

Definition The **closure** in a topological space of a subset $Y \subseteq X$ is the intersection of all the closed sets containing Y and is denoted by $\overline{Y}$.

Proposition 3.18 *The following are true:*

(1) *If Y is irreducible, then $\overline{Y}$ is irreducible.*

(2) *Y is irreducible if and only if any two nonempty proper open subsets of Y must have a nonempty intersection.*

(3) *If $x \in X$, then $\overline{\{x\}}$ is an irreducible closed set.*

(4) *Y is irreducible if and only if every nonempty open set is dense in Y.*

Proof Exercise. ■

Definition A closed set is called a **maximal** set if it is not contained in a larger closed set.

Note that every irreducible closed set is contained in a maximal irreducible set by Zorn's Lemma.

Definition A maximal irreducible set in X is called a **component** of X.

Definition If X is a topological space, X is called **Noetherian** if any of the following equivalent conditions hold:

(1) Every nonempty family of open sets has a maximal element.

(2) Any increasing family of open sets terminates.

(3) Every nonempty family of closed sets has a minimal element.

(4) Any decreasing family of closed sets terminates.

Definition A topological space is called **compact** if every open cover of X has a finite subcover.

Remark Our definition of compact above does not include the assumption that X is Hausdorff—recall that a Hausdorff space is one where given any two points you can find open sets containing those points such that the intersection of the open sets is empty. It used to be the case that all compact topological spaces were taken to be Hausdorff and topological spaces that would be otherwise be compact had they been Hausdorff were called **quasicompact**. However, the restriction that compact spaces be Hausdorff is becoming less common and so we will not require compact spaces to be Hausdorff.

Proposition 3.19 *Let X be a Noetherian topological space. The following are true:*

(1) *Any subset of X is Noetherian.*

(2) *X is compact.*

(3) *Any open subset of X is compact.*

(4) *If in addition X is Hausdorff, then X is a finite set with the discrete topology.*

Proof Exercise. ■

Proposition 3.20 *If X is Noetherian, then $X = X_1 \cup \cdots \cup X_n$, where each X_i is a component of X. Moreover, this decomposition is unique and any irreducible closed set of X is contained in one of the X_i's as above.*

Proof If X is Noetherian, then by Proposition 3.19 every subset of X is Noetherian. Hence let

$$\mathcal{S} = \left\{ Y \subseteq X : \begin{array}{l} Y \text{ is closed in } X \text{ and } Y \text{ is not a union} \\ \text{of irreducible closed subsets} \end{array} \right\}.$$

Suppose that $\mathcal{S} \neq \varnothing$. Then $\mathcal{S}$ has a minimal element, call it Z. Z is not irreducible as $Z \in \mathcal{S}$. Thus $Z = Z_1 \cup Z_2$, where neither Z_1 nor Z_2 are elements of $\mathcal{S}$. Hence

$$Z_1 = V_{1,1} \cup V_{1,2} \cup \cdots \cup V_{1,r},$$
$$Z_2 = V_{2,1} \cup V_{2,2} \cup \cdots \cup V_{2,s},$$

where each $V_{1,i}$ is a component of Z_1 and each $V_{2,i}$ is a component of Z_2. Hence

$$Z = V_{1,1} \cup \cdots \cup V_{1,r} \cup V_{2,1} \cup \cdots \cup V_{2,s}.$$

Now throw out $V_{1,i}$ if it is contained in $V_{2,j}$ and vice versa. Hence $\mathcal{S}$ has no minimal elements and thus must be empty.

To see the second part of the proposition, let Y be an irreducible closed set in X. Then

$$\begin{aligned} Y &= Y \cap X \\ &= Y \cap (X_1 \cup \cdots \cup X_n) \\ &= \bigcup_{i=1}^{n} Y \cap X_i. \end{aligned}$$

Since $Y \cap X_i$, is closed and Y is irreducible, we see that $Y \cap X_i = \varnothing$ for each i except one. ■

Definition Let X be a topological space, the **dimension** of X, denoted by $\dim(X)$ is defined as

$$\dim(X) := \sup \left\{ d : \begin{array}{l} \text{there exists a chain } X_0 \supsetneq \cdots \supsetneq X_d \text{ of} \\ \text{length } d \text{ of irreducible closed subsets of } X, \end{array} \right\}.$$

Proposition 3.21 *If X is a Noetherian topological space,*

$$\dim(X) = \sup \dim(X_i)$$

where X_i is a component of X.

3.3.2 The Zariski Topology and the Prime Spectrum

Definition If A is a commutative ring, the **prime spectrum** of A, denoted by $\mathrm{Spec}(A)$, is defined as

$$\mathrm{Spec}(A) := \{\mathfrak{p} : \mathfrak{p} \text{ is a prime ideal of } A\}.$$

Similarly, the set of maximal ideals of a ring A is denoted by

$$\mathrm{MaxSpec}(A) := \{\mathfrak{m} : \mathfrak{m} \text{ is a maximal ideal of } A\}.$$

Example 3.22

(1) *If k is a field,* $\mathrm{Spec}(k) = \{(0)\}$.

(2) $\mathrm{Spec}(\mathbb{Z}) = \{(0), (2), (3), (5), (7), (11), (13), (17), \dots\}$.

(3) $\mathrm{Spec}(\mathbb{C}[X]) = \{(0)\} \cup \{(X - a) : a \in \mathbb{C}\}$.

(4) *If k is an algebraically closed field,* $\mathrm{Spec}(k[X]) = \{(0)\} \cup \{(X - a) : a \in k\}$.

We should note that in general, the prime spectrum of a ring is not easy to compute.

Definition Let $\mathfrak{a}$ be any ideal of A. Define

$$V(\mathfrak{a}) := \{\mathfrak{p} \in \text{Spec}(A) : \mathfrak{p} \supseteq \mathfrak{a}\}.$$

We define the Zariski topology on $\text{Spec}(A)$ as follows: Define $V(\mathfrak{a})$ to be the closed sets of $\text{Spec}(A)$. One should check that:

(1) $V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2) = V(\mathfrak{a}_1 \cap \mathfrak{a}_2) = V(\mathfrak{a}_1\mathfrak{a}_2)$.

(2) $\bigcap_i V(\mathfrak{a}_i) = V(\sum_i \mathfrak{a}_i)$.

Now define the open sets to be the complement of the closed sets, that is, the open sets of $\text{Spec}(A)$ are sets of the form

$$\text{Spec}(A) - V(\mathfrak{a}) = \left\{\mathfrak{p} \in \text{Spec}(A) : \begin{array}{l}\mathfrak{p} \text{ does not contain the generators} \\ \text{of the ideal } \mathfrak{a}\end{array}\right\}$$

for some $\mathfrak{a} \subseteq A$.

On one hand the Zariski topology is very nice. It applies to **all** rings. However, there is a price to be paid. The Zariski topology is not Mr. Roger's Neighborhood. In general, $\text{Spec}(A)$ under the Zariski topology is not Hausdorff. In particular if A contains a unique minimal prime ideal, then then only closed set containing it is all of $\text{Spec}(A)$. This sort of point is everywhere dense and is called a **generic point**.

Definition Let f be any element of A. Define

$$D(f) := \text{Spec}(A) - V(f) = \{\mathfrak{p} \in \text{Spec}(A) : f \notin \mathfrak{p}\}.$$

Proposition 3.23 *$\{D(f) : f \in A\}$ form a basis of* $\text{Spec}(A)$.

Proof First we need to check

$$\text{Spec}(A) = \bigcup_{f \in A} D(f)$$

and this is clear.

Next we should check if whenever $\mathfrak{p} \in D(f)$ and $\mathfrak{p} \in D(g)$, does there exist h such that

$$\mathfrak{p} \in D(h) \subseteq D(f) \cap D(g)?$$

This is true as we merely need to set $h = fg$. ■

Exercise 3.24 *Show that* $\text{Spec}(\mathbb{C}[X]) = \overline{\{(0)\}}$.

Definition Let Z be any subset of $\text{Spec}(A)$. Define

$$I(Z) := \bigcap_{\mathfrak{p} \in Z} \mathfrak{p}.$$

Proposition 3.25 *For any ideal $\mathfrak{a}$ of A,*

$$I(V(\mathfrak{a})) = \bigcap_{\mathfrak{p} \supseteq \mathfrak{a}} \mathfrak{p} = \sqrt{\mathfrak{a}}.$$

Proof Exercise. ■

Proposition 3.26 *If $Z_1 \subseteq Z_2$ are two closed subsets of* $\mathrm{Spec}(A)$*, then*

$$I(Z_2) \subseteq I(Z_1).$$

Proof Exercise. ■

Proposition 3.27 *For any subset Z of* $\mathrm{Spec}(A)$*,*

$$V(I(Z)) = \overline{Z}.$$

Proof Exercise. ■

Remark From the previous propositions, one sees that there is a bijective inclusion reversing correspondence between closed sets of $\mathrm{Spec}(A)$ and the radical ideals of A.

Proposition 3.28 *If Z is a closed subset of* $\mathrm{Spec}(A)$*, then Z is irreducible if and only if $I(Z)$ is a prime ideal.*

Proof ($\Rightarrow$) If $I(Z)$ is not prime, then there exists $a, b \in I(Z)$ such that $a, b \notin I(Z)$ such that $ab \in I(Z)$. Set

$$I_1 = I(Z) + a,$$
$$I_2 = I(Z) + b.$$

Hence $V(I_1) \subseteq Z$ and $V(I_2) \subseteq Z$ and more importantly $V(I_1) \cup V(I_2) \subseteq Z$.

However, $I_1 I_2 \subseteq I(Z)$. Hence $Z \subseteq V(I_1 I_2) = V(I_1) \cup V(I_2)$. Thus $Z = V(I_1) \cup V(I_2)$ is not irreducible.

($\Leftarrow$) Now suppose that $I(Z)$ is prime. Since $I(Z)$ is prime, $V(I(Z)) = \{\mathfrak{p} \in \mathrm{Spec}(A) \,|\, \mathfrak{p} \supseteq I(Z)\} = \overline{\{I(Z)\}}$ is the closure of a point and hence it is irreducible. ■

Proposition 3.29 *If A is a Noetherian ring, then* $\mathrm{Spec}(A)$ *is a Noetherian topological space.*

Proof Suppose A is Noetherian. Suppose $Z_1 \supseteq Z_2 \supseteq \cdots$ is a descending chain of closed subsets of $\mathrm{Spec}(A)$. Thus we have an ascending chain of ideals $I(Z_1) \subseteq I(Z_2) \subseteq \cdots$. Since A is Noetherian, this chain eventually stabilizes, that is, there exists $n > 0$ such that $I(Z_n) = I(Z_m)$ for all $m \geq n$. Therefore, $Z_n = \overline{Z_n} = V(I(Z_n)) = V(I(Z_m)) = \overline{Z_m} = Z_m$ for all $m \geq n$. ■

WARNING 3.30 *The converse of the above proposition is* ***not*** *true. We leave it as an exercise to show that if k is a field, then*

$$A = \frac{k[X_1, \ldots, X_n, \ldots]}{(X_1^2, \ldots, X_n^2, \ldots)}$$

is not a Noetherian ring but $\mathrm{Spec}(A)$ *is a Noetherian topological space.*

Definition (Second Notion of Dimension) If A is a ring, the **Krull dimension**, denoted by $\dim(A)$, is the dimension of the topological space $\mathrm{Spec}(A)$. To be explicit:

$$\dim(A) = \sup\{d \,|\, \text{there exists } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d \text{ such that } \mathfrak{p}_i \in \mathrm{Spec}(A)\}.$$

This notion of dimension is often simply referred to as the **dimension** of a ring. If M is an A-module, then

$$\dim(M) := \dim(A/\operatorname{Ann}(M)) = \dim(\operatorname{Supp}_A(M)).$$

Example 3.31 *While*

$$\dim(A) = \sup\{d : \textit{there exists } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d \textit{ such that } \mathfrak{p}_i \in \mathrm{Spec}(A)\}.$$

Nagata gives an example of a ring A such that A is Noetherian but with infinite dimension in [14]. Let $S = k[x_1, x_2, \ldots]$ be a polynomial ring in infinitely many variables over a field k. Set $\mathfrak{p}_i = (x_{2^{i-1}}, \ldots, x_{2^i-1})$ and $U = \bigcap_{i\geq 1}(S - \mathfrak{p}_i)$. Consider the ring $A = U^{-1}S$. One checks that the maximal ideals of A are exactly $\mathfrak{m}_i = \mathfrak{p}_i A$ for $i \geq 1$ and $A_{\mathfrak{m}_i} \cong R_{\mathfrak{p}_i}$ is a Noetherian ring of dimension 2^{i-1}. Therefore A is Noetherian while $\dim(A) = \sup\{\dim(A_{\mathfrak{m}_i}) \,|\, i \geq 1\} = \infty$.

Example 3.32 *In the ring $\mathbb{C}[X_1, \ldots, X_n]$ we have the chain of prime ideals*

$$(0) \subsetneq (X_1) \subsetneq \cdots \subsetneq (X_1, \ldots, X_n).$$

Thus the dimension of $\mathbb{C}[X_1, \ldots, X_n]$ is at least n.

Suppose that a ring A has finite dimension. If $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ are maximal prime ideals in $\mathrm{Spec}(A)$, then $\dim(A) = d$ implies that there exists a chain of length d ending at one of the $\mathfrak{m}_i$'s. Thus for some i,

$$\dim(A_{\mathfrak{m}_i}) = \dim(A).$$

Hence we see that some questions about the dimension of a ring can be reduced to questions about local rings.

Remark We can characterize dimension in two useful ways:

(1) $\dim(A) = \sup \dim(A_{\mathfrak{m}})$ where $\mathfrak{m} \in \mathrm{MaxSpec}(A)$.

(2) $\dim(A) = \sup \dim(A/\mathfrak{p})$ where $\mathfrak{p}$ is a minimal prime ideal of A.

3.4 Systems of Parameters and the Dimension Theorem

Definition (Third Notion of Dimension) Let A be a local ring and M a finitely generated A-module. Define

$$\dim_{sop}(M) := \inf\left\{ d \,\middle|\, \begin{array}{l}\text{there exists } x_1,\ldots,x_d \in \mathfrak{m} \text{ such}\\ \text{that } \lambda(M/(x_1,\ldots,x_d)M) < \infty\end{array} \right\}.$$

If M is finitely generated as an A-module then, $M/\mathfrak{m}M$ is finitely generated as an $A/\mathfrak{m}$ module. Hence as a vector space over $A/\mathfrak{m}$, $M/\mathfrak{m}M$ has finite dimension. If A is Noetherian, then we see that $M/\mathfrak{m}M$ has finite length. This idea helps motivate our next definition.

Definition Let A be Noetherian and M be a finitely generated A-module. Then if $\dim_{sop}(M) = d$, then any sequence $x_1,\ldots,x_d$ such that

$$\lambda(M/(x_1,\ldots,x_d)M) < \infty$$

is called a **system of parameters** of M.

Theorem 3.33 (The Dimension Theorem) *Let A be a local ring and M a finitely generated A-module. Then*

$$\dim(M) = \dim_{HS}(M) = \dim_{sop}(M).$$

Proof We will show $\dim(M) \leq \dim_{HS}(M) \leq \dim_{sop}(M) \leq \dim(M)$.

$\dim(M) \leq \dim_{HS}(M)$ We proceed by induction on $\dim_{HS}(M)$. Suppose that $\dim_{HS}(M) = 0$. Then

$$P_{\mathfrak{m}}(M,n) = \lambda(M/\mathfrak{m}^n M)$$

is constant for n sufficiently large. Thus for large enough n,

$$\lambda(M/\mathfrak{m}^n M) = \lambda(M/\mathfrak{m}^{n+1}M)$$

which shows us that $\lambda(\mathfrak{m}^n M/\mathfrak{m}^{n+1}M) = 0$. Hence $\mathfrak{m}^n M/\mathfrak{m}^{n+1}M = 0$. So,

$$\mathfrak{m}^n M = \mathfrak{m}^{n+1}M = \mathfrak{m}(\mathfrak{m}^n M)$$

and hence by Nakayama's Lemma, Corollary 0.29, $\mathfrak{m}^n M = 0$ and hence $\mathfrak{m}^n \subseteq \operatorname{Ann}_A(M)$. Since

$$\dim(M) = \dim(A/\operatorname{Ann}(M)) = \dim(A/\sqrt{\operatorname{Ann}(M)}) = \dim(A/\mathfrak{m}),$$

we see that $\dim(M) = 0$.

Now assume $\dim_{HS}(M) = n > 0$. Take any maximal chain

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m$$

in $\mathrm{Supp}(M)$. We need to show $m \leq n$. We may assume that $\mathfrak{p}_0$ is a minimal element of $\mathrm{Supp}(M)$ (else we could consider a longer chain) and hence is a minimal element in $\mathrm{Ass}_A(M)$. So we have an injection

$$A/\mathfrak{p}_0 \hookrightarrow M.$$

Set $N = A/\mathfrak{p}_0$. By Corollary 3.14, $\dim_{HS}(N) \leq \dim_{HS}(M)$. So it suffices to show that $m \leq \dim_{HS}(N)$. Let $x \in \mathfrak{p}_1 - \mathfrak{p}_0$. Consider the short exact sequence

$$0 \longrightarrow N \xrightarrow{x} N \longrightarrow N/xN \longrightarrow 0.$$

By Proposition 3.13, we have that

$$P_{\mathfrak{m}}(N, n) = P_{\mathfrak{m}}(N, n) + P_{\mathfrak{m}}(N/xN, n) - R(n),$$

where $\deg(R(n)) < \deg(P_{\mathfrak{m}}(N, n)) = \dim_{HS}(N)$. But then

$$P_{\mathfrak{m}}(N/xN, n) = R(n).$$

Thus $\dim_{HS}(N/xN) = \deg(P_{\mathfrak{m}}(M, n)) = \deg(R(n)) < n$. By the inductive hypothesis, $\dim(N/xN) \leq \dim_{HS}(N/xN)$. Since

$$\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m$$

is a strict chain of prime ideals in $\mathrm{Supp}(N/xN)$, we have that

$$m - 1 \leq \dim(N/xN) \leq \dim_{HS}(N/xN) \leq n - 1.$$

Hence $\dim(M) = m \leq n = \dim_{HS}(M)$.

$\dim_{HS}(M) \leq \dim_{sop}(M)$ If $n = \dim_{sop}(M)$, consider $x_1, \ldots, x_n$ a system of parameters for M. In this case we have by definition that

$$\lambda(M/(x_1, \ldots, x_n)M) < \infty.$$

Consider $\mathfrak{a} = (x_1, \ldots, x_n)$. Now if we consider the image of $\mathfrak{a}$ in $A/\operatorname{Ann}_A(M)$, we have that

$$\overline{\mathfrak{a}} = (\overline{x}_1, \ldots, \overline{x}_n)$$

where $\overline{x}_i$ is the image of $x_i \in A/\operatorname{Ann}_A(M)$. By Proposition 3.15, $\dim_{HS}(M)$ depends only on M and

$$\mathrm{Supp}(M/\mathfrak{m}M) = \mathrm{Supp}(M/\mathfrak{a}M),$$

and thus we see that

$$\dim_{HS}(M) = \deg(P_{\mathfrak{m}}(M, n)) = \deg(P_{\mathfrak{a}}(M, n)) \leq n,$$

using that $\mathfrak{a}$ is generated by n elements and applying Corollary 3.12.

$\dim_{sop}(M) \leq \dim(M)$ We proceed by induction on $\dim(M)$. Clearly

$$\dim(M) = 0 \Leftrightarrow \mathrm{Supp}_A(M) = \{\mathfrak{m}\} \Leftrightarrow \mathrm{Ass}_A(M) = \{\mathfrak{m}\}, \Leftrightarrow \lambda_A(M) < \infty.$$

So if $\dim(M) = 0$, then $\dim_{sop}(M) = 0$.

Now assume that $\dim(M) = n > 0$. Let $\mathfrak{p}_i$ be the minimal prime ideals in $\mathrm{Supp}(M)$. By Corollary 1.38, these primes are also minimal in $\mathrm{Ass}(M)$ so there are only finitely many such primes. By the Prime Avoidance Lemma, Lemma 0.11, we may pick $x \in \mathfrak{m}$ such that x is not in any of these minimal primes. Thus

$$\dim(M/xM) < \dim(M)$$

and thus by induction, $\dim_{sop}(M/xM) \leq \dim(M/xM)$. But $\dim_{sop}(M) - 1 \leq \dim_{sop}(M/xM)$ and so

$$\dim_{sop}(M) \leq \dim_{sop}(M/xM) + 1 \leq \dim(M/xM) + 1 \leq \dim(M).$$

Putting the above steps together we have shown

$$\dim(M) \leq \dim_{HS}(M) \leq \dim_{sop}(M) \leq \dim(M),$$

and hence $\dim(M) = \dim_{HS}(M) = \dim_{sop}(M)$. ■

Corollary 3.34 *If $(A, \mathfrak{m})$ is a local ring, then it is has finite dimension.*

Proof Since A is Noetherian, $\mathfrak{m}$ is finitely generated, thus $\dim_{sop}(A) = \dim(A)$ is less than or equal to the number of generators of $\mathfrak{m}$. ■

Corollary 3.35 *If $(A, \mathfrak{m})$ is a local ring and M is a finitely generated A-module, then*

$$\dim_A(M) = \dim_{\widehat{A}}(\widehat{M}).$$

Proof We know from Proposition 2.17

$$M/\mathfrak{m}^n M \cong \widehat{M}/\widehat{\mathfrak{m}^n}\widehat{M} \cong \widehat{M}/\widehat{\mathfrak{m}}^n\widehat{M},$$

and so $P_{\mathfrak{m}}(M, n) = P_{\widehat{\mathfrak{m}}}(\widehat{M}, n)$. ■

Corollary 3.36 *If $(A, \mathfrak{m})$ is a local ring, then*

$$\dim(A) = \min\{i : (a_1, \ldots, a_i) = \mathfrak{a} \text{ where } \mathfrak{a} \text{ is } \mathfrak{m}\text{-primary}\}.$$

Proof Let $\dim(A) = n$, then there exists $\mathbf{x} = x_1, \ldots, x_n$ a system of parameters of A such that $\lambda(A/\mathbf{x}) < \infty$. Thus $(x_1, \ldots, x_n)$ is $\mathfrak{m}$-primary. Since $\dim_{sop}(A) = n$, we see that we cannot obtain $y_1, \ldots, y_t$ with $t < n$ such that $\lambda(A/\mathbf{y}) < \infty$. So for any $y_1, \ldots, y_t$ with $t < n$, $(y_1, \ldots, y_t)$ is not $\mathfrak{m}$-primary. ■

Corollary 3.37 *If A is a Noetherian ring, not necessarily local, consider any decreasing chain of prime ideals in A*

$$\mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_i \supsetneq \cdots$$

Then there exists n such that $\mathfrak{p}_n = \mathfrak{p}_{n+1} = \cdots$.

Proof If we localize at $\mathfrak{p}_0$, then $\dim(A_{\mathfrak{p}_0}) < \infty$. So for some n

$$\mathfrak{p}_n A_{\mathfrak{p}_0} = \mathfrak{p}_{n+1} A_{\mathfrak{p}_0} = \cdots$$

and so $\mathfrak{p}_n = \mathfrak{p}_{n+1} = \cdots$. ■

Definition If A is a Noetherian ring and $\mathfrak{p}$ is a prime ideal of A, then the **height** of $\mathfrak{p}$ is

$$\operatorname{ht}(\mathfrak{p}) = \sup \left\{ n : \begin{array}{l} \text{there exists a chain of prime ideals} \\ \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{n-1} \subsetneq \mathfrak{p}_n = \mathfrak{p} \end{array} \right\}.$$

Remark Note that $\operatorname{ht}(\mathfrak{p}) = \dim(A_{\mathfrak{p}})$.

Definition If A is a Noetherian ring and I is any ideal of A, then the **height** of I is

$$\begin{aligned} \operatorname{ht}(I) &= \inf\{\operatorname{ht}(\mathfrak{p}) : I \subseteq \mathfrak{p}\} \\ &= \inf\{\operatorname{ht}(\mathfrak{p}) : \mathfrak{p} \text{ is minimal in } \operatorname{Ass}_A(A/I)\}. \end{aligned}$$

Exercise 3.38 *Check that for any ideal I, $\operatorname{ht}(I) + \dim(A/I) \leq \dim(A)$.*

WARNING 3.39 *Even if I is a prime ideal, the above inequality may be strict.*

Corollary 3.40 (Krull's Ideal Theorem) *Let A be a Noetherian ring and $\mathfrak{p}$ is a prime ideal. Then $\operatorname{ht}(\mathfrak{p}) \leq n$ if and only if there exist $a_1, \ldots, a_n \in \mathfrak{p}$ such that $\mathfrak{p}$ is a minimal prime containing $(a_1, \ldots, a_n)$.*

Proof $\operatorname{ht}(\mathfrak{p}) = \dim(A_{\mathfrak{p}}) \leq n$ if and only if there exists

$$\frac{x_1}{u_1}, \ldots, \frac{x_n}{u_n}$$

in $A_{\mathfrak{p}}$ such that

$$\left(\frac{x_1}{u_1}, \ldots, \frac{x_n}{u_n}\right)$$

is $\mathfrak{p}A_{\mathfrak{p}}$-primary by Corollary 3.36. This is the case if and only if there exist $x_1, \ldots, x_n \in \mathfrak{p}$ and $\mathfrak{p}$ contains $(x_1, \ldots, x_n)$ minimally. ■

Corollary 3.41 (Krull's Principal Ideal Theorem) *Let A be a Noetherian ring and x be an element of A which is not a unit or a zerodivisor. Then every prime which contains (x) minimally has height 1.*

Proof By Corollary 3.40 the minimal prime containing (x) has height at most one. If $\operatorname{ht}(\mathfrak{p}) = 0$, then $\mathfrak{p} \in \operatorname{Ass}(A)$ by Corollary 1.38, which implies that every element of $\mathfrak{p}$ is a zerodivisor, contradicting that x is a nonzerodivisor. Therefore $\operatorname{ht}(\mathfrak{p}) = 1$. ■

Corollary 3.42 *Let $(A, \mathfrak{m})$ be a local ring and x be an element of $\mathfrak{m}$ which is not a zerodivisor. Then $\dim(A/xA) = \dim(A) - 1$.*

Proof This follows from the previous corollary and the definition of dimension. ■

Exercise 3.43 *If $(A, \mathfrak{m})$ is a local ring and M is a finitely generated A-module with $x_1, \ldots, x_i \in \mathfrak{m}$, then*

$$\dim(M/(x_1, \ldots, x_i)M) \geq \dim(M) - i.$$

Equality holds if and only if $x_1, \ldots, x_i$ form part of a system of parameters for M.

Exercise 3.44 *Let A be a Noetherian ring of dimension at least 2. Then A has infinitely many prime ideals of height 1.*

Example 3.45 *A ring A is Artinian if and only if $\dim(A) = 0$.*

Example 3.46 *A PID has dimension one. So in particular, if k is a field, then $\dim(k[X]) = \dim(k[\![x]\!]) = \dim(\mathbb{Z}) = 1$.*

Lemma 3.47 *If A is a ring and $P_1 \subsetneq P_2$ are two prime ideals of $A[X]$ such that*

$$P_1 \cap A = P_2 \cap A = \mathfrak{p},$$

then $P_1 = \mathfrak{p}A[X]$.

Proof Suppose not. Then

$$\mathfrak{p}A[X] \subsetneq P_1 \subsetneq P_2$$

and so

$$(0) \subsetneq P_1/\mathfrak{p}A[X] \subsetneq P_2/\mathfrak{p}A[X]$$

in $A[X]/\mathfrak{p}A[X]$. Set $U = A - \mathfrak{p}$. Since $P_1 \cap U = P_2 \cap U = \varnothing$, and since localizations are exact, we have

$$(0) \subsetneq U^{-1}(P_1/\mathfrak{p}A[X]) \subsetneq U^{-1}(P_2/\mathfrak{p}A[X])$$

is a strict chain of prime ideals in $A_{\mathfrak{p}}[X]/\mathfrak{p}A_{\mathfrak{p}}[X] = U^{-1}(A/\mathfrak{p})[X]$. But this contradicts that $\dim(k[X]) = 1$ when k is a field as $k[X]$ is a PID, hence all primes are principal and so are of height one or zero. Thus $P_1 = \mathfrak{p}[X]$. ■

Lemma 3.48 *If A is Noetherian and I is an ideal of A, then*

$$\mathrm{ht}(I) = \mathrm{ht}(IA[X]).$$

Proof By the Primary Decomposition Theorem, Theorem 1.16,

$$\mathrm{Ass}\left(\frac{A[X]}{IA[X]}\right) = \{\mathfrak{p}_i A[X] : \mathfrak{p}_i \in \mathrm{Ass}(A/I)\},$$

as A/I injects into $A/I[X]$. So it is enough to show that if $\mathfrak{p}$ is a prime ideal in A, then

$$\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{p}A[X]).$$

Suppose that $\mathrm{ht}(\mathfrak{p}) = n$. Then there exist $a_1, \ldots, a_n \in \mathfrak{p}$ such that $\mathfrak{p} \supseteq (a_1, \ldots, a_n)$ minimally. By the Primary Decomposition Theorem, Theorem 1.16, we see that $\mathfrak{p}A[X] \supseteq (a_1, \ldots, a_n)A[X]$ minimally. Thus $\mathrm{ht}(\mathfrak{p}A[X]) \leq n$.

On the other hand, if

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}$$

is a chain of prime ideals where $\mathrm{ht}(\mathfrak{p}) = n$, then

$$\mathfrak{p}_0A[X] \subsetneq \mathfrak{p}_1A[X] \subsetneq \cdots \subsetneq \mathfrak{p}_nA[X] = \mathfrak{p}A[X]$$

is a chain of prime ideals in $A[X]$. Thus $\mathrm{ht}(\mathfrak{p}A[X]) \geq \mathrm{ht}(\mathfrak{p})$ and so we see that $\mathrm{ht}(\mathfrak{p}A[X]) = \mathrm{ht}(\mathfrak{p})$. ■

Theorem 3.49 *If A is a Noetherian ring, $\dim(A[X]) = \dim(A) + 1$.*

Proof First note that given a chain of primes $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ in A, we can construct the chain of primes $\mathfrak{p}_0A[X] \subsetneq \cdots \subsetneq \mathfrak{p}_nA[X] \subsetneq \mathfrak{p}_nA[X] + xA[X]$ in $A[X]$. It is then clear that $\dim(A[X]) \geq \dim(A) + 1$, so it is enough to show $\dim(A[X]) \leq \dim(A) + 1$. If $\dim(A) = \infty$, then there is nothing to prove. We will proceed by induction on the dimension of A. If $\dim(A) = 0$, then for P_i a prime ideal in $A[X]$ write $\mathfrak{p}_i = P_i \cap A$. So if

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$$

then since $\dim(A) = 0$, we have $\mathfrak{p}_0 = \mathfrak{p}_1 = \cdots = \mathfrak{p}_n$. Thus by Lemma 3.47, we have

$$\mathfrak{p}_0A[X] = P_0 = P_1 = \cdots = P_{n-1} \subsetneq P_n.$$

Thus $n \leq 1$ and so we see that $\dim(A[X]) = 1$.

Now suppose that $\dim(A) = d > 0$ and let $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ be a strict chain of prime ideals in $A[X]$. Set $\mathfrak{p}_i = P_i \cap A$.

Case 1: Suppose that $\mathfrak{p}_{n-1} \subsetneq \mathfrak{p}_n$. Then

$$\dim(A_{\mathfrak{p}_{n-1}}) < \dim(A).$$

By induction we then have that $\dim(A_{\mathfrak{p}_{n-1}}[X]) = \dim(A_{\mathfrak{p}_{n-1}}) + 1 \leq \dim(A)$. In $A_{\mathfrak{p}_{n-1}}[X]$ we have a strict chain

$$P_0A_{p_{n-1}} \subsetneq P_1A_{p_{n-1}} \subsetneq \cdots \subsetneq P_{n-1}A_{p_{n-1}}$$

and thus

$$n - 1 \leq \dim(A_{\mathfrak{p}_{n-1}})[X] \leq \dim(A).$$

Thus $n \leq \dim(A) + 1$ and so $\dim(A[X]) = \dim(A) + 1$.

Case 2: Suppose that $\mathfrak{p}_{n-1} = \mathfrak{p}_n$. By Lemma 3.47, we have $P_{n-1} = \mathfrak{p}_{n-1}A[X]$. By Lemma 3.48, we have $\mathrm{ht}(\mathfrak{p}_{n-1}A[X]) = \mathrm{ht}(\mathfrak{p}_{n-1})$. Thus

$$\dim(A) \geq \mathrm{ht}(\mathfrak{p}_{n-1}) = \mathrm{ht}(P_{n-1}) \geq n - 1.$$

Thus $n \leq \dim(A) + 1$ and so we see that $\dim(A[X]) = \dim(A) + 1$. ■

Exercise 3.50 *If A is Noetherian, show that*

$$\dim(A[\![X]\!]) = \dim(A) + 1$$

Hint: Does every maximal ideal in $A[\![X]\!]$ contain X?

Corollary 3.51 *We have that if k is a field, then*

$$\begin{aligned}\dim(k[X_1,\dots,X_n]) &= \dim(k[\![X_1,\dots,X_n]\!]) = n,\\ \dim(\mathbb{Z}[X_1,\dots,X_n]) &= \dim(\mathbb{Z}[\![X_1,\dots,X_n]\!]) = n+1,\\ \dim(\mathbb{Z}_{(p)}[X_1,\dots,X_n]) &= \dim(\mathbb{Z}_{(p)}[\![X_1,\dots,X_n]\!]) = n+1.\end{aligned}$$

Example 3.52 *Let k be a field and consider $A = k[\![w,x,y,z]\!]/(wy-x^2, wz-xy, xz-y^2) \cong k[\![s^3, s^2t, st^2, t^3]\!]$. Let's compute the dimension of A. Set $\mathfrak{p} = (xy-x^2, wz-xy, xz-y^2) \subseteq k[\![w,x,y,z]\!]$. By abuse of notation, we identity w,x,y,z with their images in A. Clearly $\mathfrak{p}A \subsetneq (w,x,y)A \subsetneq (w,x,y,z)A$ is a chain of prime ideals of A of length 2. So* $\dim(A) \geq 2$. *Since*

$$\begin{aligned}A/(w,z) &= k[\![w,x,y,z]\!]/(wy-x^2, wz-xy, xz-y^2, w, z)\\ &= k[\![w,x,y,z]\!]/(w,z,x^2,xy,y^2).\end{aligned}$$

Since $\sqrt{(w,z,x^2,y^2)} = (w,z,x,y)$, which is the maximal ideal of A, the elements w,z form a system of parameters for A and hence $\dim(A) \leq 2$. *Combining these facts we get* $\dim(A) = 2$.

Alternatively, we could compute the Hilbert-Samuel polynomial of A. Write $\mathfrak{m} = (w,x,y,z)$. Clearly $\lambda(A/\mathfrak{m}) = 1$ and $\lambda(A/\mathfrak{m}^2) = 5$. Now consider $A/\mathfrak{m}^n$ for $n \geq 2$. We can identify $A/\mathfrak{m}^n$ with $k[w,x,y,z]/[(wy-x^2, wz-xy, xz-y^2) + (w,x,y,z)^n)$. So let $p \in k[w,x,y,z]$ have degree $n \geq 2$. Since $x^2 - wy, xy - wz, y^2 - xz$ are 0 in the the quotient, we can write $p = a(w,z) + xb(w,z) + yc(w,z)$ uniquely for $a(w,z) \in k[w,z]_n$ and $b(w,z), c(w,z) \in k[w,z]_{n-1}$. So $\lambda(\mathfrak{m}^{n-1}/\mathfrak{m}^n) = (n) + 2(n-1) = 3n-2$. So $P_{\mathfrak{m}}(A) = \deg(\lambda(A/\mathfrak{m}^n)) = \deg\left(\frac{3}{2}n^2 - 2n\right)$. It follows that $\dim(A) = 2$.

Chapter 4

Integral Extensions

4.1 Basic Properties

Definition Let $A \subseteq B$ be commutative rings. An element $b \in B$ is called **integral** over A if b satisfies a monic equation of the form

$$b^n + a_{n-1}b^{n-1} + \cdots + ba_1 + a_0 = 0$$

where $a_0, \ldots, a_{n-1} \in A$. If every element of B is integral over A, we say that B is **integral** over A.

Proposition 4.1 *Let $A \subseteq B$ be commutative rings and let $b \in B$. Then the following are equivalent:*

(1) *b is integral over A.*

(2) *$A[b]$ is a finitely generated A-module.*

(3) *$A[b]$ is contained in a subring of B which is a finitely generated A-module.*

(4) *There exists an $A[b]$-submodule of B which is faithful as an $A[b]$-module and is finitely generated as an A-module.*

Proof (1) $\Rightarrow$ (2) Suppose x is integral over A. Then

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

for some $a_0, \ldots, a_{n-1} \in A$. Thus $A[b]$ is generated by $1, b, b^2, \ldots, b^{n-1}$ as an A-module.

(2) $\Rightarrow$ (3) If $A[b]$ is finitely generated, then taking $B = A[b]$ gives $A[b]$ as a subring of a ring that is finitely generated as an A-module.

(3) $\Rightarrow$ (4) If $A[b] \subseteq C \subseteq B$, where C is a subring of B which is finitely generated as an A-module, then C is faithful as an $A[b]$-module.

(4) $\Rightarrow$ (1) Suppose there exists an $A[b]$-submodule C of B which is faithful as an $A[b]$-module and finitely generated over A. Let $c_1, \ldots, c_n$ be generators for C over A. Since C is an $A[b]$-module, $bc_i \in C$ for all i. So we may write

$$\begin{aligned} bc_1 &= a_{1,1}c_1 + a_{1,2}c_2 + \cdots + a_{1,n}c_n, \\ bc_2 &= a_{2,1}c_1 + a_{2,2}c_2 + \cdots + a_{2,n}c_n, \\ &\vdots \\ bc_n &= a_{n,1}c_1 + a_{n,2}c_2 + \cdots + a_{n,n}c_n. \end{aligned}$$

We can write this in matrix form as

$$\begin{bmatrix} b - a_{1,1} & -a_{1,2} & \cdots & -a_{1,n} \\ -a_{2,1} & b - a_{2,2} & \cdots & -a_{2,n} \\ \vdots & \vdots & & \vdots \\ -a_{n,1} & -a_{n,2} & \cdots & b - a_{n,n} \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Let X be the $n \times n$ matrix shown. Let Y_i be the identity $n \times n$ matrix with the ith column replaced by the column in the above equation with entries $c_1, \ldots, c_n$. Then by the above equation, the ith column in the product $X \cdot Y_i$ will be the 0 column for all i. Thus $\det(X \cdot Y_i) = 0$. Therefore

$$\det(X)c_i = \det(X)\det(Y_i) = \det(X \cdot Y_i) = 0$$

for all i. Since C is a faithful $A[b]$-module, $\det(X) \in \mathrm{Ann}_{A[b]}(C) = 0$. So $\det(X) = 0$ and this monic equation in b gives an integral dependence for b over A. ■

Example 4.2 *If X is an indeterminate over $\mathbb{Z}$, it is clear that $\mathbb{Z}[X]$ is not an integral extension of $\mathbb{Z}$. However, $\mathbb{Z}[X]/(X^2+1) \cong \mathbb{Z}[i]$ is an integral extension of $\mathbb{Z}$.*

Corollary 4.3 *Suppose $B = A[x_1, \ldots, x_n]$ is a finitely generated A-algebra, and suppose each x_i is integral over A. Then B is a finitely generated A-module. In this case we say that B is a* ***module-finite*** *A-algebra.*

Proof Induct on n. The base case follows from the previous proposition. Since x_n is integral over A, it is integral over $C = A[x_1, \ldots, x_{n-1}]$. Therefore $C[x_n] = B$ is a finitely generated C-module. By induction, C is a finitely generated A-module. It follows that B is a finitely generated A-module. ■

Corollary 4.4 *Let $A \subseteq B$ be rings. Then the set S of elements in b that are integral over A is a subring of B containing A.*

Proof Clearly $A \subseteq S$. So consider $x, y \in B$ which are integral over A. By the previous corollary, $A[x, y]$ is a module-finite extension of A. Since $x - y, xy \in A[x, y]$, we get $x - y, xy \in S$ by Proposition 4.1. ■

Definition Let $A \subseteq B$ be commutative rings. Let

$$A' = \{b \in B : b \text{ is integral over } A\}.$$

By Corollary 4.4, A' is a subring of B called the **integral closure** of A in B. If $A' = A$ we say A is **integrally closed** in B. By the above proposition, A' is a subring of B.
If A is a domain, the **integral closure** of A, without reference to another ring, means the integral closure of A in $\mathrm{Frac}(A)$. We denote the integral closure of A by $\widetilde{A}$ and when $A = \widetilde{A}$, we say that A is **integrally closed**.

Theorem 4.5 *If A is a UFD, then A is integrally closed.*

Proof Let $x \in \mathrm{Frac}(A)$ and suppose $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, where $a_0, \ldots, a_{n-1} \in A$. Write $x = \frac{r}{s}$ for relatively prime $r, s \in A$. Clearing denominators we have $s(a_{n-1}r^{n-1} + a_{n-2}r^{n-2}s + \cdots + a_1 r s^{n-2} + a_0 s^{n-1}) = -r^n$, and so s divides r^n. Since A is a UFD and $\gcd(r, s) = 1$, s must be a unit. Therefore $x = \frac{r}{s} \in A$ and hence A is integrally closed. ■

Remark The converse of the previous theorem is false. $A = K[x, y, z]/(xy - z^2)$ and $\mathbb{Z}[\sqrt{-5}]$ are integrally closed domains that are not a UFDs.

Exercise 4.6 *If A is integrally closed in B, and if U is a multiplicatively closed subset of A, then $U^{-1}A$ is integrally closed in $U^{-1}B$.*

Exercise 4.7 *Let $A \subseteq B \subseteq C$ be rings where $A \subseteq B$ and $B \subseteq C$ are both integral extensions. Then $A \subseteq C$ is an integral extension.*

Proposition 4.8 *Let A be a domain. Suppose that for every maximal ideal $\mathfrak{m}$ of A, $A_{\mathfrak{m}}$ is integrally closed. Then A is integrally closed.*

Proof First we show that

$$A = \bigcap_{\mathfrak{m}} A_{\mathfrak{m}}$$

where $\mathfrak{m} \in \mathrm{MaxSpec}(A)$. Note that for every maximal ideal $\mathfrak{m}$, $A \subseteq A_{\mathfrak{m}} \subseteq K$ where $K = \mathrm{Frac}(A)$. So

$$A \subseteq \bigcap_{\mathfrak{m}} A_{\mathfrak{m}}.$$

Now take

$$x \in \bigcap_{\mathfrak{m}} A_{\mathfrak{m}}$$

and let $I = (A :_A x)$. Suppose $I \neq A$. Then $I \subseteq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Since $x \in A_{\mathfrak{m}}$ we can write $x = a/b$ with $b \notin \mathfrak{m}$. But $bx = a \in A$ implies that $b \in I \subseteq \mathfrak{m}$; a contradiction. Therefore $I = A$. In particular $x \in A$, so we have

$$A = \bigcap_{\mathfrak{m}} A_{\mathfrak{m}}.$$

Now let $x \in K$ be integral over A. Then trivially x is integral over $A_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$. Since $A_{\mathfrak{m}}$ is integrally closed for every maximal ideal $\mathfrak{m}$, we have that

$$x \in \bigcap_{\mathfrak{m}} A_{\mathfrak{m}} = A.$$

So A is integrally closed. ■

Remark By the previous proposition, we see that the property of being integrally closed is a local property.

Proposition 4.9 *Suppose $A \subseteq B$ is an integral extension with B a domain. Then A is a field if and only if B is a field.*

Proof ($\Rightarrow$) Suppose A is a field and consider some nonzero $b \in B$. Then b is integral over A. So there is a minimal relation of the form

$$b^n + \lambda_{n-1}b^{n-1} + \cdots + \lambda_1 b + \lambda_0 = 0,$$

where $\lambda_0, \ldots, \lambda_{n-1} \in A$ and $\lambda_0 \neq 0$. If $\lambda_0 = 0$, then by factoring out b and using that B is a domain, we would get an integral relation of smaller degree. So we can write

$$\frac{1}{b} = -\frac{1}{\lambda_0}(b^{n-1} + \lambda_{n-1}b^{n-2} + \cdots + \lambda_1).$$

Therefore B is a field.

($\Leftarrow$) Suppose B is a field and consider some nonzero $a \in A$. Then $a^{-1} \in B$. So a^{-1} is integral over A, meaning we may write

$$\left(\frac{1}{a}\right)^n + \lambda_{n-1}\left(\frac{1}{a}\right)^{n-1} + \cdots + \lambda_1\left(\frac{1}{a}\right) + \lambda_0 = 0,$$

where $\lambda_0, \ldots, \lambda_{n-1} \in A$. Multiplying by a^{n-1} we have

$$\frac{1}{a} = -\lambda_{n-1} - \lambda_{n-2}a - \cdots - \lambda_0 a^{n-1} \in A.$$

Therefore A is a field. ■

Definition Let $f : A \to B$ be a map of rings and let and let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in A and B respectively. We say that $\mathfrak{b}$ **lies over** $\mathfrak{a}$ if $\mathfrak{a} = f^{-1}(\mathfrak{b})$.

Remark This will usually be used in the case where $\mathfrak{a}$ and $\mathfrak{b}$ are prime ideals and $A \hookrightarrow B$ is an integral extension. Then $f^{-1}(\mathfrak{b}) = \mathfrak{a}$ becomes $\mathfrak{b} \cap A = \mathfrak{a}$.

Proposition 4.10 *Suppose $A \subseteq B$ is an integral extension and suppose that P lies over $\mathfrak{p}$. Then P is maximal if and only if $\mathfrak{p}$ is maximal.*

Proof $A/\mathfrak{p} \hookrightarrow B/P$ is an integral extension. The rest then follows from Proposition 4.9. ■

Proposition 4.11 *Suppose $A \subseteq B$ is an integral extension and let x be a nonzerodivisor in B. Then $xB \cap A \neq 0$.*

Proof Pick an integral equation for x of least degree, say

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0, \quad a_i \in A.$$

Then

$$x(x^{n-1} + \cdots + a_1) = -a_0.$$

If $a_0 = 0$, then since x is a nonzerodivisor, $x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1 = 0$ is an integral dependence for x of smaller degree, a contradiction. Therefore $0 \neq a_0 \in xB \cap A$. ■

Proposition 4.12 *Suppose $A \subseteq B$ is an integral extension. Suppose P is a prime ideal of B, I is an ideal of B and $P \subseteq I$. If $P \cap A = I \cap A$ then $P = I$.*

Proof Let $\mathfrak{p} = P \cap A$. Then $A/\mathfrak{p} \hookrightarrow B/P$ is an integral extension. If $I \neq P$, then $I/P \neq 0$. So let $0 \neq x \in I/P$. Since B/P is a domain x is a nonzerodivisor on B/P. So by the previous proposition $x(B/P) \cap A/\mathfrak{p} \neq 0$. But this contradicts $I \cap A = \mathfrak{p}$. Therefore $I = P$. ■

Proposition 4.13 *Suppose $A \subseteq B$ is an integral extension and suppose P lies over $\mathfrak{p}$. Then P contains $\mathfrak{p}B$ minimally.*

Proof Suppose there exists a prime ideal Q of B such that $\mathfrak{p}B \subseteq Q \subseteq P$. Then

$$\mathfrak{p} \subseteq \mathfrak{p}B \cap A \subseteq Q \cap A \subseteq P \cap A = \mathfrak{p}.$$

Then $P \cap A = Q \cap A$. By the previous proposition $Q = P$. ■

Proposition 4.14 *Suppose $A \subseteq B$ is an integral extension and suppose*

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$$

is a strict chain of prime ideals in B. Then

$$P_0 \cap A \subsetneq P_1 \cap A \subsetneq \cdots \subsetneq P_n \cap A$$

is a strict chain of prime ideals in A. In particular $\dim(B) \leq \dim(A)$.

Proof Follows from Proposition 4.12. ■

Definition Let $f : A \to B$ be a map of rings. We say f has the **Lying-Over Property** if for every prime ideal $\mathfrak{p}$ of A there exists a prime ideal P of B such that $\mathfrak{p} = f^{-1}(P)$.

Definition Let $f : A \to B$ be a map of rings, $\mathfrak{a}$ an ideal of A, and $\mathfrak{b}$ an ideal of B such that $f^{-1}(\mathfrak{b}) = \mathfrak{a}$. We say f has the **Going-Up Property** if given a chain of ideals $\mathfrak{a} \subseteq \mathfrak{p}$ where $\mathfrak{p}$ is a prime ideal, then there exists a prime ideal P in B containing $\mathfrak{b}$ such that $f^{-1}(P) = \mathfrak{p}$. Pictorially, the situation can be described by:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \cup & & \cup \\ \mathfrak{p} & \longrightarrow & \exists P \\ \cup & & \cup \\ \mathfrak{a} & \longrightarrow & \mathfrak{b} \end{array}$$

Remark Note that if $\mathrm{Ker}(f) \subseteq \sqrt{0}$, then the Going-Up Property implies the Lying-Over Property as we may take $\mathfrak{b} = (0)$ and $\mathfrak{a} = \mathrm{Ker}(f)$. In particular, the Going-Up Property implies the Lying-Over Property when f is injective.

For the purposes of integral extensions, $f : A \to B$ is an inclusion and $f^{-1}(P)$ becomes $P \cap A$. We will see through exercises later in the section that the generality of the previous definitions will be used when discussing flat and faithfully flat maps.

Theorem 4.15 (Lying-Over and Going-Up for Integral Extensions) *Suppose*

$$A \hookrightarrow B$$

is an integral extension. Let $\mathfrak{p}$ be a prime ideal in A. Then there exists a prime ideal P in B lying over $\mathfrak{p}$. Moreover, P may be chosen to contain any ideal I such that $I \cap A \subseteq \mathfrak{p}$. In other words, integral extensions satisfy the Lying-Over and Going-Up Properties.

Proof Factoring out I and $A \cap I$ in B and A respectively, we may assume that $I = 0$. Now let $U = A - \mathfrak{p}$. Then $A_{\mathfrak{p}} \hookrightarrow U^{-1}B$ is an integral extension. Pick a maximal ideal $\mathfrak{m}$ in $U^{-1}B$. Then $\mathfrak{m} \cap A_{\mathfrak{p}}$ is a maximal ideal of $A_{\mathfrak{p}}$ by Proposition 4.32. Thus $\mathfrak{m} \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$. Now take $P = i_B^{-1}(\mathfrak{m}) \subseteq B$, where i_B is the localization map $i_B : B \to U^{-1}B$. Then P lies over $\mathfrak{p}$. ■

Corollary 4.16 (Integral Extensions Preserve Dimension) *If $A \hookrightarrow B$ is an integral extension, then* $\dim(B) = \dim(A)$.

Proof Let $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ be a strict chain of prime ideals of A. By Theorem 4.15 there is a prime ideal P_0 lying over $\mathfrak{p}_0$. By Theorem 4.15 there is a prime ideal P_1 lying over $\mathfrak{p}_1$ containing P_0. Similarly we may pick $P_2, \ldots, P_n$ a necessarily strict ascending chain of prime ideals lying over $\mathfrak{p}_2, \ldots, \mathfrak{p}_n$. In particular we have a strict chain of prime ideals $P_0 \subsetneq \cdots \subsetneq P_n$ in B. Therefore $\dim(B) \geq \dim(A)$. But by Proposition 4.14, $\dim(B) \leq \dim(A)$. Therefore $\dim(B) = \dim(A)$. ■

Corollary 4.17 *Suppose $A \subseteq B$ is an integral extension. Let I be any ideal in B lying over an ideal $\mathfrak{a}$ in A. Then* $\mathrm{ht}(I) \leq \mathrm{ht}(\mathfrak{a})$.

Proof Take any minimal prime $\mathfrak{p} \supseteq \mathfrak{a}$ so that $\mathrm{ht}(\mathfrak{a}) = \mathrm{ht}(\mathfrak{p})$. By Theorem 4.15 there is a prime ideal P of B lying over $\mathfrak{p}$ such that $P \supseteq I$. By Proposition 4.14 it follows that $\mathrm{ht}(P) \leq \mathrm{ht}(\mathfrak{p})$. Thus

$$\mathrm{ht}(I) = \inf_{Q \supseteq I} \mathrm{ht}(Q) \leq \mathrm{ht}(P) \leq \mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{a}).$$

■

Proposition 4.18 *Suppose A is an integral domain, $K = \mathrm{Frac}(A)$, L is an algebraic extension of K, and B is the integral closure of A in L. Then:*

(1) *$L = U^{-1}B$ where $U = A - \{0\}$; that is, if $x \in L$, then $x = b/a$ where $b \in B$ and $0 \neq a \in A$.*

(2) *If $\sigma \in \mathrm{Gal}_K(L)$ and if a prime $P \subseteq B$ lies over the prime $\mathfrak{p} \subseteq A$, then $\sigma(P)$ also lies over $\mathfrak{p}$.*

Proof (1) We have the following diagram:

$$\begin{array}{ccc} B & \hookrightarrow & L \\ \uparrow & & \uparrow \\ A & \hookrightarrow & K \end{array}$$

Let $x \in L$. Since L is an algebraic extension of K, there is a relation of the form

$$x^n + \lambda_{n-1}x^{n-1} + \cdots + \lambda_0 = 0,$$

where $\lambda_0, \ldots, \lambda_{n-1} \in K$. Since $K = \mathrm{Frac}(A)$, by taking a common denominator we can write $\lambda_i = a_i/a$ for each i where $a, a_0, \ldots, a_{n-1} \in A$. Replacing the λ_i's and multiplying by a^n we get

$$(ax)^n + a_{n-1}(ax)^{n-1} + a_{n-2}a(ax)^{n-2} + \cdots + a_n a^{n-1} = 0.$$

Thus ax is integral over A, and so $ax \in B$. Hence $x = \frac{b}{a}$ for some $b \in B$.

(2) Let $\sigma \in \mathrm{Gal}_K(L)$. Let $x \in B$. Then

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

Applying σ we get

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

In particular $\sigma(B)$ is integral over A. Since B is the integral closure of A in L, $\sigma(B) \subseteq B$. Similarly we have $\sigma^{-1}(B) \subseteq B$ and hence $B \subseteq \sigma(B)$. Therefore $\sigma(B) = B$. Hence σ is an automorphism of B. Let P be a prime ideal lying over $\mathfrak{p}$. Since $P \cap A = \sigma(P) \cap A = \mathfrak{p}$, $\sigma(P)$ also lies over $\mathfrak{p}$. ■

For the next couple theorems we recall some ideas from basic algebra.

Definition Let L be an algebraic extension of K. Then L is said to be **normal** over K if L is the splitting field over K of a finite number of polynomials.

Definition Let L be a field extension of K. Then L is said to be **separable** over K if L is generated over K by a set of elements each of which is the root of a separable polynomial in $K[x]$, i.e. an irreducible polynomial with distinct roots. An extension that is not separable is called **inseparable**.

Definition Let L be a field extension of K in characteristic $p \neq 0$. Then L is said to be **purely inseparable** over K if there exists $n > 0$ such that $\alpha^{p^n} \in K$ for all $\alpha \in L$.

Proposition 4.19 *Let L be a normal extension of K and let $G = \mathrm{Gal}_K(L)$. Then L is separable over L^G and L^G is purely inseparable over K. Note that L^G denotes the subfield of L fixed by G.*

Proof See your favorite algebra text, or see [7]. ■

Theorem 4.20 *Let A be an integrally closed domain and $K = \mathrm{Frac}(A)$. Let L be a normal extension of K, let $G = \mathrm{Gal}_K(L)$, and let B be the integral closure of A in L. Let $\mathfrak{p} \subseteq A$ be a prime ideal. Then G acts transitively on the set of prime ideals in B lying over $\mathfrak{p}$.*

Proof First assume that $[L : K] < \infty$. Write

$$G = \{\sigma_1, \ldots, \sigma_n\}.$$

Let P, Q be primes of B lying over $\mathfrak{p}$. It is enough to show that $P \subseteq \sigma_i(Q)$ for some i, for then by Proposition 4.12, $P = \sigma_i(Q)$. Suppose $P \not\subseteq \sigma_i(Q)$ for any i. Then by prime avoidance, Lemma 0.11, $P \not\subseteq \bigcup_{i=1}^n \sigma_i(Q)$. So there exists $x \in P$ with $x \notin \sigma_i(Q)$ for all i. Let

$$y = \sigma_1(x) \cdots \sigma_n(x).$$

Since $\sigma_i(y) = y$ for all i, we have $y \in L^G$ by the previous theorem. Thus $y^m \in K$ for some $m \in \mathbb{N}$ by the previous proposition. But then $y^m \in P \cap K = \mathfrak{p}$. Thus $y \in \mathfrak{p} \subseteq Q$. Thus $\sigma_i(x) \in Q$ for some i. Hence, $x \in \sigma_i(Q)$ for some i, a contradiction. Thus $P \subseteq \sigma_i(Q)$ for some i, and by the earlier remarks, $P = \sigma_i(Q)$.

Now assume that $[L : K] = \infty$. Then we can write $L = \bigcup_i L_i$ where for each i, L_i is a finite normal extension of K. Let P, Q be primes of B lying over $\mathfrak{p}$ in A. Let $P_i = P \cap L_i$ and $Q_i = Q \cap Q_i$. Let $G_i = \mathrm{Gal}_K(L_i)$. Let us write $(L_i, \sigma_i) \leq (L_j, \sigma_j)$ if $L_i \subseteq L_j$ and $\sigma_j|_{L_i} = \sigma_i$. This puts a partial ordering on the set of pairs

$$\{(L_i, \sigma_i) : \sigma_i \in \mathrm{Gal}_K(L_i) \text{ and } \sigma_i(P_i) = Q_i\}.$$

Further any chain

$$(L_{i_1}, \sigma_{i_1}) \leq (L_{i_2}, \sigma_{i_2}) \leq \cdots$$

has a least upper bound, namely $(\bigcup_j L_{i_j}, \bigcup_j \sigma_{i_j})$. So we may apply Zorn's Lemma to state the existence of a maximal element (L_0, σ_0). We claim that $L_0 = L$. So suppose $L_0 \subsetneq L$. Pick $x \in L - L_0$. Let L' be a splitting field for x over L_0 inside L. By assumption

$$\begin{aligned}\sigma_0(P \cap L_0) &= Q \cap L_0 \\ &= Q_0.\end{aligned}$$

Let $P' = P \cap L'$ and $Q' = Q \cap L'$ and let σ' be any extension of σ_0 to $\mathrm{Gal}_K(L')$. Then $\sigma'(P')$ and Q' both lie over Q_0. By the finite case there exists $\sigma'' \in \mathrm{Gal}_{L_0}(L')$ such that $\sigma''(\sigma'(P')) = Q'$. Write $\sigma = \sigma'' \circ \sigma' \in \mathrm{Gal}_K(L')$. Then $\sigma(P') = Q'$ and $(L_0, \sigma_0) < (L', \sigma)$, a contradiction. ■

Definition Let $f : A \to B$ be a map of rings. We say the f has the **Going-Down Property** if for all for $\mathfrak{p}, \mathfrak{q} \in \mathrm{Spec}(A)$ and $Q \in \mathrm{Spec}(B)$ where $\mathfrak{p} \subsetneq \mathfrak{q}$ with Q lying over $\mathfrak{q}$, then there exists a prime P of B such that P lies over $\mathfrak{p}$ and $P \subsetneq Q$. Pictorially the situation can be described by:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \cup & & \cup \\ \mathfrak{q} & \longrightarrow & Q \\ \cup & & \cup \\ \mathfrak{p} & \longrightarrow & \exists P \end{array}$$

Theorem 4.21 (Going-Down for Integral Extensions) *Suppose A is an integrally closed domain, $A \hookrightarrow B$ is an integral extension of rings, and B is torsion free over A. Then the Going-Down Property holds.*

Proof There are two basic cases for the proof.

Case 1. Suppose B is a domain. Let $K = \mathrm{Frac}(A)$ and let $L = \mathrm{Frac}(B)$. Let $\overline{L}$ to be the normal closure of L and let $\overline{B}$ to be the integral closure of B in $\overline{L}$. By the Lying-Over Property, we obtain $\overline{Q}$ in the following diagram:

$$\begin{array}{ccc} B & \hookrightarrow & \overline{B} \\ \cup & & \cup \\ Q & \longrightarrow & \overline{Q} \end{array}$$

By the Going-Up Property there is a prime ideal $Q' \subseteq \overline{B}$ lying over $\mathfrak{q}$ and $P' \subseteq \overline{B}$ lying over $\mathfrak{p}$ such that $P' \subseteq Q'$:

$$\begin{array}{ccc} A & \hookrightarrow & \overline{B} \\ \cup & & \cup \\ \mathfrak{q} & \longrightarrow & Q' \\ \cup & & \cup \\ \mathfrak{p} & \longrightarrow & P' \end{array}$$

Since $\overline{Q}$ and Q' both lie over $\mathfrak{q}$ and since $\overline{L}/K$ is normal by Theorem 4.20, there exists $\sigma \in \mathrm{Gal}_K(\overline{L})$ such that $\sigma(Q') = \overline{Q}$. Thus $\sigma(P')$ lies over $\mathfrak{p}$ and $\sigma(P') \subseteq \sigma(Q') = \overline{Q}$. Now take $P = \sigma(P') \cap B$. Then $P \subseteq \overline{Q} \cap L = Q$ and $P \cap A = \mathfrak{p}$ by construction.

Case 2. Now suppose B is torsion free over A. Suppose $\mathfrak{p} \subseteq \mathfrak{q}$ are prime. We want to apply Case 1, so given

$$\begin{array}{ccc} A & \hookrightarrow & B \\ \cup & & \cup \\ \mathfrak{q} & \longrightarrow & Q \\ \cup & & \\ \mathfrak{p} & & \end{array}$$

we first want a prime ideal $P \subseteq Q$ such that $P \cap A = \mathfrak{p}$. Let $U_1 = A - \mathfrak{p}$ and let $U_2 = B - Q$ and set $U = U_1U_2$. Since B is torsion free over A, $0 \notin U$. It follows that U is a multiplicative set in B and that $\eta : B \hookrightarrow U^{-1}B$. Let P' be any prime ideal of $U^{-1}B$. Set $P = \eta^{-1}(P') \subseteq B$. One should check that $P \subseteq Q$ and $P \cap A = (0)$. Setting $\overline{B} = B/P$ we still have an injection $A \hookrightarrow \overline{B}$ where $\overline{B}$ is a domain. We now have the following diagram

$$\begin{array}{ccc} A & \hookrightarrow & \overline{B} \\ \cup & & \cup \\ \mathfrak{q} & \longrightarrow & \overline{Q} \\ \cup & & \\ \mathfrak{p} & & \end{array}$$

where $\overline{Q} = Q/P$ is a prime in $\overline{B}$ lying over $\mathfrak{q}$. By Case 1 there is a prime ideal $\overline{P} \subseteq \overline{B}$ contained in $\overline{Q}$ lying over $\mathfrak{p}$. Finally, if $\varphi : B \to \overline{B}$, take $P'' = \varphi^{-1}(\overline{P})$ and check that $P'' \subseteq Q$ and that P'' lies over $\mathfrak{p}$ as required. ■

Exercise 4.22 *To show that the both the hypotheses are necessary in the Going-Down Theorem, we give two examples, but leave the details as an exercise.*

(1) *Let $A = k[X, Y]$ and $B = k[X, Y, Z]/(Z^2 - Z, YZ)$ so that $A \hookrightarrow B$ is an integral extension but B is not torsion free over A. Take $Q = (Z - 1, X, Y) \subseteq B$, $\mathfrak{q} = (X, Y) \subseteq A$ and $\mathfrak{p} = (x) \subseteq A$. Show that Q lies over $\mathfrak{q}$ but contains no prime ideal lying over $\mathfrak{p}$.*

(2) *Let $A = k[X^2, XY, Y]$ and $B = k[X, Y]$ so that $A \hookrightarrow B$ is an integral extension but A is not integrally closed. Take $Q = (X - 1, Y)$, $\mathfrak{q} = (XY, Y, X^2 - 1)$ and $\mathfrak{p} = (X^2 - 1, XY - Y)$. Show that Q lies over $\mathfrak{q}$ but contains no prime lying over $\mathfrak{p}$.*

Corollary 4.23 *Suppose A is an integrally-closed domain, $A \hookrightarrow B$ is an integral extension of rings, and B is torsion free over A. If $\mathfrak{p}$ is a prime ideal in A and P is a prime ideal in B, then P lies over $\mathfrak{p}$ if and only if $P \supseteq \mathfrak{p}B$ minimally.*

Proof ($\Rightarrow$) This follows from Proposition 4.13.
($\Leftarrow$) Suppose $P \supseteq \mathfrak{p}B$ minimally. Let $\mathfrak{q} = P \cap A$. Suppose further that $\mathfrak{q} \neq \mathfrak{p}$. Then by the Going-Down Theorem, there exists a prime $Q \subseteq P$ such that $Q \cap A = \mathfrak{p}$. Since $Q \cap A = \mathfrak{p}$, $Q \supseteq \mathfrak{p}B$. This contradicts that P contains $\mathfrak{p}B$ minimally. Thus $P \cap A = \mathfrak{p}$. ■

Exercise 4.24 *Suppose A is an integrally-closed domain, $A \hookrightarrow B$ is an integral extension of rings, and B is torsion free over A. Let $\mathfrak{b}$ be an ideal in B and $\mathfrak{a} = \mathfrak{b} \cap A$. Then* $\operatorname{ht} \mathfrak{b} = \operatorname{ht} \mathfrak{a}$.

Exercise 4.25 *Let $A \to B$ be flat. Then the Going-Down Property holds. (And hence* $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ *is an open map.)*

Example 4.26 *Let k be a field. Let*

$$P = (x^3 - yz, y^2 - xz, z^3 - x^2 z) \subseteq k[x, y, z]$$

and let $A = k[x, y, z]/P$. What is $\dim A$*? We note that $A \cong k[t^3, t^4, t^5]$ and that $k[t^3, t^4, t^5] \hookrightarrow k[t]$ is an integral extension. Since* $\dim k[t] = 1$, $\dim A = 1$.

Exercise 4.27 *Suppose $f : A \to B$ is a ring homomorphism. Then the following hold:*

(1) *If P is a prime ideal of B, then $f^{-1}(P)$ is a prime ideal of A.*

(2) *If we define f^* as follows*

$$\begin{aligned} f^* : \operatorname{Spec}(B) &\to \operatorname{Spec}(A), \\ P &\mapsto f^{-1}(P), \end{aligned}$$

f^* is a continuous map in the Zariski topology.

(3) $\operatorname{Spec}(A)$ *is compact.*

(4) *Suppose A and B are Noetherian. The map f has the Going-Up Property if and only if f^* is a closed map, i.e. if $V \subseteq \operatorname{Spec}(B)$ is a closed set, then so is $f^*(V)$. (Can you do this without the Noetherian hypothesis?)*

(5) *Suppose A and B are Noetherian. The map f has the Going-Down Property if and only if f^* is an open map, i.e. if $U \subseteq \operatorname{Spec}(B)$ is an open set, then so is $f^*(U)$. (Can you do this without the Noetherian hypothesis?)*

Exercise 4.28 *Suppose $f : A \to B$ is a ring map such that B a flat A-module. Then f has the Going-Down Property and hence by the previous exercise f^* is an open map.*

Exercise 4.29 *Let $f : A \to B$ be a ring map such that B is a flat A-module. Then $f^* : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is surjective (i.e. f satisfying Lying-Over) if and only if B is faithfully flat over A.*

4.2 Valuation Rings

Definition Let R be an integral domain with field of fractions $K = \text{Frac}(R)$. Then R is a **valuation ring** of K if for every nonzero $x \in K$, $x \in R$ or $x^{-1} \in R$ (or both).

Example 4.30 *Note that fields are always valuation rings as the defining condition is vacuously true. For an example that is not a field, consider $\mathbb{Z}_{(p)}$. If $\frac{x}{y} \in \mathbb{Q} \setminus \mathbb{Z}_{(p)}$ with x, y relatively prime, then $p|y$. Thus $p \nmid x$ and so $\frac{y}{x} \in \mathbb{Z}_{(p)}$.*

Theorem 4.31 *Let R be a valuation ring. If I and J are ideals of R then $I \subseteq J$ or $J \subseteq I$; in particular, R is quasi-local.*

Proof Suppose $J \not\subseteq I$. Then there exists and element $x \in J - I$. Fix any nonzero $y \in I$. If $\frac{x}{y} \in R$, then $x = y\frac{x}{y} \in I$, a contradiction; so $\frac{x}{y} \notin R$. Since R is a valuation ring, $\frac{y}{x} \in R$ and so $y = x\frac{y}{x} \in J$. Therefore $I \subseteq J$.

It follows that the ideals of R form a totally ordered set. By Zorn's Lemma, R has a unique maximal ideal. ■

Proposition 4.32 *Let $(R, \mathfrak{m})$ be a valuation ring with field of fractions $K = \text{Frac}(R)$. Then*

(1) $\mathfrak{m} = \{x \in K \mid x^{-1} \notin R\}$.

(2) *R is integrally closed.*

(3) *If R' is a ring such that $R \subseteq R' \subseteq K$, then R' is a valuation ring.*

Proof (1) Since R is quasi-local, $x \in R$ is invertible if and only $x^{-1} \in R$ if and only if $x \notin \mathfrak{m}$.
(2) Let $x \in K$ satisfy the integral dependence $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$. Suppose $x \notin R$ and thus $x^{-1} \in \mathfrak{m}$. Dividing the integral dependence by x^n we have Therefore $1 = -a_{n-1}x^{-1} - a_{n-2}x^{-2} - \cdots - a_0x^{-n} \in \mathfrak{m}$, which is a contradiction.
(3) Suppose $x \in K \setminus R'$. Then $x \notin R$. Since R is a valuation ring, $x^{-1} \in R \subseteq R'$. ■

Proposition 4.33 *Let K be a field, $A \subseteq K$ a subring, and $\mathfrak{p}$ a prime ideal of A. Then there exists a valuation ring $(R, \mathfrak{m})$ of K such that $R \subseteq A$ and $\mathfrak{m} \cap A = \mathfrak{p}$.*

Proof Replacing A by $A_{\mathfrak{p}}$, we may assume that A is local and $\mathfrak{p}$ is the maximal ideal of A. Let $\mathcal{F}$ be the set of subrings B of K containing A such that $1 \notin \mathfrak{p}B$. Since $A \in \mathcal{F}$ and since unions of chains in $\mathcal{F}$ are also in $\mathcal{F}$, Zorn's Lemma applies. So there is a maximal subring $R \in \mathcal{F}$. Since $\mathfrak{p}R \neq R$, there is a maximal ideal $\mathfrak{m}$ of R containing $\mathfrak{p}R$. Then $R \subseteq R_{\mathfrak{m}} \in \mathcal{F}$ and so $R = R_{\mathfrak{m}}$ by the maximality of R. Since $\mathfrak{p} \subseteq \mathfrak{m}$ and since $\mathfrak{p}$ is maximal in A, $\mathfrak{m} \cap A = \mathfrak{p}$. We claim then that $(R, \mathfrak{m})$ is a valuation ring.

Suppose $x \in K - R$. Since $R \subsetneq R[x]$, $R[x] \notin \mathcal{F}$ and so $1 \in \mathfrak{p}R[x]$. So we can write

$$1 = a_0 + a_1x + \cdots + a_nx^n$$

for some $a_0, \ldots, a_n \in \mathfrak{p}R$. Since $1 - a_0$ is a unit, we can rewrite this as

$$1 = b_1 x + \cdots b_n x^n,$$

where $b_1, \ldots, b_n \in \mathfrak{m}$. Among all such relations, pick one with n minimal.

If $x^{-1} \notin R$, then $R[x^{-1}] \notin \mathcal{F}$ and so $1 \in \mathfrak{p}R[x^{-1}]$. As above we can write

$$1 = c_1 x^{-1} + \cdots + c_m x^{-m}$$

for some $c_1, \ldots, c_m \in \mathfrak{m}$. Again we pick such a relation with m minimal.

If $n \geq m$, then

$$\begin{aligned} 1 &= b_1 x + \cdots + b_n x^n \\ &= b_1 x + \cdots + b_n x^n - b_n x^n (1 - c_1 x^{-1} + \cdots + c_m x^{-m}) \\ &= b_1 x + \cdots + b_{n-m-1} x^{n-m-1} + (b_{n-m} - b_n c_m) x^{n-m} + \cdots + (b_{n-1} - b_n c_1) x^{n-1} \end{aligned}$$

is a relation of smaller degree than n, a contradiction. (If a constant appears, we modify the equation as we did above.) Similarly if $n < m$, then we get a contradiction by exchanging the roles of x and x^{-1}. Therefore $x^{-1} \in R$ and so R is a valuation ring.

■

Theorem 4.34 *Let K be a field and $A \subseteq K$ a ring. Let B be the integral closure of A in K. Then B is the intersection of all valuation rings of K containing A.*

Proof Let B' be the intersection of all valuation rings of K containing A. Since every valuation ring is integrally closed, $B \subseteq B'$. Suppose $x \in K$ is not integral over A so that $x \notin B$. We wish to show that $x \notin B'$; that is, there is some valuation ring R of K with $x \notin R$. Let $y = x^{-1}$. If $1 \in yA[y]$, then $1 = a_1 y + a_2 y^2 + \cdots + a_n y^n$ for some $a_1, \ldots, a_n \in A$. Multiplying this equation by x^n we get $x^n - a_1 x^{n-1} - a_2 x^{n-2} - \cdots - a_n = 0$, an integral dependence for x. Since x is not integral over A, $1 \notin yA[y]$ and so $yA[y]$ is a proper ideal of $A[y]$. So there is a maximal ideal $\mathfrak{n} \subseteq A[y]$ containing $yA[y]$. By the previous proposition, there is a valuation ring $(R, \mathfrak{m})$ such that $A[y] \subseteq R \subseteq K$ with $\mathfrak{m} \cap A[y] = \mathfrak{n}$. Since $x^{-1} = y \in yA[y] \subseteq \mathfrak{m}$, $x \notin R$ by Proposition 4.32. ■

Definition A **totally ordered abelian group** is a pair $(G, \leq)$, where G is an abelian group written additively, $\leq$ is a total order on G and for all $x, y, z \in G$, $x \leq y \Rightarrow x + z \leq y + z$.

It is easy to check that $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$ and $(\mathbb{R}, \leq)$ are totally ordered abelian groups, as is $(\mathbb{Z}^n, \leq_{\text{lex}})$, where $\leq_{\text{lex}}$ denotes the lexicographic order.

Now let R be a valuation ring with field of fractions $K = \text{Frac}(R)$. Let $\Gamma = K^*/R^*$ with group law written additively. For $\alpha, \beta \in \Gamma$, define $\alpha \leq \beta$ if $\beta - \alpha$ is in the image of $R \smallsetminus \{0\} \to \Gamma$. It follows from the definition of a valuation ring that $(\Gamma, \leq)$ is a totally ordered abelian group.

Definition Let K be a field and let $(G, \leq)$ be a totally ordered abelian group. Then a group homomorphism $\nu : K^* \to G$ is a **valuation** if

$$\nu(x+y) \geq \min\{\nu(x), \nu(y)\}$$

for all $x, y \in K$ such that $x + y \neq 0$.

Remark In some texts, a valuation is extended to all of K by insisting that $\nu(0) = \infty$, where $\infty > x$ for all $x \in G$. This of course breaks the group homomorphism property as K is not a group under multiplication, nor is $G \cup \{\infty\}$ under addition.

It is easy to check from the definition that if R is a valuation ring with fraction field K as above, $\nu : K^* \twoheadrightarrow K^*/R^* = \Gamma$ is a valuation. Moreover we see that $\nu(x) = 0$ if and only if $x \in R^*$. So from each valuation ring, we get a valuation. The following converse also holds.

Proposition 4.35 *Let K be a field and let $\nu : K^* \to (G, \leq)$ be a valuation. Set*

$$R = \{x \in K^* \mid \nu(x) \geq 0\} \cup \{0\},$$
$$\mathfrak{m} = \{x \in K^* \mid \nu(x) > 0\} \cup \{0\}.$$

Then $(R, \mathfrak{m})$ is a valuation ring with group of units

$$R^* = \mathrm{Ker}(\nu) = \{x \in K^* \mid \nu(x) = 0\}.$$

Proof Exercise. ■

Proposition 4.36 *Let R be a ring. Then the following are equivalent:*

(1) *R is a valuation ring.*

(2) *$(R, \mathfrak{m})$ is a quasi-local domain such that every finitely-generated ideal is principal.*

Proof ($\Rightarrow$) That every valuation ring is quasi-local and a domain follows from the definition. Let $f_1, \ldots, f_n \in R$. Pick f_i with $\nu(f_i)$ minimal. For $j \neq i$, $\nu(f_j) - \nu(f_i) \geq 0$ and by the previous proposition $\frac{f_j}{f_i} \in R$. Thus $f_j = f_i \frac{f_j}{f_i} \in (f_i)$ and so $(f_i) = (f_1, \ldots, f_n)$.

($\Leftarrow$) Let $x, y \in R$. By assumption $(x, y) = (z)$ for some $z \in R$. Write $x = az$, $y = bz$ and $z = cx + dy$ with $a, b, c, d \in R$. Then $z = caz + dbz = (ca + db)z$ and so $ca + db = 1$ as R is a domain. If $a, b \in \mathfrak{m}$, then $1 \in \mathfrak{m}$, a contradiction. Thus either a or b is a unit and hence either $\frac{x}{y} = \frac{a}{b}$ or $\frac{y}{x} = \frac{b}{a}$ is in R. ■

4.3 Normal Domains and DVRs

Now we study what happens when we add the Noetherian condition into the mix.

Definition A Noetherian integrally closed domain is called a **normal domain**.

Example 4.37 *$k[X_1, \ldots, X_n]$ and $k[\![X_1, \ldots, X_n]\!]$ are normal domains.*

Definition Let $(R, \mathfrak{m})$ be a valuation ring with fraction field K and valuation $\nu : K^* \to \Gamma = K^*/R^*$. The ring R is called a **discrete valuation ring**, or **DVR** for short if $\Gamma \cong \mathbb{Z}$.

Example 4.38 *The rings $\mathbb{Z}_{(p)}$, $k[\![X]\!]$, and $k[X]_{(X)}$, where k is a field, are DVRs.*

There are many ways of characterizing DVRs. The first characterization is that, along with fields, they are the only Noetherian valuation rings.

Theorem 4.39 *A valuation ring R is Noetherian if and only if R is a DVR or a field. Moreover, every DVR is a local PID.*

Proof ($\Rightarrow$) Suppose $(R, \mathfrak{m})$ is a Noetherian valuation ring that is not a field. Then there exists $r \in R$ with $\nu(r) > 0$. By the Noetherian property, there exists $r_0 \in R$ such that if $r \in \mathfrak{m}$, then $\nu(r) \geq \nu(r_0) = g_0$. Let $g \in G_{\geq 0}$ and consider $g, g - g_0, g - 2g_0, \ldots$. Again by the Noetherian property these cannot all by > 0. So there is the greatest n such that $g - ng_0 \geq 0$. By minimality of g_0, $g - ng_0 = 0$ and so $g = ng_0$; that is, G is infinite, cyclic, and generated by g_0. ($\Leftarrow$) Let $(R, \mathfrak{m})$ be a DVR and suppose I is an ideal generated by $f_1, f_2, \ldots \in R$. Since the value group is $\mathbb{Z}$ we can choose f_i so that $\nu(f_i)$ is minimal. It follows easily that $I = (f_i)$ and in particular R is Noetherian and a PID.

■

Example 4.40 *To construct a non-Noetherian valuation ring, we must pick a field with a valuation to some nontrivial totally ordered abelian group besides $\mathbb{Z}$. Consider $\Gamma = \mathbb{Z} \times \mathbb{Z}$, ordered lexicographically. Let k be a field and set $K = k(x, y)$. Define $\nu : K^* \to \Gamma$ by setting $\nu(x^i y^j) = (i, j)$ for $i, j \in \mathbb{Z}$. Check that this uniquely defines a valuation ν on all of K^*. Then the valuation ring associated to ν is*

$$R = k\left[x, y, \frac{x}{y}, \frac{x}{y^2}, \frac{x}{y^3}, \ldots\right]_{\mathfrak{m}},$$

where $\mathfrak{m} = \left(x, y, \frac{x}{y}, \frac{x}{y^2}, \frac{x}{y^3}, \ldots\right)$. We leave it as an exercise to check that R is a non-Noetherian valuation ring but has Krull dimension 2.

Proposition 4.41 (Characterization of DVRs) *Let $(A, \mathfrak{m})$ be a local domain. Then the following are equivalent:*

(1) *A is a DVR.*

(2) *A is normal and $\dim(A) = 1$.*

(3) *A is normal and there exists $0 \neq x \in A$ such that $\mathfrak{m}$ is an essential prime of Ax. In other words, $\mathfrak{m} \in \mathrm{Ass}_A(A/Ax)$.*

(4) $\mathfrak{m} \neq 0$, *and* $\mathfrak{m}$ *is principal.*

Proof (1) $\Rightarrow$ (2) Suppose A is a DVR. Then by assumption A is a PID. Thus $\dim(A) = 1$. We also know that PID $\Rightarrow$ UFD $\Rightarrow$ integrally closed. Since A is a domain and integrally closed, it is thus normal.

(2) $\Rightarrow$ (3) Suppose A is normal and $\dim(A) = 1$. Take any $0 \neq x \in \mathfrak{m}$. Since $x \in \mathfrak{m}$, x is a system of parameters itself and so $\lambda(A/xA) < \infty$. It follows that $\mathrm{Ass}_A(A/xA) = \{\mathfrak{m}\}$.

(3) $\Rightarrow$ (4) Suppose A is normal and there exists $0 \neq x \in A$ with $\mathrm{Ass}_A(A/xA) = \{\mathfrak{m}\}$. Then $A/\mathfrak{m} \hookrightarrow A/xA$. Let $\overline{y} \in A/xA$ be the image of 1 under this map. Then $\mathfrak{m}y \subseteq xA$. Thus $\mathfrak{m}yx^{-1} \subseteq A$ and so $\mathfrak{m}yx^{-1}$ is an ideal of A.

Suppose $\mathfrak{m}yx^{-1} \subseteq \mathfrak{m}$. Since $y \notin xA$, $yx^{-1} \notin A$. Write $z = yx^{-1}$. The maximal ideal $\mathfrak{m}$ is finitely generated, so we can write $\mathfrak{m} = (x_1, \ldots, x_n)$. So we can write $zx_i = \sum a_{ij}x_j$ for each i. So

$$-a_{i1}x_1 - a_{i2}x_2 + \cdots + (z - a_{ii}x_i) + \cdots - a_{in}x_n = 0$$

for each $i = 1, \ldots, n$. Using the same determinant trick as in Proposition 4.1, we get that $\det(A)x_i = 0$ for all i, where A is the matrix

$$\begin{bmatrix} z - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & z - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & & \vdots \\ -a_{n1} & -a_{n2} & \cdots & z - a_{nn} \end{bmatrix}.$$

Thus $\det(A)\mathfrak{m} = 0$. So by Nakayama's Lemma, Corollary 0.29, $\det(A) = 0$. Thus z is integral over A. Since A is integrally closed, $z \in A$. This is a contradiction to $z \notin A$. So we must have that $\mathfrak{m}yx^{-1} = A$. But now $\mathfrak{m} = xy^{-1}A$. Thus $\mathfrak{m}$ is principal.

(4) $\Rightarrow$ (1) Set $\mathfrak{m} = xA$. Since x is a domain, x is a nonzerodivisor. So $x^n \neq 0$ for all $n \geq 0$. By Krull's Intersection Theorem **??**, $\bigcap_{n \geq 0} x^n A = (0)$. So for any $y \in A$, there is a greatest integer m such that $y \in x^m A \smallsetminus x^{m+1}A$. Writing $y = ux^m$, then $u \notin \mathfrak{m}$ and so u is a unit. Thus if $z \in \mathrm{Frac}(A)$, then $z = vx^\nu$ for some unit v and some integer ν. It is easy to check that setting $\nu(z) = \nu$ defines a valuation with valuation group $\mathbb{Z}$ and with valuation ring A. Therefore A is a DVR. ■

Theorem 4.42 (Serre) *Let A be Noetherian, then A is normal if and only if both of the following hold:*

(1) $A_\mathfrak{p}$ *is a DVR for all primes* $\mathfrak{p}$ *of height* 1.

(2) *For all* $0 \neq x \in A$, *if* $\mathfrak{p} \in \mathrm{Ass}(A/Ax)$ *then* $\mathrm{ht}(\mathfrak{p}) = 1$.

Proof ($\Rightarrow$) Suppose A is normal. Pick a prime P with $\mathrm{ht}(P) = 1$. Then $\dim(A_P) = 1$ and A_P is integrally closed. So A_P is a DVR. Now take $Q \in \mathrm{Ass}_A(A/xA)$ for some $0 \neq x \in A$. Then $QA_Q \in \mathrm{Ass}_{A_Q}(A_Q/xA_Q)$. Since A_Q is

normal and since QA_Q is an essential prime of xA_Q, we have by the previous proposition that A_Q is a DVR. Thus $\dim(A_Q) = \mathrm{ht}(Q) = 1$.

($\Leftarrow$) Since A is a domain, for every ideal P of A with $\mathrm{ht}(P) = 1$ we have $A_{\mathfrak{m}} \subseteq A_P \subseteq \mathrm{Frac}(A)$ for some maximal ideal $\mathfrak{m}$. Thus

$$A \subseteq \bigcap_{\mathfrak{m} \in \mathrm{MaxSpec}(A)} A_{\mathfrak{m}} \subseteq \bigcap_{\substack{P \in \mathrm{Spec}(A) \\ \mathrm{ht}(P)=1}} A_P.$$

Thus to show A is normal it is enough to show that $A = \bigcap_{P\,:\,\mathrm{ht}(P)=1} A_P$.

Take $z \in \bigcap_{P\,:\,\mathrm{ht}(P)=1} A_P$. We can write $z = x/y$ where $x, y \in A$ and $y \neq 0$. Thus $x \in yA_P$ for all P with $\mathrm{ht}(P) = 1$. Let

$$yA = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$$

be a primary decomposition of yA, where $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary. Then for each i, $\mathfrak{p}_i \in \mathrm{Ass}_A(A/yA)$ and so $\mathrm{ht}(p_i) = 1$. Thus $yA_{\mathfrak{p}_i} = \mathfrak{q}_i A_{\mathfrak{p}_i}$ for each i. So $x \in \mathfrak{q}_i A_{\mathfrak{p}_i} \cap A = \mathfrak{q}_i$ for all i. Thus $x \in yA$. So $z = \frac{x}{y} \in A$. Hence A is normal. ■

Example 4.43 *Consider $f(x, y) = y^2 - x^2(1+x) \in k[x, y]$, which is irreducible by Eisenstein's Criterion. To see this, note $x + 1$ is prime in $k[x]$ and divides all coefficients of y^i but the leading term y^2 and $(x + 1)^2$ does not divide the coefficient of y^0.*

Therefore, $A = k[x, y]/(f(x))$ is a domain. Is A normal? No, since $\frac{y}{x}$ is integral over A but is not in A. To see this, note $\frac{y}{x} = (1 + x)^{\frac{1}{2}}$ is an infinite series. It follows then that A is not normal.

Example 4.44 *Consider $A = k[x, y, z]/(xz - y^2, x^3 - yz, x^2y - z^2)$. Note $A \cong k[t^3, t^4, t^5]$, and we have the integral extension*

$$k[t^3, t^4, t^5] \hookrightarrow k[t].$$

Since $k[t]$ is the integral closure of $k[t^3, t^4, t^5]$, we see that A is not normal.

Example 4.45 *$k[x_1, x_2, \ldots, x_n]$ is a UFD, and so it is normal.*

4.4 Dedekind Domains

Definition An integral domain A is called a **Dedekind domain** if A is normal and $\dim(A) = 1$.

Note then that a DVR is just a local Dedekind domain. Some authors modify the definition to $\dim(A) \leq 1$ to allow fields to be Dedekind domains. We do not take that point of view.

Throughout this section A will be an integral domain and $K = \mathrm{Frac}(A)$ will denote the field of fractions.

Definition Let A be an integral domain and $K = \mathrm{Frac}(A)$. A nonzero A-submodule M of K is called a **fractional ideal** of A if all elements of M have a common denominator; that is,

$$M \subseteq A \cdot \frac{1}{d} \qquad \text{for some } 0 \neq d \in A.$$

A fractional ideal M of A is called **invertible** if there is a fractional ideal M^{-1} such that $MM^{-1} = A$. The set of fractional ideals of A is denoted $D(A)$.

For any fractional ideal $M \subseteq A \cdot \frac{1}{d}$, $dM \subseteq A$ and so, as an A-module, M is isomorphic to an ideal I of A. So if A is Noetherian, all fractional ideals of A are finitely generated.

Remark If M_1 and M_2 are fractional ideals of A and $K = \mathrm{Frac}(A)$, then the following are again fractional ideals of A:

(1) $M_1 + M_2$

(2) $M_1 \cap M_2$

(3) $M_1 M_2$

(4) $(M_1 :_K M_2) = \{x \in K : xM_2 \subseteq M_1\}$

Proposition 4.46 *Suppose M is an invertible fractional ideal. Then $M^{-1} = (A :_K M)$.*

Proof We have that $MM^{-1} = A$. Thus $M^{-1} \subseteq (A :_K M)$.

We also have

$$\begin{aligned}(A :_K M) &= (A :_K M)A \\ &= (A :_K M)MM^{-1} \\ &\subseteq AM^{-1} \\ &= M^{-1}.\end{aligned}$$

Thus $M^{-1} = (A :_K M)$. ■

Proposition 4.47 *Suppose M is an invertible fractional ideal. Then M is finitely generated over A.*

Proof Since $MM^{-1} = A$ we can write $1 = \sum_i m_i n_i$ where $m_i \in M$ and $n_i \in M^{-1}$ for each i. Now take $x \in M$. Then

$$\begin{aligned}x &= \sum_i m_i n_i x \\ &= \sum_i a_i m_i,\end{aligned}$$

where $a_i = n_i x \in M^{-1}M = A$. Thus M is finitely generated over A. ■

Proposition 4.48 *If a finite product of fractional ideals is invertible if and only if each fractional ideal in the product is invertible.*

Proof Exercise. ■

Proposition 4.49 *Let I be an ideal of A. Suppose I can be factored into a product of invertible prime ideals. Then any other factorization of I into a product of prime ideals is identical.*

Proof Suppose $I = P_1 \cdots P_n$ where each P_i is an invertible prime ideal and also $I = Q_1 \cdots Q_m$ where each Q_i is a prime ideal. Pick a minimal prime P_i in $\{P_1, \ldots, P_n\}$. Then $I \subseteq P_i$. Since P_i is prime we must have $Q_j \subseteq P_i$ for some j. Similarly we must have $P_k \subseteq Q_j$ for some k. Since P_i was minimal, $i = k$. Therefore $P_i = Q_j$. Now consider $IP_i^{-1} = P_1 \cdots \widehat{P_i} \cdots P_n$ and use induction on the number of factors. ■

Proposition 4.50 *Let A be an integral domain. Suppose every ideal can be expressed as a product of prime ideals. Then every nonzero prime ideal is invertible and maximal, in particular A is Noetherian.*

Proof First we show that every invertible prime ideal of A is maximal. Let P be an invertible prime ideal. Choose $a \notin P$. By assumption we can write

$$\begin{aligned}(P + aA)^2 &= P_1 \cdots P_n, \\ P + a^2A &= Q_1 \cdots Q_m.\end{aligned}$$

Let $\overline{(-)}$ denote the image in A/P. Since $\overline{(P + aA)^2} = \overline{P + a^2A}$, we have that

$$\overline{(a^2)} = \overline{P}_1 \cdots \overline{P}_n = \overline{Q}_1 \cdots \overline{Q}_m.$$

Since the principal ideal $\overline{(a^2)}$ is invertible, so are $\overline{P}_i$ and $\overline{Q}_j$ for each i, j by Proposition 4.48. By Proposition 4.49 we must have that $n = m$ and for each i there exists j with $\overline{P}_i = \overline{Q}_j$. Therefore by the Correspondence Theorem, $P_i = Q_j$ in A. Hence $P + a^2A = (P + aA)^2$. We now have

$$P \subseteq P + a^2A = (P + aA)^2 \subseteq P^2 + aA,$$

so for any $y \in P$ we may write $y = z + ax$, where $z \in P^2$ and $x \in A$. Since $ax = y - z \in P$ and since $a \notin P$ we have that $x \in P$. Hence

$$P \subseteq P^2 + Pa \subseteq P.$$

Thus

$$\begin{aligned}P &= P^2 + Pa \\ &= P(P + Aa).\end{aligned}$$

Since P is invertible there is a fractional ideal P^{-1} with $PP^{-1} = A$. Hence

$$\begin{aligned} A &= P^{-1}P \\ &= P^{-1}P(P + (a)) \\ &= P + (a). \end{aligned}$$

Therefore $P + (a) = A$ and so P is maximal.

Now take any prime ideal P and pick some nonzero $a \in P$. Write $Aa = P_1 \cdots P_n$, a product of invertible prime ideals. Since the principal ideal aA is invertible, so are $P_1, \ldots, P_n$ by Proposition 4.48. It is easy to see that P must contain one of the P_i, otherwise, consider a product of elements x_i where $x_i \in P_i - P$ and note that $x_1 \ldots x_n \in P_1 \ldots P_n - P$, a contradiction. By our work above each P_i is maximal since they are each invertible. Therefore P is itself maximal. Again by Proposition 4.48, P is invertible since the P_i's are invertible.

Finally note that since any nonzero ideal I is invertible, we have $II^{-1} = A$. Thus we can write $\sum_{i=1}^{n} a_i b_i$ where $a_i \in I$ and $b_i \in I^{-1}$ for each i. Thus for any $x \in I$, $x = \sum_{i=1}^{n} (xb_i)a_i$. So $a_1, \ldots, a_n$ generate I. Therefore every nonzero ideal is finitely generated and A is Noetherian. ■

Theorem 4.51 *Let A be a Dedekind domain. Then any fractional ideal M can be written uniquely as $M = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$, where $\mathfrak{p}_i$ is a prime ideal and $n_i \in \mathbb{Z}$ for $i = 1, \ldots, r$.*

Proof First we show that every ideal can be written as a product of prime ideals. Let $\mathfrak{a}$ be an ideal. We may assume since (0) is prime that $(0) \neq \mathfrak{a}$. Let $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ be a primary decomposition with $\mathfrak{q}_i$ being $\mathfrak{p}_i$-primary. Since $\dim(A) = 1$, each $\mathfrak{p}_i$ is maximal. Thus $A_{\mathfrak{p}_i}$ is a DVR and so $\mathfrak{q}_i A_{\mathfrak{p}_i} = \mathfrak{p}_i^{n_i} A_{\mathfrak{p}_i}$. Since $\mathfrak{p}_i$ is maximal, $\mathfrak{p}_i^{n_i}$ is $\mathfrak{p}_i$-primary. So $\mathfrak{p}_i^{n_i} A_{\mathfrak{p}_i} \cap A = \mathfrak{p}^{n_i} = \mathfrak{q}_i$. Therefore

$$\mathfrak{a} = \mathfrak{p}_i^{n_i} \cap \cdots \cap \mathfrak{p}_r^{n_r} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}.$$

Since any fractional ideal M is contained in $\frac{1}{d}A$ for some $d \in A$, by writing dM and dA as products of primes we can write M is a product of primes with possibly negative exponents. ■

Definition Let A be a Dedekind domain. Given a prime $\mathfrak{p}$, we define for a fractional ideal M, $v_{\mathfrak{p}}(M) = n$ if $M = \mathfrak{p}^n \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$ is the factorization of M. The function v_p is called a **discrete valuation**.

Proposition 4.52 *Let $v_{\mathfrak{p}}$ be a discrete valuation for the Dedekind domain A, with $K = \mathrm{Frac}(A)$. Then for fractional ideals M_1, M_2 :*

(1) $v_{\mathfrak{p}}(M_1 + M_2) = \min\{v_{\mathfrak{p}}(M_1), v_{\mathfrak{p}}(M_2)\}$

(2) $v_{\mathfrak{p}}(M_1 \cdot M_2) = v_{\mathfrak{p}}(M_1) + v_p(M_2)$

(3) $v_{\mathfrak{p}}(M_1 \cap M_2) = \max\{v_{\mathfrak{p}}(M_1), v_{\mathfrak{p}}(M_2)\}$

(4) $v_{\mathfrak{p}}((M_1 :_K M_2)) = v_{\mathfrak{p}}(M_1 M_2^{-1}) = v_{\mathfrak{p}}(M_1) - v_p(M_2)$

(5) *$M_1 \subseteq M_2$ if and only if $v_{\mathfrak{p}}(M_1) \leq v_{\mathfrak{p}}(M_2)$ for all primes $\mathfrak{p}$.*

Proof Exercise. ■

Corollary 4.53 *Let M_1 be a fractional ideal in a Dedekind domain A. Then M_1 is an integral ideal, $M_1 \subseteq A$, if and only if $v_{\mathfrak{p}}(M_1) \geq 0$ for all primes $\mathfrak{p}$.*

Theorem 4.54 *Let A be an integral domain. Then every ideal in A is a product of prime ideals if and only if the fractional ideals of A form a group under multiplication.*

Proof ($\Rightarrow$) This is clear from the above.
($\Leftarrow$) So assume the fractional ideals of A form a multiplicative group. Since every ideal of A is invertible, it is finitely generated by Proposition 4.47. So A is Noetherian. Consider the family

$$\mathcal{F} = \{\text{ideals } \mathfrak{a} \subsetneq A : \mathfrak{a} \text{ is not a product of primes.}\}.$$

Suppose $\mathcal{F} \neq \varnothing$. Then $\mathcal{F}$ has a maximal element, say $\mathfrak{a}$. Clearly $\mathfrak{a}$ cannot be a maximal ideal so there exists a maximal ideal $\mathfrak{m}$ with $\mathfrak{a} \subsetneq \mathfrak{m}$. So $\mathfrak{a}\mathfrak{m}^{-1} \subsetneq A$.

We clearly have $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{m}^{-1}$. If $\mathfrak{a} = \mathfrak{a}\mathfrak{m}^{-1}$ then also $\mathfrak{a} = \mathfrak{a}\mathfrak{m}$. But $\mathfrak{a}$ is finitely generated so by Krull's Intersection Theorem 0.28, there is $m \in \mathfrak{m}$ such that $(1-m)\mathfrak{a} = (0)$. This is a contradiction as A is a domain. Therefore $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{m}^{-1} \subsetneq A$. Therefore, since $\mathfrak{a}$ was maximal in $\mathcal{F}$, $\mathfrak{a}\mathfrak{m}^{-1} \notin \mathcal{F}$. So we can write $\mathfrak{a}\mathfrak{m}^{-1} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$. So $\mathfrak{a} = \mathfrak{m}\mathfrak{p}_1^{n-1} \cdots \mathfrak{p}_r^{n_r}$, contradicting $\mathfrak{a} \in \mathcal{F}$. Therefore $\mathcal{F} = \varnothing$. ■

Theorem 4.55 *Suppose A is an integral domain. Then A is a Dedekind domain if and only if every ideal can be expressed as a product of prime ideals.*

Proof ($\Rightarrow$) This follows from Theorem 4.51.

($\Leftarrow$) By the previous theorem every nonzero ideal is invertible. By Proposition 4.50 we have that every nonzero prime ideal is maximal. Therefore A is Noetherian and $\dim(A) = 1$. We must show that A is integrally closed. Set $K = \text{Frac}(A)$. Take $x \in K - A$. Suppose x is integral over A. Then

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

for some $a_i \in A$. Since $x \in K$ we can write $x = \frac{\lambda}{\mu}$, where $\lambda, \mu \in A$. Since we can write

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

and since the right hand side contains denominators μ_i for i at most $n-1$, we have that $\mu^{n-1}x^n \in A$. Setting $d = \mu^{n-1}$ we have that $dx^t \in A$ for all $t > 0$. Let P be any nonzero prime ideal. Then $v_P(dx^t) \geq 0$ for all $t > 0$. By Proposition 4.52, $v_P((d)) + tv_P((x)) \geq 0$ for all $t > 0$. Thus $v_P((x)) \geq 0$ for all $P \in \text{Spec}(A) - \{(0)\}$. Therefore $x \in A$. So A is integrally closed. ■

Corollary 4.56 *If A is a Dedekind domain, then its group of fractional ideals $D(A)$ is isomorphic to the free abelian group on the nonzero prime ideals of A.*

4.5 The Krull-Akizuki Theorem

Definition Given a domain A and an A-module M we define the **rank** of M, denote $\text{rank}_A(M)$, to be the following vector space rank

$$\text{rank}_A(M) := \{\text{rank}_K(K \otimes_A M)\},$$

where $K = \text{Frac}(A)$. If A is not a domain we define the rank of M to be

$$\text{rank}_A(M) := \max\{\text{rank}_{A/\mathfrak{p}}(M/\mathfrak{p}M) : \mathfrak{p} \text{ is a minimal prime of } A\}$$

Lemma 4.57 *Let A be a Noetherian domain with $\dim(A) \leq 1$ and M a torsion free module over A of rank $r < \infty$. Then for any nonzero $a \in A$,*

$$\lambda(M/aM) \leq r \cdot \lambda(A/aA).$$

Proof We first prove the finitely generated case.

Case 1 Assume M is finitely generated over A.
Since M is torsion free over A, the localization map $M \hookrightarrow U^{-1}M$ is injective, where $U = A - \{0\}$. Let $\alpha_1, \ldots, \alpha_n$ be a set of generators for M. Then $\frac{\alpha_1}{1}, \ldots, \frac{\alpha_n}{1}$ is a set of generators for $U^{-1}M$. By assumption $U^{-1}M$ is an r dimensional vector space over $K = \text{Frac}(A)$. In particular we may suppose that $\frac{\alpha_1}{1}, \ldots, \frac{\alpha_r}{1}$ form a K-basis for $U^{-1}M$ by throwing away linearly dependent elements. Thus for $i > r$ we have

$$\frac{\alpha_i}{1} = \sum_{j=1}^{r} \lambda_{ij} \frac{\alpha_j}{1} \quad \text{where} \quad \lambda_j \in K.$$

Finding a common denominator we may write

$$\lambda_{ij} = \frac{\mu_{ij}}{s} \quad \text{where} \quad \mu_{ij}, s \in A$$

for all i, j. So by clearing denominators we get that

$$s\alpha_i = \sum_{i=1}^{r} \mu_{ij}\alpha_j \quad \text{for} \quad r < i \leq n.$$

Let F be the free A-module generated by $\alpha_1, \ldots, \alpha_r$. Then we have the exact sequence

$$0 \to F \to M \to Q \to 0$$

where Q is generated by the images of $\alpha_{r+1}, \ldots, \alpha_n$. Since $s\alpha_j \in F$ for $i > r$ and since $Q \cong M/F$, we have $sQ = 0$. Thus Q is a finitely generated module over A/sA. Since $\dim(A/sA) = 0$, $\lambda(Q) < \infty$. Tensoring the above exact sequence with A/a^nA we get the exact sequence

$$F/a^nF \to M/a^nA \to Q/a^nQ \to 0.$$

Therefore

$$\lambda(M/a^nM) \leq \lambda(F/a^nF) + \lambda(Q/a^nQ).$$

Since $M/aM \cong a^{n-1}M/a^nM$ and since M is torsion free, we have that $\lambda(M/a^nM) = n\lambda(M/aM)$. Similarly $\lambda(F/a^nF) = n \cdot \lambda(F/aF) = nr \cdot \lambda(A/aA)$. Since $\lambda(Q) < \infty$, we must have $\lambda(Q/a^nQ) \leq \lambda(Q)$. Thus for all n,

$$\begin{aligned}\lambda(M/aM) &= \frac{1}{n}\lambda(M/a^nM) \\ &\leq \frac{1}{n}\lambda(F/a^nF) + \frac{1}{n}\lambda(Q/a^nQ) \\ &= r \cdot \lambda(A/aA) + \frac{1}{n}\lambda(Q).\end{aligned}$$

Therefore

$$\lambda(M/aM) \leq r \cdot \lambda(A/aA).$$

Case 2 We now prove the general case. Suppose that the assertion is not true for the module M, in other words there exists $a \in A$ such that $\lambda(M/aM) > r \cdot \lambda(A/aA)$. Then we may choose a finitely generated submodule $M' \subseteq M$ such that $\lambda(M'/aM') > r\lambda(A/aA)$. But then

$$\begin{aligned}\lambda(M'/aM') &> r \cdot \lambda(A/aA) \\ &\geq \operatorname{rank}_A(M') \cdot \lambda(A/aA),\end{aligned}$$

a contradiction of the finitely generated case. ■

Theorem 4.58 (Krull-Akizuki) *Let A be a Noetherian domain, $\dim(A) \leq 1$, $K = \operatorname{Frac}(A)$, L/K a finite field extension, $A \subseteq B \subseteq L$, and B a subring of L. Then B is Noetherian and $\dim(B) \leq 1$.*

Proof We prove this theorem in two steps:

Step 1 We first reduce to the case that $\operatorname{Frac}(A) = K = L$.
WLOG we can assume that $L = \operatorname{Frac}(B)$. Since $[L : K] < \infty$, we can find $b_1, \ldots, b_n \in B$ such that $L = K(b_1, \ldots, b_n)$. Set $x = b_i$. Since each b_i are algebraic over K they satisfy relations of the form

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

where $a_0, \ldots, a_{n-1}, c \in A$. Therefore

$$(cx)^n + a_{n-1}(cx)^{n-1} + \cdots + c^{n-1}a_0 = 0.$$

So cx is integral over A. So replacing each b_i by an A-multiple which is integral over A we can assume that $b_1, \ldots, b_n$ are all integral over A. Set $D = A[b_1, \ldots, b_n]$. Thus $\dim(D) = \dim(A)$, $\operatorname{Frac}(D) = \operatorname{Frac}(B) = L$ and

$$D \subseteq B \subseteq L.$$

Since D is finitely generated over A, it is Noetherian. Thus we are reduced to the case where $L = K$.

Step 2 We now prove the theorem assuming $L = K$.
In our situation we have $A \subseteq B \subseteq K = \mathrm{Frac}(A)$. Thus $\mathrm{rank}_A(B) = 1$. So we may apply Lemma 4.57 to get that $\lambda(B/aB) \leq \lambda(A/aA) < \infty$ for any $0 \neq a \in A$. Let $\mathfrak{b} \neq 0$ be an ideal in B. Pick $0 \neq b \in \mathfrak{b}$. Since b is algebraic over A it satisfies a relation of the form

$$a_m b^m + a_{m-1} b^{m-1} + \cdots + a_0 = 0 \quad \text{with} \quad a_i \in A.$$

Since B is a domain we can assume $a_0 \neq 0$. Thus $0 \neq a_0 \in \mathfrak{b} \cap A$. So $\lambda_B(\mathfrak{b}/a_0 B) \leq \lambda_A(\mathfrak{b}/a_0 B) \leq \lambda_A(B/a_0 B) < \infty$. Thus $\mathfrak{b}/a_0 B$ is a finitely generated B-module; hence $\mathfrak{b}$ is finitely generated. Thus B is Noetherian. Further, if $\mathfrak{p}$ is any nonzero prime ideal of B, then $B/\mathfrak{p}B$ is Artinian and a domain, hence a field. So $\mathfrak{p}$ is maximal. Therefore $\dim(B) = 1$. ■

Corollary 4.59 *Let A be a Noetherian domain with $\dim(A) \leq 1$. Then the integral closure of A is Noetherian.*

Remark Many extensions of the above theorem that one might want are actually false. For the following A is a Noetherian domain, $K = \mathrm{Frac}(A)$, $[L : K] < \infty$ and B is the integral closure of A in L.

(1) If A is as above even if $\dim(A) \leq 1$, then B is not necessarily a finitely generated A-module.

(2) If $\dim(A) \geq 2$ and C is a ring such that $A \subseteq C \subseteq L$ then C is not necessarily Noetherian.

(3) If $\dim(A) \geq 3$ then B is not necessarily Noetherian.

See [14] for examples of these.

We include a couple of similar results:

Theorem 4.60 *Let A be a Noetherian domain with $\dim(A) \leq 2$. Then the integral closure of A is Noetherian.*

Proof See [14], Theorem 33.12. ■

Theorem 4.61 *Let A be a finitely generated k-algebra, $K = \mathrm{Frac}(A)$, $[L : K] < \infty$ and let B be the integral closure of A in L. Then B is a finitely generated A-module and is Noetherian.*

Proof See [6], Chapter 13. ■

Definition Given field L which is a finite extension of another field K, the **trace** of an element $\alpha \in L$ is defined as

$$\mathrm{tr}_{L/K}(\alpha) := \sum_{\sigma \in \mathrm{Gal}_K(L)} \sigma(\alpha).$$

Theorem 4.62 *Let L/K be a finite field extension. Then L/K is separable if and only if there exists $0 \neq x \in L$ such that $\mathrm{tr}_{L/K}(x) \neq 0$.*

Proof See [16]. ■

Theorem 4.63 *Let A be a normal domain, $K = \mathrm{Frac}(A)$, L/K a finite, separable field extension, and let B be the integral closure of A in L. Then B is a finitely generated A-module*

Proof Let $e_1, \ldots, e_n$ be a basis of L over K such that $e_1, \ldots, e_n \in B$. Let $\widetilde{e}_1, \ldots, \widetilde{e}_n$ be the corresponding dual basis of L, that is $\mathrm{tr}_{L/K}(\widetilde{e}_i e_j) = \delta_{ij}$. Fix $b \in B$. Then thinking of B as a submodule of $L^* = \mathrm{Hom}_K(L, K)$, we can write $b = \lambda_1 \widetilde{e}_1 + \cdots + \lambda_n \widetilde{e}_n$ where $\lambda_1, \ldots, \lambda_n \in K$. Then $\lambda_i = \mathrm{tr}_{L/K}(be_i) \in K$. But the trace of an element is the sum of its conjugates, each of which are integral over A. Thus λ_i is integral over A for each i. So $\lambda_i \in A$ for each i. Therefore $B \subseteq A\widetilde{e}_1 + \cdots + A\widetilde{e}_n \subseteq L^*$ and so B is finitely generated over A. ■

4.6 Unique Factorization and Class Groups

First we consider the case of Dedekind domains followed by a generalization to all domains.

Definition Let A be a domain and let $C(A)$ denote the set of invertible fractional ideals of A. Let $P(A)$ denote the subgroup of principal ideals and let $\mathrm{Pic}(A) = C(A)/P(A)$ denote the quotient group called the **Picard group** of A.

In the case when A is a Dedekind domain, every fractional ideal is invertible and the Picard group is sometimes called the **ideal class group** of A.

The following result shows that the size of the class group of a Dedekind domain A is a measure of the failure of A to be a UFD.

Theorem 4.64 *Let A be a Noetherian domain. Then A is a UFD if and only if every height one prime ideal is principal.*

Proof ($\Rightarrow$) Suppose A is a UFD and let $\mathfrak{p}$ be a height one prime of A. Let $x \in \mathfrak{p}$. Write $x = a_1 a_2 \cdots a_n$ as a product of irreducible elements. Since $\mathfrak{p}$ is prime, $a_i \in \mathfrak{p}$ for some i. Since a_i is irreducible, (a_i) is a prime ideal contained in $\mathfrak{p}$. Since $\mathfrak{p}$ has height one, $(a_i) = \mathfrak{p}$.
($\Leftarrow$) Now suppose that every height one prime is principal. Since A is Noetherian, every nonzero nonunit element can be written as a finite product of irreducible elements so it suffices to show that every irreducible element is prime. Let $x \in A$ be irreducible element and let $\mathfrak{p}$ be a minimal, hence height one, prime containing x. By assumption $\mathfrak{p} = (y)$ for some $y \in R$. So $x = yz$ for some $z \in A$. Since x is irreducible, z is a unit. So $(x) = (y) = \mathfrak{p}$ is a prime ideal and x is a prime element. ■

Corollary 4.65 *Let A be a Dedekind domain. Then the following are equivalent:*

(1) $\mathrm{Pic}(A)$ *is trivial.*

(2) *A is a UFD.*

(3) *A is a PID.*

The first instance class groups were investigated was the case of the rings of integers $\mathcal{O}_K$ in a number field K, that is, the integral closure of $\mathbb{Z}$ inside some algebraic field extension of the rationals $\mathbb{Q}$. By the Krull-Akizuki Theorem 4.58, $\mathcal{O}_K$ is an integrally closed, Noetherian domain of dimension one, hence a Dedekind domain. Not all rings of integers are UFDs though as the following example shows:

Example 4.66 *Let $K = \mathbb{Q}(\sqrt{-5})$. Then the ring of integers is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. One checks that $\mathrm{Pic}(A) \cong \mathbb{Z}/2\mathbb{Z}$ and the ideal $\mathfrak{p} = (2, 1+\sqrt{-5})$ is a representative of the non-identity class in $\mathrm{Pic}(A)$. (It is not hard to check that $\mathfrak{p}^2 = (2)$ is principal.) It follows that A is not a UFD.*

A result of Minkowski shows that the class group of the ring of integers of any number field is a finite group, yet there are Dedekind domains with infinite class groups. Moreover, it is known that *every* abelian group can be realized as the class group of some Dedekind domain.

One can also show that, when A is a Dedekind domain, the fractional ideals are precisely projective (i.e. locally free) rank one modules of A.

Exercise 4.67 *Let $(A, \mathfrak{m})$ be a local ring. Every projective A-module is free.*

Exercise 4.68 *Let A be a ring and M a finitely presented A-module. (i.e. $M \cong \mathrm{Coker}(\phi : A^n \to A^m)$ with $m, n \in \mathbb{N}$.) Then M is a projective A-module if and only if $M_\mathfrak{m}$ is a free $A_\mathfrak{m}$-module for every maximal ideal $\mathfrak{m}$ of A.*

Exercise 4.69 *Let A be a ring and M a finitely presented A-module. Then M is flat if and only if it is projective.*

Exercise 4.70 *Let $(A, \mathfrak{m})$ be a local ring. Then all finitely presented (and hence all finitely generated) flat modules are free.*

Exercise 4.71 *Let A be a domain and let M be a fractional ideal of A. Then the following are equivalent:*

(1) *M is invertible.*

(2) *M is a projective A-module.*

(3) *M is finitely generated and for every maximal ideal $\mathfrak{m}$ of A, $M_\mathfrak{m}$ is a free $A_\mathfrak{m}$-module of rank one.*

For an arbitrary ring, one defines the Picard group as the group of isomorphism classes of rank one projective modules; tensor product is the group operation and $P^{-1} = \mathrm{Hom}_R(P, R)$ is the inverse operation. Over a Dedekind domain, this is the same thing as the ideal class group. In geometric situations, this provides information about line bundles on a variety. See [6] for more details.

If A is a domain that is not a Dedekind domain, then the set $D(A)$ of fractional ideals does not form a group. But in the case of a Dedekind domain, $D(A)$ was just the free abelian group on the height one prime ideals of A. This provides an obvious way to generalize class groups to non-Dedekind domains.

Definition Let A be a domain. Let $\mathrm{Div}(A)$ denote the free abelian group on height one prime ideals of A.

4.7 Noether's Normalization Lemma

The following strengthened version of Noether's 1926 result (without the chain of ideals) is due to Nagata 1996. Geometrically, it says that for each d-dimensional variety $X \subseteq \mathbb{A}^n$ and a chain of subvarieties $X_1 \subseteq \cdots \subseteq X_r \subseteq X$, there is a finite map $X \to \mathbb{A}^d$ such that the image of each X_i is a coordinate plane.

Theorem 4.72 (Noether's Normalization Lemma) *Let k be a field, A a finitely generated k-algebra. Let*

$$\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \cdots \subsetneq \mathfrak{a}_r \subsetneq A$$

be an increasing sequence of ideals in A. Then there exist $x_1, \ldots, x_d \in A$ that are algebraically independent over k such that:

(1) *A is integral over $C = k[x_1, \ldots, x_d]$.*

(2) *For all $i = 1, \ldots, r$, we have integers $h(i) \in [0, d]$ such that*

$$\mathfrak{a}_i \cap C = (x_1, \ldots, x_{h(i)}).$$

Proof We prove this theorem in four steps:

Step 1 Reduce to the case where A is a polynomial ring. Since A is a finitely generated k-algebra, we may write $A = k[y_1, \ldots, y_n]$. Set $B = k[Y_1, \ldots, Y_n]$, a polynomial ring in n variables. Then we have the surjection

$$\begin{aligned} \eta : B &\to A, \\ Y_i &\mapsto y_i. \end{aligned}$$

Hence we obtain an increasing sequence of ideals in B:

$$\eta^{-1}(0) \subseteq \eta^{-1}(\mathfrak{a}_1) \subseteq \eta^{-1}(\mathfrak{a}_2) \subseteq \cdots \subseteq \eta^{-1}(\mathfrak{a}_r)$$

Assuming the theorem is true for the polynomial ring B, we have algebraically independent elements $x_1, \ldots, x_n \in B$ such that B is integral over $D = k[x_1, \ldots, x_n]$ and such that

$$\mathrm{Ker}(\eta) \cap B = (x_1, \ldots, x_{h(0)})$$

and

$$\eta^{-1}(\mathfrak{a}_i) \cap B = (x_1, \ldots, x_{h(i)}) \qquad \text{for } i < j \text{ and} \qquad h(0) \leq h(i) \leq h(j).$$

Setting $C = \eta(D)$ we see that $C = k[z_{h(0)+1}, \ldots, z_n]$, where $z_i = \eta(x_i)$. Since B is integral over D, A is integral over C and

$$\mathfrak{a}_i \cap C = (z_{h(0)+1}, \ldots, z_{h(i)}).$$

It is also clear that the elements $z_{h(0)+1}, \ldots, z_n$ remain algebraically independent over k. Thus we have proved the theorem for A.

Step 2 Assuming A is a polynomial ring we prove the theorem for $r = 1$ and $\mathfrak{a}_1 = (x_1)$ principal with $x_1 \notin k$. (Note that the case where $x_1 \in k$ is obvious.) By assumption we can write $A = k[Y_1, \ldots, Y_n]$. Set

$$x_i = Y_i - Y_1^{\alpha_i} \qquad \text{for } i = 2, \ldots, n,$$

where the α_i are yet-to-be-determined constants. Then we have the inclusion $C = k[x_1, \ldots, x_n] \hookrightarrow A$. If Y_1 is integral over C then A would be integral over C and we would be done. So we proceed to show that for some choice of the α_i, Y_1 is integral over C.

Since $x_1 \in A$ we may write

$$x_1 = f(Y_1, \ldots, Y_n) = \sum a_{i_1 \ldots i_n} Y_1^{i_1} Y_2^{i_2} \cdots Y_n^{i_n}.$$

We then have that

$$f(Y_1, x_2 + Y_1^{\alpha_2}, x_3 + Y_1^{\alpha_3}, \ldots, x_n + Y_1^{\alpha_n}) = x_1.$$

We want to choose the α_i so that they the highest degree term in $f(Y_1, x_2 + Y_1^{\alpha_2}, \ldots, x_n + Y_1^{\alpha_n})$ is of the form $a_{i_1 \ldots i_n} Y_1^{i_1 + \alpha_2 i_2 + \cdots + \alpha_n i_n}$. Pick s larger than all exponents i_k appearing in the expansion of f. We leave it to the reader to check that setting $\alpha_2 = s$, $\alpha_3 = s^2$,...,$\alpha_n = s^{n-1}$ satisfies the above criterion. With this choice of α_i we have that A is integral over C. Thus we have $\dim(C) = \dim(A) = n$.

We must also show that these elements $x_1, \ldots, x_n$ are algebraically independent; in other words, we must show that $C = k[x_1, \ldots, x_n]$ is isomorphic to a polynomial ring. So take an onto map

$$k[X_1, \ldots, X_n] \xrightarrow{\eta} k[x_1, \ldots, x_n].$$

Since $\dim(k[X_1, \ldots, X_n]) = \dim(C) = n$, $\mathrm{Ker}(\eta) = 0$, for otherwise $\dim(C) = \dim(k[X_1, \ldots, X_n]/\mathrm{Ker}(\eta)) < n$.

Last, we must verify that $\mathfrak{a}_1 \cap C = (x_1)$. Clearly $\mathfrak{a}_1 \cap C \supseteq (x_1)$. But by the Going-Down Theorem, $\mathrm{ht}(\mathfrak{a}_1 \cap C) = \mathrm{ht}(\mathfrak{a}_1) = 1$. Since (x_1) is a prime ideal of height 1 inside $\mathfrak{a}_1 \cap C$, we must have $\mathfrak{a}_1 \cap C = (x_1)$.

Step 3 We now prove the theorem for $r = 1$ and $\mathfrak{a}$ any ideal of the polynomial ring $A = k[Y_1, \ldots, Y_n]$.

Pick nonzero $x_1 \in \mathfrak{a}$ and consider the ideal $x_1 A$. Then by Step 2 there are $x_2, \ldots, x_n \in A$ such that A is integral over $C = k[x_1, \ldots, x_n]$ and $x_1 A \cap C = (x_1)$. Now consider $\mathfrak{a} \cap C$. We proceed by induction on the number of variables n.

If $n = 1$ then the theorem is obvious. So we consider the ideal $\mathfrak{a} \cap k[x_2, \ldots, x_n]$ in the polynomial ring $B = k[x_2, \ldots, x_n]$. By induction there are $t_2, \ldots, t_n \in B$ such that B is integral over $k[t_2, \ldots, t_n]$ and $\mathfrak{a} \cap k[t_2, \ldots, t_n] = (t_2, \ldots, t_d)$ for some $d \leq n$. Setting $D = k[x_1, t_2, \ldots, t_n]$ we have that A is integral over D and

$$\mathfrak{a} \cap D = x_1 D + \mathfrak{a} \cap k[t_2, \ldots, t_n] = (x_1) + (t_2, \ldots, t_n) = (x_1, t_2, \ldots, t_d).$$

Step 4 We now prove the general case of the theorem for the polynomial ring $A = k[Y_1, \ldots, Y_n]$.

We proceed by induction on r. Step 3 finished the base case of $r = 1$. So by induction we may assume that there exists algebraically independent elements $x_1, \ldots, x_n$ such that A is integral over $C = k[x_1, \ldots, x_n]$ and such that

$$\mathfrak{a}_i \cap C = (x_1, \ldots, x_{h(i)}) \qquad \text{with } h(i) \leq h(j) \text{ for } 1 \leq i \leq j \leq r-1.$$

Write $d = h(r-1)$. We may assume that $h(r-1) > 0$. Consider $\mathfrak{a}_r \cap k[x_{d+1}, \ldots, x_n]$ in $D = k[x_{d+1}, \ldots, x_n]$. By Step 3 we can find $t_{d+1}, \ldots, t_n$ algebraically independent over k such that D is integral over $k[t_{d+1}, \ldots, t_n]$ and

$$\mathfrak{a}_r \cap k[t_{d+1}, \ldots, t_n] = (t_d, \ldots, t_{h(r)}) \qquad \text{where } h(r) \leq n.$$

We leave it to the reader to check that A is integral over

$$B = k[x_1, \ldots, x_d, t_{d+1}, \ldots, t_n]$$

and that

$$\mathfrak{a}_i \cap B = (x_1, \ldots, x_{h(i)}) \qquad \text{for } i < r$$

and

$$\mathfrak{a}_r \cap B = (x_1, \ldots, x_d, t_{d+1}, \ldots, t_{h(r)}).$$

This completes the proof. ■

Definition If k is a field, A is called an **affine k-algebra** if A is a finitely generated k-algebra. If in addition A is a domain, then A is called an **affine k-domain**.

Definition If K is a field extension of k, then the **transcendence degree** of K over k is the cardinality of a maximal algebraically independent set S over k. Hence, K is an algebraic extension of $k(S)$. We denote the transcendence degree of K over k by $\operatorname{tr\,deg}_k(K)$.

Corollary 4.73 *Suppose A is an affine k-domain. Then $\dim(A) = \operatorname{tr\,deg}_k(K)$, where $K = \operatorname{Frac}(A)$.*

Proof Let $\dim(A) = n$ and let

$$\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

be a corresponding chain of prime ideals in A. By Noether's Normalization Lemma, Theorem 4.72, we have algebraically independent elements $x_1, \ldots, x_d \in A$ such that

$$k[x_1, \ldots, x_d] \hookrightarrow A$$

is an integral extension and such that

$$\mathfrak{p}_i \cap k[x_1, \ldots, x_d] = (x_1, \ldots, x_{h(i)})$$

where $i < j$ implies that $h(i) \leq h(j)$. In particular, since $k[x_1, \ldots, x_d] \hookrightarrow A$ is an integral extension, we have that $d = n$ and $\mathfrak{p}_i \cap k[x_1, \ldots, x_n] = (x_1, \ldots, x_i)$. Taking fraction fields we have

$$k \hookrightarrow k(x_1, \ldots, x_n) \hookrightarrow K$$

where the second inclusion is an algebraic field extension. Thus $\operatorname{tr\,deg}_k(K) \leq n$. If $\operatorname{tr\,deg}_k(K) < n$ then we would have an integral extension

$$k[y_1, \ldots, y_m] \hookrightarrow A$$

with $m < n$. But this would imply that $\dim(A) = m < n$, a contradiction. Therefore $\operatorname{tr\,deg}_k(K) = n = \dim(A)$. ■

Corollary 4.74 *Let A be an affine k-algebra and let $\mathfrak{m}$ be a maximal ideal of A. Then $A/\mathfrak{m}$ is a finite-dimensional vector space over k.*

Proof By Noether's Normalization Lemma we can find $x_1, \ldots, x_n \in A$ that are algebraically independent over k such that

$$k[x_1, \ldots, x_n] \hookrightarrow A$$

is an integral extension and such that

$$\mathfrak{m} \cap k[x_1, \ldots, x_n] = (x_1, \ldots, x_n).$$

Therefore

$$k = k[x_1, \ldots, x_n]/(x_1, \ldots, x_n) \hookrightarrow A/\mathfrak{m}$$

is an integral extension which is finitely generated as a k-algebra. Thus $A/\mathfrak{m}$ is a finitely generated k-module. ■

Corollary 4.75 *Let $A = k[X_1, X_2, \ldots, X_n]$. Then any maximal ideal $\mathfrak{m}$ is generated by n elements. Moreover, $\mathfrak{m}$ can be written as*

$$\mathfrak{m} = (f_1(X_1), f_2(X_1, X_2), \ldots, f_n(X_1, \ldots, X_n)).$$

Proof Let $\mathfrak{m}$ be a maximal ideal of A. Then by the previous corollary

$$k \hookrightarrow A/\mathfrak{m}$$

is a finite field-extension. Write α_i for $\overline{X_i} \in A/\mathfrak{m}$. So we have:

$$\begin{aligned} A/\mathfrak{m} &= k[\alpha_1, \ldots, \alpha_n] \\ &= k(\alpha_1, \ldots, \alpha_n). \end{aligned}$$

Letting $\mathrm{P}_k^{\alpha}(X)$ denote the minimal irreducible polynomial for α over k, consider the polynomials

$$\begin{array}{ll} \mathrm{P}_{k_0}^{\alpha_1}(X_1) & \text{where } k_0 = k, \\ \mathrm{P}_{k_1}^{\alpha_2}(X_2) & \text{where } k_1 = k[\alpha_1], \\ \vdots & \vdots \\ \mathrm{P}_{k_{n-1}}^{\alpha_n}(X_n) & \text{where } k_{n-1} = k[\alpha_1, \ldots, \alpha_{n-1}]. \end{array}$$

Let $f_i(X_1, \ldots, X_i)$ be $\mathrm{P}_{k_{i-1}}^{\alpha_i}(X_i)$ where $\alpha_1, \ldots, \alpha_{i-1}$ are replaced by $X_1, \ldots, X_{i-1}$ respectively. We now show that

$$\mathfrak{m} = (f_1(X_1), f_2(X_1, X_2), \ldots, f_n(X_1, \ldots, X_n)).$$

That

$$(f_1(X_1), f_2(X_1, X_2), \ldots, f_n(X_1, \ldots, X_n)) \subseteq \mathfrak{m}$$

is clear. The other containment will follow if we show that

$$K := k[X_1, \ldots, X_n]/(f_1(X_1), f_2(X_1, X_2), \ldots, f_n(X_1, \ldots, X_n)) \cong A/\mathfrak{m}.$$

Note that

$$\begin{aligned} K &= \frac{k[X_1, \ldots, X_n]}{(f_1(X_1), f_2(X_1, X_2), \ldots, f_n(X_1, \ldots, X_n))} \\ &\cong \frac{k[\alpha_1, X_2, \ldots, X_n]}{(f_2(\alpha_1, X_2), \ldots, f_n(\alpha_1, X_2, \ldots, X_n))} \\ &\cong \frac{k[\alpha_1, \alpha_2, \ldots, X_n]}{(f_3(\alpha_1, \alpha_2, X_3), \ldots, f_n(\alpha_1, \alpha_2, X_3, \ldots, X_n))} \\ &\vdots \\ &\cong k[\alpha_1, \ldots, \alpha_n] \\ &\cong A/\mathfrak{m}. \end{aligned}$$

So we are done. ■

Corollary 4.76 *Let k be an algebraically closed field and let $A = k[X_1, \ldots, X_n]$. Then every maximal ideal of A is of the form*

$$\mathfrak{m} = (X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n),$$

where $a_1, a_2, \ldots, a_n \in k$.

Proof Use the previous corollary. ■

Exercise 4.77 *By the previous Corollary, we have a bijective correspondence between k^n and* $\mathrm{MaxSpec}(k[X_1, \ldots, X_n])$ *when k is algebraically closed. Show that $k^n \cong \mathrm{MaxSpec}(k[X_1, \ldots, X_n])$ is dense in* $\mathrm{Spec}(k[X_1, \ldots, X_n])$.

Corollary 4.78 *Let A be an affine domain, $\mathfrak{p}$ a prime ideal of A. Then*

$$\mathrm{ht}(\mathfrak{p}) + \dim(A/\mathfrak{p}) = \dim(A).$$

Proof By Noether's Normalization Lemma we can find $x_1, \ldots, x_n \in A$ which are algebraically independent over k with A integral over $k[x_1, \ldots, x_n]$ and such that $\mathfrak{p} \cap k[x_1, \ldots, x_n] = (x_1, \ldots, x_i)$. By the Going-Down Theorem $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}((x_1, \ldots, x_n)) = i$. Also since $k[x_1, \ldots, x_n] \hookrightarrow A$ is an integral extension, so is

$$k[x_{i+1}, \ldots, x_n] = k[x_1, \ldots, x_n]/(x_1, \ldots, x_i) \hookrightarrow A/\mathfrak{p}.$$

Thus $\dim(A/\mathfrak{p}) = n - i = \dim(A) - \mathrm{ht}(\mathfrak{p})$. ■

Remark As a special case of this corollary we get the following result:
If $\mathfrak{m}$ is a maximal ideal in an affine domain A, then $\mathrm{ht}(\mathfrak{m}) = \dim(A)$.

Definition Let A be a ring. If any two saturated chains of primes of A between two primes $\mathfrak{p} \subsetneq \mathfrak{q}$ have the same length, then A is called **catenary**.

Corollary 4.79 *Let A be an affine k-algebra, then A is catenary.*

Proof Let

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

and

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

be two saturated chains of prime ideals in A. By considering both chains in $A/\mathfrak{p}$, which is an affine domain, we may assume $\mathfrak{p} = 0$. Since $A/\mathfrak{p}$ is an affine domain we have by the previous corollary that

$$\begin{aligned} \dim(A) - r &= \dim(A/\mathfrak{p}_r) \\ &= \dim(A/\mathfrak{q}) \\ &= \dim(A/\mathfrak{q}_s) \\ &= \dim(A) - s. \end{aligned}$$

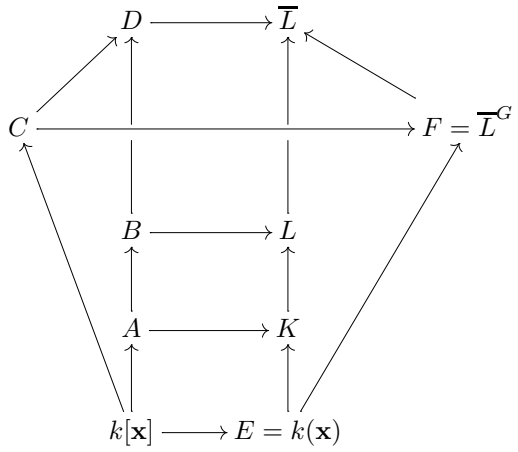
Therefore $r = s$. ■

Corollary 4.80 *Let A be an affine k-domain, $K = \mathrm{Frac}(A)$, L/K a finite field-extension, and B the integral closure of A in L. Then B is a finitely generated A-module.*

Proof By Noether's Normalization Lemma we can find $x_1, \ldots, x_n \in A$ such that A is integral over $k[x_1, \ldots, x_n]$ where $x_1, \ldots, x_n$ are algebraically independent over k. So it suffices to show that B is a finitely generated $k[x_1, \ldots, x_n]$-module. Now let $\overline{L}$ be the normal closure of L in the algebraic closure of K and let D be the integral closure of $k[x_1, \ldots, x_n]$ in $\overline{L}$.

Set $F = \overline{L}^G$ where $G = \mathrm{Gal}_{k(\mathbf{x})}(\overline{L})$. Then $\overline{L}$ is separable over F and F is purely inseparable over $k(x_1, \ldots, x_n)$ by Proposition 4.19. Let C be the integral closure of $k[x_1, \ldots, x_n]$ in F. If we can show that C is a finitely generated $k[x_1, \ldots, x_n]$-module, then C would be Noetherian, and hence normal. It would then follow from Theorem 4.63 that D was a finitely generated C-module, and hence that B was a finitely generated A-module.

Therefore we must show that C is a finitely generated $k[x_1, \ldots, x_n]$-module in the situation where $C \subseteq F$ and F is purely inseparable over $E = k(x_1, \ldots, x_n)$. We have the following diagram:



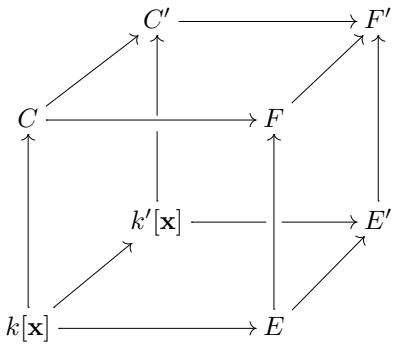
Since $F/k(\mathbf{x})$ is purely inseparable, we can write $F = E(y_1, \ldots, y_d)$ where $E = k(\mathbf{x})$, such that there exists $i > 0$ with $y_j^{p^i} \in E$ for each $j = 1, \ldots, d$. Thus we can write

$$y_j^{p^i} = \frac{f_j(x_1, \ldots, x_n)}{g_j(x_1, \ldots, x_n)} \in k(\mathbf{x}) = E$$

where $f_j, g_j \in k[x_1, \ldots, x_n]$. Let S be the (finite) set of coefficients of the polynomials f_j, g_j. Set $k' = k\left(S^{\frac{1}{p^i}}\right)$. Since we are appending a finite number of p^i-th roots, $[k' : k] < \infty$. Set

$$\begin{aligned} E' &= k'(x_1, \ldots, x_n), \\ F' &= k'(x_1^{\frac{1}{p^i}}, \ldots, x_n^{\frac{1}{p^i}}), \\ C' &= k[x_1^{\frac{1}{p^i}}, \ldots, x_n^{\frac{1}{p^i}}]. \end{aligned}$$

Then we have the following diagram:



Clearly $k'[x_1, \ldots, x_n]$ is a finitely generated $k[x_1, \ldots, x_n]$-module since $[k' : k] < \infty$. Also note that C' is a polynomial ring. So C' is a UFD and hence normal. So C' is the integral closure of $k[x_1, \ldots, x_n]$ in F'. Since C is integral over $k[x_1, \ldots, x_n]$, C' is the integral closure of C in F'. Since C' is integral over $k'[x_1, \ldots, x_n]$ and is finitely generated as an algebra over $k'[x_1, \ldots, x_n]$, we have that C' is a finitely generated as a $k'[x_1, \ldots, x_n]$-module. It follows that C is a finitely generated $k[x_1, \ldots, x_n]$-module. ■

Exercise 4.81 *Let $f : A \to B$ be a map of finitely generated k-algebras, where k is a field. Suppose $\mathfrak{m}$ is a maximal ideal of B. Then $f^{-1}(\mathfrak{m})$ is a maximal ideal of A.*

Exercise 4.82 *Let A be a finitely generated k-algebra, where k is a field. For any ideal I of A we have*

$$\sqrt{I} = \bigcap_{I \subseteq \mathfrak{m}} \mathfrak{m},$$

where $\mathfrak{m}$ runs through all maximal ideals of A.

Exercise 4.83 *Suppose A is a Noetherian domain and B is a finitely generated A-algebra. Then there exist $x_1, \ldots, x_n \in B$ algebraically independent over A and $0 \neq a \in A$ such that $A[\frac{1}{a}][x_1, \ldots, x_n] \hookrightarrow B[\frac{1}{a}]$ is an integral extension.*

Exercise 4.84 *Let $f_1, \ldots, f_t \in \mathbb{Z}[X_1, \ldots, X_n]$. Then $f_1, \ldots, f_t$ have a common root over $\mathbb{C}$ if and only if they have a common root over finite fields of infinitely many prime characteristics.*

Exercise 4.85 *Let K be an algebraically closed field and let $L \supseteq K$ be a field-extension. Then a set of polynomials in $K[x_1, \ldots, x_n]$ has a common solution in L if and only if they have a common solution in K.*

Chapter 5

Homological Methods

At first, homological methods may seem very abstract. How can something so abstract be useful? Consider the following:

Definition If $(A, \mathfrak{m})$ is local, A is a **regular local ring** if

$$\dim(A) = \boldsymbol{\mu}(\mathfrak{m}) := \{\text{the minimal number of generators of } \mathfrak{m}\}.$$

In particular, every field is a regular local ring of dimension 0 and every DVR is a regular local ring of dimension 1 (and vice versa). Regular local rings correspond to smooth points of an algebraic variety. Before homological methods, proving the following result took hundreds of pages even in special cases.

Theorem *If A is a regular local ring and $\mathfrak{p}$ is a prime ideal of A, then $A_{\mathfrak{p}}$ is a regular local ring.*

We will develop the tools of homological algebra and kill this problem with ease.

5.1 Complexes and Homology

Definition Let A be a ring, by a **complex**, we mean a sequence of A-modules and A-module homomorphisms

$$\cdots \longrightarrow X_{n+1} \xrightarrow{d_{n+1}} X_n \xrightarrow{d_n} X_{n-1} \longrightarrow \cdots$$

such that $d_{n-1} \circ d_n = 0$ for all $n \in \mathbb{Z}$. We denote a complex by $X_\bullet$.

Definition If $X_\bullet$ is a complex of A-modules, then the nth **homology** of $X_\bullet$ is

$$H_n(X_\bullet) := \frac{\operatorname{Ker}(d_n)}{\operatorname{Im}(d_{n+1})}.$$

Definition Let A be a ring. By a **cocomplex**, we mean a sequence of A-modules and A-module homomorphisms

$$\cdots \longrightarrow X^{n-1} \xrightarrow{d^{n-1}} X^n \xrightarrow{d^n} X^{n+1} \longrightarrow \cdots$$

such that $d^n \circ d^{n-1} = 0$ for all $n \in \mathbb{Z}$. We denote a cocomplex by $X^\bullet$.

Definition If $X^\bullet$ is a cocomplex of A-modules, then the nth **cohomology** of $X^\bullet$ is

$$H^n(X^\bullet) := \frac{\mathrm{Ker}(d^n)}{\mathrm{Im}(d^{n-1})}.$$

Since complexes and cocomplexes are dual notions, we will only discuss the situation for complexes, and leave the rest as an exercise for the reader.

Definition Let $X_\bullet$ and $Y_\bullet$ be two complexes over a ring A. A **map of complexes**

$$f_\bullet : X_\bullet \to Y_\bullet$$

is a collection of A-module homomorphisms such that the diagram below commutes:

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & X_{n+1} & \xrightarrow{d^X_{n+1}} & X_n & \xrightarrow{d^X_n} & X_{n-1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f_{n+1}} & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \\
\cdots & \longrightarrow & Y_{n+1} & \xrightarrow[d^Y_{n+1}]{} & Y_n & \xrightarrow[d^Y_n]{} & Y_{n-1} & \longrightarrow & \cdots
\end{array}$$

Exercise 5.1 *Show that a map of complexes $f_\bullet : X_\bullet \to Y_\bullet$, defines a collection of homomorphisms:*

$$\begin{aligned}
f_i &: \mathrm{Ker}(d^X_i) \to \mathrm{Ker}(d^Y_i). \\
f_i &: \mathrm{Im}(d^X_{i+1}) \to \mathrm{Im}(d^Y_{i+1}). \\
H_n(f_\bullet) &: H_n(X_\bullet) \to H_n(Y_\bullet).
\end{aligned}$$

Definition Two maps of A-complexes

$$\begin{aligned}
f_\bullet &: X_\bullet \to Y_\bullet, \\
g_\bullet &: X_\bullet \to Y_\bullet,
\end{aligned}$$

are called **homotopic** if there exist A-module maps $h_n : X_n \to Y_{n+1}$ such that in the diagram below

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & X_{n+1} & \xrightarrow{d^X_{n+1}} & X_n & \xrightarrow{d^X_n} & X_{n-1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f_{n+1}}\downarrow{\scriptstyle g_{n+1}} & \swarrow{\scriptstyle h_n} & \downarrow{\scriptstyle f_n}\downarrow{\scriptstyle g_n} & \swarrow{\scriptstyle h_{n-1}} & \downarrow{\scriptstyle f_{n-1}}\downarrow{\scriptstyle g_{n-1}} & & \\
\cdots & \longrightarrow & Y_{n+1} & \xrightarrow[d^Y_{n+1}]{} & Y_n & \xrightarrow[d^Y_n]{} & Y_{n-1} & \longrightarrow & \cdots
\end{array}$$

we have

$$d^Y_{n+1} \circ h_n + h_{n-1} \circ d^X_n = f_n - g_n$$

for all $n \in \mathbb{Z}$. We denote this by $f_\bullet \sim g_\bullet$.

Exercise 5.2 *Check that $f_\bullet \sim g_\bullet$ implies that $H_n(f_\bullet) = H_n(g_\bullet)$.*

Definition A sequence of complexes and complex maps

$$0 \longrightarrow X'_\bullet \xrightarrow{f_\bullet} X_\bullet \xrightarrow{g_\bullet} X''_\bullet \longrightarrow 0$$

is called an **exact sequence** if for all $n \in \mathbb{Z}$,

$$0 \longrightarrow X'_n \xrightarrow{f_n} X_n \xrightarrow{g_n} X''_n \longrightarrow 0$$

is an exact sequence of A-modules and A-module homomorphisms.

Lemma 5.3 *Given an exact sequence of complexes,*

$$0 \longrightarrow X'_\bullet \xrightarrow{f_\bullet} X_\bullet \xrightarrow{g_\bullet} X''_\bullet \longrightarrow 0$$

we obtain a long exact sequence of homologies:

$$\cdots \longrightarrow H_{n+1}(X'_\bullet) \xrightarrow{H_{n+1}(f_\bullet)} H_{n+1}(X_\bullet) \xrightarrow{H_{n+1}(g_\bullet)} H_{n+1}(X''_\bullet) \xrightarrow{\partial_{n+1}}$$
$$H_n(X'_\bullet) \xrightarrow{H_n(f_\bullet)} H_n(X_\bullet) \xrightarrow{H_n(g_\bullet)} H_n(X''_\bullet) \xrightarrow{\partial_n}$$
$$H_{n-1}(X'_\bullet) \xrightarrow{H_{n-1}(f_\bullet)} H_{n-1}(X_\bullet) \xrightarrow{H_{n-1}(g_\bullet)} H_{n-1}(X''_\bullet) \longrightarrow \cdots$$

Proof Consider the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & X'_{n+1} & \xrightarrow{f_{n+1}} & X_{n+1} & \xrightarrow{g_{n+1}} & X''_{n+1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d'_{n+1}} & & \downarrow{\scriptstyle d_{n+1}} & & \downarrow{\scriptstyle d''_{n+1}} & & \\
0 & \longrightarrow & X'_n & \xrightarrow{f_n} & X_n & \xrightarrow{g_n} & X''_n & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d'_n} & & \downarrow{\scriptstyle d_n} & & \downarrow{\scriptstyle d''_n} & & \\
0 & \longrightarrow & X'_{n-1} & \xrightarrow{f_{n-1}} & X_{n-1} & \xrightarrow{g_{n-1}} & X''_{n-1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

First we will show that

$$H_n(X'_\bullet) \overset{H_n(f_\bullet)}{\longrightarrow} H_n(X_\bullet) \overset{H_n(g_\bullet)}{\longrightarrow} H_n(X''_\bullet)$$

is exact. By the construction of $H_n(f_\bullet)$ and $H_n(g_\bullet)$ we know that $\operatorname{Im} H_n(f_\bullet) \subseteq \operatorname{Ker} H_n(g_\bullet)$. Thus we must show that

$$\operatorname{Ker} H_n(g_\bullet) \subseteq \operatorname{Im} H_n(f_\bullet).$$

Let $x_n \in X_n$ and suppose that $\overline{x}_n \in \operatorname{Ker} H_n(g_\bullet)$. Then there exists $x''_{n+1} \in X''_{n+1}$ such that

$$d''_{n+1}(x''_{n+1}) = g_n(x_n).$$

By exactness of the rows, there exists $x_{n+1} \in X_{n+1}$ such that

$$g_{n+1}(x_{n+1}) = x''_{n+1}.$$

This x_{n+1} in turn maps down via d_{n+1} to some element of X_n, call it y_n. By the commutativity of the diagram

$$g_n(x_n - y_n) = 0$$

and so by the exactness of the rows, there exists $x'_n \in X'_n$ such that

$$f_n(x'_n) = x_n - y_n.$$

However, since $y_n = d_{n+1}(x_{n+1})$ we have $\overline{y}_n = 0$ and

$$\overline{x}_n = \overline{x}_n - \overline{y}_n \in H_n(X_\bullet).$$

Thus, $\overline{x}_n \in \operatorname{Im} H_n(f_\bullet)$. The method used in the above part of the proof is called **diagram chasing**. Often when it is done in practice, the elements found above are written next to the object they live in on the commutative diagram itself.

Now we need to define the ∂_n's. Consider $\overline{x}''_n \in H_n(X''_\bullet)$ we will define $\partial_n(\overline{x}''_n)$. Take $x_n \in X_n$ such that

$$g_n(x_n) = x''_n.$$

Since $x''_n \in \operatorname{Ker}(d''_n)$, $d''_n(x''_n) = 0$. Hence if $x_{n-1} = d_n(x_n)$, then

$$g_{n-1}(x_{n-1}) = 0.$$

So by the exactness of the rows above, there exists $x'_{n-1} \in X'_{n-1}$ such that

$$f_{n-1}(x'_{n-1}) = x_{n-1}.$$

Hence $d'_{n-1}(x'_{n-1}) = 0$. Since $d_{n-1}(x_{n-1}) = d_{n-1} \circ d_n(x_n) = 0$,

$$d'_{n-1}(x'_{n-1}) = 0.$$

Now we define

$$\partial_n(x''_n) := \overline{x}'_{n-1} \in H_{n-1}(X'_\bullet).$$

It is left as an exercise for the reader to check that this definition of ∂_n is well defined. Moreover, the reader should check that the sequences

$$H_n(X_\bullet) \xrightarrow{H_n(g_\bullet)} H_n(X''_\bullet) \xrightarrow{\partial_n} H_{n-1}(X'_\bullet),$$
$$H_n(X''_\bullet) \xrightarrow{\partial_n} H_{n-1}(X'_\bullet) \xrightarrow{H_{n-1}(f_\bullet)} H_{n-1}(X_\bullet),$$

are both exact. ■

Definition In the above proposition, the ∂_n's are called **connecting homomorphisms**.

Corollary 5.4 *Given a commutative diagram of complexes with short exact rows:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X'_\bullet & \longrightarrow & X_\bullet & \longrightarrow & X''_\bullet & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & Y'_\bullet & \longrightarrow & Y_\bullet & \longrightarrow & Y''_\bullet & \longrightarrow & 0 \end{array}$$

we get a commutative diagram with long exact rows:

$$\begin{array}{ccccccccccccc} \cdots & \longrightarrow & H_{n+1}(X''_\bullet) & \longrightarrow & H_n(X'_\bullet) & \longrightarrow & H_n(X_\bullet) & \longrightarrow & H_n(X''_\bullet) & \longrightarrow & H_{n-1}(X'_\bullet) & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & H_{n+1}(Y''_\bullet) & \longrightarrow & H_n(Y'_\bullet) & \longrightarrow & H_n(Y_\bullet) & \longrightarrow & H_n(Y''_\bullet) & \longrightarrow & H_{n-1}(Y'_\bullet) & \longrightarrow & \cdots \end{array}$$

Definition Given a map of complexes $f_\bullet : X_\bullet \to Y_\bullet$, the **mapping cone** of $f_\bullet$ is the following complex:

$$\cdots \longrightarrow X_i \oplus Y_{i+1} \longrightarrow X_{i-1} \oplus Y_i \longrightarrow X_{i-2} \oplus Y_{i-1} \longrightarrow \cdots$$

where the degree i part is $X_{i-1} \oplus Y_i$ and the differentials are defined as follows:

$$\begin{aligned} d_i : X_{i-1} \oplus Y_i &\to X_{i-2} \oplus Y_{i-1} \\ (x, y) &\mapsto (-d^X_{i-1}(x), d^Y_i(y) - f_{i-1}(x)) \end{aligned}$$

Exercise 5.5 *Show that the mapping cone of a map of complexes is a complex.*

Definition Given a complex $(X_\bullet, d^X_\bullet)$, $X_\bullet(j)$ is used to denote a **shift**, where $X_i(j) := X_{i+j}$ and with differential $d_i^{X(j)} = (-1)^j d^X_{i+j}$.

Exercise 5.6 *Given a map of complexes $f_\bullet : X_\bullet \to Y_\bullet$, let $C_\bullet$ be the mapping cone of $f_\bullet$. Then there is a short exact sequence of complexes:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Y_\bullet & \longrightarrow & C_\bullet & \longrightarrow & X_\bullet(-1) & \longrightarrow & 0 \\ & & y & \longmapsto & (0, y) & & & & \\ & & & & (x, y) & \longmapsto & x & & \end{array}$$

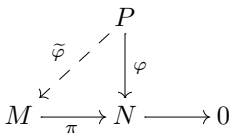
The above short exact sequence of complexes induces a long exact sequence:

$$\cdots \longrightarrow H_i(X_\bullet) \xrightarrow{H_i(f_\bullet)} H_i(Y_\bullet) \longrightarrow H_i(C_\bullet) \longrightarrow \cdots$$

5.1.1 Projective Resolutions

Definition An A-module P is **projective** if any of the following equivalent conditions are met:

(1) Given any right exact sequence $M \to N \to 0$ of A modules and a homomorphism $\varphi : P \to N$, there exits $\widetilde{\varphi} : P \to M$ such that the diagram below commutes:



(2) $\mathrm{Hom}_A(P, -)$ is an exact functor.

(3) Every short exact sequence $0 \to M' \to M \to P \to 0$ is split exact.

(4) There is a free module F such that $F \cong P \oplus Q$ for some A-module Q.

Exercise 5.7 *Show that the conditions in the above definition are actually equivalent.*

Exercise 5.8 *Show that if $A \to B$ is a ring homomorphism and P is a projective A-module, then $P \otimes_A B$ is a projective B-module.*

Definition If M is an A-module, a **projective resolution** of M is a complex of projective modules $P_\bullet$ and a map $\pi : P_0 \to M$ such that

$$\cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\pi} M \longrightarrow 0$$

is exact.

Given a ring A, every module M has a projective resolution. Firstly, note that given any module M, we may map a free module F_0 onto M. Set

$$S_1 := \mathrm{Ker}(F_0 \to M).$$

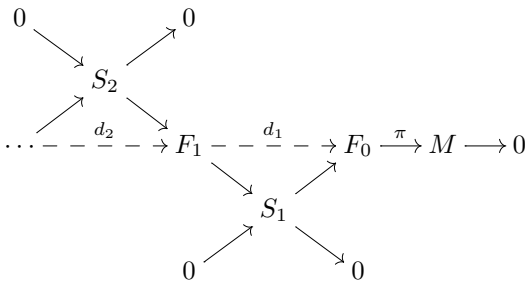
Now we may map another free module onto S_1. Hence we may inductively define

$$S_{i+1} := \mathrm{Ker}(F_i \to S_i).$$

Now we may inductively write the exact sequences:

$$0 \to S_1 \to F_0 \to M \to 0,$$
$$0 \to S_{i+1} \to F_i \to S_i \to 0.$$

Now we put the above short exact sequences together letting each S_i connect the short exact sequences:



The d_i's above are formed by taking the composition of the relevant maps, while π is the canonical surjection. Hence we obtain a free resolution of M. Since every free module is projective, we obtain a projective resolution of M. Note that if M were a finitely generated module over a Noetherian ring, then we could insist that each F_i be a finitely generated free module.

Lemma 5.9 *Let $f : M \to N$ be a homomorphism of A-modules. If $P_\bullet$ is a complex of projective A-modules such that $H_0(P_\bullet) = M$ and $Q_\bullet$ is an exact complex with $H_0(Q_\bullet) = N$, then there exists a map of complexes $f_\bullet : P_\bullet \to Q_\bullet$ lifting f.*

Proof Here is the situation in question:

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & P_1 & \xrightarrow{d_1^M} & P_0 & \xrightarrow{\pi_M} & M & \longrightarrow & 0 \\ & & & & & & \downarrow{\scriptstyle f} & & \\ \cdots & \longrightarrow & Q_1 & \xrightarrow{d_1^N} & Q_0 & \xrightarrow{\pi_N} & N & \longrightarrow & 0 \end{array}$$

Since P_0 is projective, we can obtain f_0 by:

$$\begin{array}{ccccc} & & P_0 & & \\ & \swarrow^{f_0} & \downarrow{\scriptstyle f\circ\pi_M} & & \\ Q_0 & \xrightarrow[\pi_N]{} & N & \longrightarrow & 0 \end{array}$$

Now since $S_1 = \mathrm{Ker}(\pi_N) = \mathrm{Im}(d_1^N)$, we can obtain f_1 by:

$$\begin{array}{ccccc} & & P_1 & & \\ & \swarrow^{f_1} & \downarrow{\scriptstyle f_0\circ d_1^M} & & \\ Q_1 & \xrightarrow[d_1^N]{} & S_1 & \longrightarrow & 0 \end{array}$$

Note that $f_0 \circ d_1^M$ maps into S_1 since it is in $\mathrm{Ker}(\pi_N)$. Working inductively, we repeat a similar procedure to find $f_\bullet$. ■

Remark Note that the lift $f_\bullet$ is not unique.

Lemma 5.10 *Let $f : M \to N$ be a homomorphism of A-modules, $P_\bullet$ be a complex of projective A-modules such that $H_0(P_\bullet) = M$, and $Q_\bullet$ be an exact complex with $H_0(Q_\bullet) = N$. If $f_\bullet$ and $g_\bullet$ are two lifts of the map f, then $f_\bullet \sim g_\bullet$.*

Proof Here is the situation in question:

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & P_1 & \xrightarrow{d_1^M} & P_0 & \xrightarrow{\pi_M} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f_1} \downarrow{\scriptstyle g_1} & & \downarrow{\scriptstyle f_0} \downarrow{\scriptstyle g_0} & & \downarrow{\scriptstyle f} & & \\
\cdots & \longrightarrow & Q_1 & \xrightarrow[d_1^N]{} & Q_0 & \xrightarrow[\pi_N]{} & N & \longrightarrow & 0
\end{array}$$

Since both $f_\bullet$ and $g_\bullet$ are chain maps, we have that

$$f \circ \pi_M = \pi_N \circ f_0 = \pi_N \circ g_0,$$

and so we see

$$0 = \pi_N \circ f_0 - \pi_N \circ g_0 = \pi_N \circ (f_0 - g_0).$$

Thus $\mathrm{Im}(f_0 - g_0) \subseteq \mathrm{Ker}(\pi_N) = \mathrm{Im}(d_1^N)$. By the projectivity of P_0, we obtain h_0

$$\begin{array}{ccccc}
 & & P_0 & & \\
 & \overset{h_0}{\swarrow} & \downarrow{\scriptstyle f_0 - g_0} & & \\
Q_1 & \xrightarrow[d_1^N]{} & \mathrm{Im}(d_1^N) & \longrightarrow & 0
\end{array}$$

such that $h_0 : P_0 \to Q_1$. Set h_{-1} to be the zero map and $d_0^M := \pi_M$. Now

$$d_1^N \circ h_0 + h_{-1} \circ d_0^M = f_0 - g_0.$$

Working inductively, suppose that we have constructed homotopy maps for $i < n$. We must show

$$d_{n+1}^N \circ h_n + h_{n-1} \circ d_n^M = f_n - g_n.$$

By the definition of a map of complexes, we have that:

$$\begin{aligned} d_n^N \circ f_n &= f_{n-1} \circ d_n^M, \\ d_n^N \circ g_n &= g_{n-1} \circ d_n^M, \end{aligned}$$

and so by the inductive hypothesis,

$$\begin{aligned} d_n^N \circ (f_n - g_n) &= (f_{n-1} - g_{n-1}) \circ d_n^M \\ &= (d_n^N \circ h_{n-1} + h_{n-2} \circ d_{n-1}^M) \circ d_n^M \\ &= d_n^N \circ h_{n-1} \circ d_n^M + h_{n-2} \circ d_{n-1}^M \circ d_n^M \\ &= d_n^N \circ h_{n-1} \circ d_n^M. \end{aligned}$$

Thus

$$\begin{aligned} d_n^N \circ (f_n - g_n - h_{n-1} \circ d_n^M) &= d_n^N \circ (f_n - g_n) - d_n^N \circ h_{n-1} \circ d_n^M \\ &= d_n^N \circ h_{n-1} \circ d_n^M - d_n^N \circ h_{n-1} \circ d_n^M \\ &= 0. \end{aligned}$$

Therefore

$$\mathrm{Im}(f_n - g_n - h_{n-1} \circ d_n^M) \subseteq \mathrm{Ker}(d_n^N) = \mathrm{Im}(d_{n+1}^N).$$

Now we obtain h_n as before

$$\begin{array}{ccccc} & & P_n & & \\ & \overset{h_n}{\swarrow} & \downarrow{\scriptstyle f_n - g_n - h_{n-1} \circ d_n^M} & & \\ Q_{n+1} & \xrightarrow[d_{n+1}^N]{} & \mathrm{Im}(d_{n+1}^N) & \longrightarrow & 0 \end{array}$$

such that $h_n : P_n \to Q_{n+1}$ and $d_{n+1}^N \circ h_n + h_{n-1} \circ d_n^M = f_n - g_n$. Thus $f_\bullet$ is homotopic to $g_\bullet$. ■

Lemma 5.11 (Horseshoe Lemma) *Consider the following short exact sequence:*

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

Let $P'_\bullet \to M'$ and $P''_\bullet \to M''$ be projective resolutions. Then, there exists a projective resolution $P_\bullet \to M$ such that the rows in the diagram below are exact:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P'_\bullet & \longrightarrow & P_\bullet & \longrightarrow & P''_\bullet & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \end{array}$$

Proof Take projective resolutions $(P'_\bullet, \pi')$ and $(P''_\bullet, \pi'')$ of M' and M'' respectively and consider the following commutative diagram:

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & P'_1 & \xrightarrow{d'_1} & P'_0 & \xrightarrow{\pi'} & M' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle f} & & \\ \cdots & \dashrightarrow & P'_1 \oplus P''_1 & \xrightarrow{d_1} & P'_0 \oplus P''_0 & \xrightarrow{\pi} & M & \longrightarrow & 0 \\ & & \downarrow & \nearrow_{\eta_1} & \downarrow & \nearrow_{\eta_0} & \downarrow{\scriptstyle g} & & \\ \cdots & \longrightarrow & P''_1 & \xrightarrow{d''_1} & P''_0 & \xrightarrow{\pi''} & M'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

First we must define $\pi : P_0 = P_0' \oplus P_0'' \twoheadrightarrow M$ such that the diagram commutes. Since P_0'' is projective, there exist $\eta_0 : P_0'' \to M$ such that $g \circ \eta_0 = \pi''$. Define

$$\pi(x', x'') := f \circ \pi'(x') + \eta_0(x'').$$

This makes the diagram above commute. From a simple diagram chase one can see that π is surjective.

Now we will define d_1 and then complete the construction by induction. Since $\pi'' \circ d_1'' = g \circ \eta_0 \circ d_1'' = 0$, we have that

$$\mathrm{Im}(\eta_0 \circ d_1'') \subseteq \mathrm{Ker}(g) = \mathrm{Im}(f).$$

Thus we have the commutative diagram:

$$\begin{array}{ccccc} & & P_1'' & & \\ & \overset{\eta_1}{\swarrow} & \downarrow{\scriptstyle \eta_0 \circ d_1''} & & \\ P_0' & \xrightarrow{f \circ \pi'} & \mathrm{Im}(f) & \longrightarrow & 0 \end{array}$$

And so

$$f \circ \pi' \circ \eta_1 = \eta_0 \circ d_1''.$$

By changing the sign of η_1 we see that

$$f \circ \pi' \circ \eta_1 + \eta_0 \circ d_1'' = 0,$$

and so we define

$$d_1(x', x'') := (d_1'(x') + \eta_1(x''), d_1''(x'')).$$

Plugging everything in we see that $\pi \circ d_1 = 0$. Following the diagram around we see that $\mathrm{Im}(d_1) = \mathrm{Ker}(\pi)$.

Now working inductively, consider the diagram:

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & P_n' & \xrightarrow{d_n'} & P_{n-1}' & \xrightarrow{d_{n-1}'} & P_{n-2}' & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \dashrightarrow & P_n' \oplus P_n'' & \xrightarrow{d_n} & P_{n-1}' \oplus P_{n-1}'' & \xrightarrow{d_{n-1}} & P_{n-2}' \oplus P_{n-2}'' & \longrightarrow & \cdots \\ & & \downarrow & \overset{\eta_n}{\nearrow} & \downarrow & \overset{\eta_n - 1}{\nearrow} & \downarrow & & \\ \cdots & \longrightarrow & P_n'' & \xrightarrow{d_n''} & P_{n-1}'' & \xrightarrow{d_{n-1}''} & P_{n-2}'' & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

Here we have inductively defined $\eta_{n-1} : P''_{n-1} \to P'_{n-2}$ similarly to how we defined η_1 and we can write

$$d_{n-1}(x', x'') := (d'_{n-1}(x') + \eta_{n-1}(x''), d''_{n-1}(x'')).$$

We must now define d_n. By construction we have that

$$d'_{n-2} \circ \eta_{n-1} + \eta_{n-2} \circ d''_{n-1} = 0,$$

and so we see

$$d'_{n-2} \circ \eta_{n-1} \circ d''_n = -\eta_{n-1} \circ d''_{n-1} \circ d''_n = 0.$$

Thus $\mathrm{Im}(\eta_{n-1} \circ d''_n) \subseteq \mathrm{Ker}(d'_{n-2}) = \mathrm{Im}(d'_{n-1})$. Again we are in the following situation:

$$\begin{array}{ccccc} & & P''_n & & \\ & \overset{\eta_n}{\swarrow} & \downarrow{\scriptstyle \eta_{n-1}\circ d''_n} & & \\ P'_{n-1} & \longrightarrow & \mathrm{Im}(d'_{n-1}) & \longrightarrow & 0 \end{array}$$

So we may now define

$$d_n(x', x'') := (d'_n(x') + \eta_n(x''), d''_n(x'')).$$

with the sign of η_n chosen so that:

$$\begin{aligned} d_n \circ d_{n-1}(x', x'') &= (d'_n(d'_{n-1}(x') + \eta_{n-1}(x'')) + \eta_n(d''_{n-1}(x'')), d''_n(d''_{n-1}(x''))) \\ &= (d'_n(\eta_{n-1}(x'')) + \eta_n(d''_{n-1}(x'')), 0) \\ &= 0. \end{aligned}$$

Since the direct sum of two projective modules is projective, and since we can see that $\mathrm{Im}(d_n) = \mathrm{Ker}(d_{n-1})$, we see that we have constructed the needed exact sequence. ■

Compare the above construction to the construction of the mapping cone as described in the previous section.

Exercise 5.12 *Show that given the following commutative diagram of A-modules with exact rows:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0 \end{array}$$

Then there exist associated projective resolutions that form a commutative diagram of A-complexes with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P'_\bullet & \longrightarrow & P_\bullet & \longrightarrow & P''_\bullet & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & Q'_\bullet & \longrightarrow & Q_\bullet & \longrightarrow & Q''_\bullet & \longrightarrow & 0 \end{array}$$

Hint: Do you know how to draw cubes?

5.1.2 Injective Resolutions

Definition An A-module E is **injective** if any of the following equivalent conditions are met:

(1) Given any left exact sequence $0 \to M' \to M$ of A-modules and a homomorphism $\varphi : M' \to E$, there exits $\widetilde{\varphi} : M \to E$ such that the diagram below commutes:

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \xrightarrow{\iota} & M \\ & & \varphi \downarrow & \swarrow_{\widetilde{\varphi}} & \\ & & E & & \end{array}$$

(2) $\mathrm{Hom}_A(-, E)$ is an exact functor.

(3) Every short exact sequence $0 \to E \to M \to M'' \to 0$ is split exact.

Exercise 5.13 *Show that the conditions in the above definition are actually equivalent.*

Theorem 5.14 (Baer's Criterion) *Let A be a ring. An A-module E is injective if and only if given any ideal I of A, a module homomorphism $\varphi : I \to E$ can be extended to a module homomorphism $\Phi : A \to E$.*

Proof ($\Rightarrow$) If E is injective, and $\varphi : I \to E$, then apply the functor $\mathrm{Hom}_A(-, E)$ to

$$0 \to I \to A.$$

Since $\mathrm{Hom}_A(-, E)$ is an exact functor, $\varphi : I \to E$ can be extended to a module homomorphism $\Phi : A \to E$.

($\Leftarrow$) Suppose that every A-module homomorphism $I \to E$ can be lifted to a homomorphism $A \to E$. Consider the diagram:

$$\begin{array}{ccccc} 0 & \longrightarrow & L & \longrightarrow & M \\ & & \varphi \downarrow & & \\ & & E & & \end{array}$$

Let L' be a submodule of M containing L and $\varphi' : L' \to E$ be a lift of φ. In this case, the ordering: $(L', \varphi') \leq (L'', \varphi'')$ if $L' \subseteq L''$ and $\varphi''|_{L'} = \varphi'$, partially orders the set $\mathcal{S}$,

$$\mathcal{S} = \{(L', \varphi') : \varphi' \text{ lifts } \varphi \text{ to } L'\}.$$

Note that $\mathcal{S} \neq \varnothing$ as $(L, \varphi) \in \mathcal{S}$. Now considering any chain $\mathcal{C}$ in $\mathcal{S}$, it is clear that

$$\bigcup_{(L', \varphi') \in \mathcal{C}} (L', \varphi')$$

is an upper bound. Hence by Zorn's Lemma this set contains a maximal element, $(M', \widetilde{\varphi})$. We will show that $M' = M$. Suppose that $m \in M - M'$. Consider the ideal $(M' :_A m)$. Note that

$$\begin{aligned}(M' :_A m) &\to E,\\ a &\mapsto \widetilde{\varphi}(am),\end{aligned}$$

is an A-module homomorphism from $(M' :_A m)$ to E, thus there exits an A-module homomorphism $\Phi : A \to E$ which restricts to the one above. Consider the submodule

$$M' + Am \subseteq M$$

and define

$$\begin{aligned}f : M' + Am &\to E,\\ m' + am &\mapsto \widetilde{\varphi}(m) + \Phi(a).\end{aligned}$$

To check that f is well defined, consider $m_1 + a_1 m = m_2 + a_2 m$. Then

$$(a_1 - a_2)m = m_2 - m_1$$

and so $(a_1 - a_2) \in (M' :_A m)$. Thus

$$\Phi(a_1 - a_2) = \widetilde{\varphi}((a_1 - a_2)m) = \widetilde{\varphi}(m_2 - m_1).$$

So we see that

$$\widetilde{\varphi}(m_1) + \Phi(a_1) = \widetilde{\varphi}(m_2) + \Phi(a_2).$$

Thus f is well defined and it is a lift extending φ to $M' + Am$, which contradicts the maximality of $(M', \widetilde{\varphi})$, and so we must conclude that $M' = M$. ■

Definition If A is a PID, an A-module M is **divisible** if given any $m \in M$ and nonzero $a \in A$, there exists $q \in M$ such that

$$m = a \cdot q \qquad \text{which essentially says} \qquad \frac{m}{a} = q.$$

From the above definition, we obtain the following corollary to Baer's Criterion, whose proof we will leave as an exercise to the reader.

Corollary 5.15 *Let A be a PID. An A-module is injective if and only if it is divisible.*

Example 5.16 *$\mathbb{Q}$ is an injective $\mathbb{Z}$-module as it is divisible. Moreover, $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module as well.*

Theorem 5.17 *If A is a ring, then every A-module can be embedded into an injective A-module.*

Proof Step 1. We will show that every A-module M can be embedded into a divisible $\mathbb{Z}$-module. First note that while M is an A-module, it is also a $\mathbb{Z}$-module. Hence there exists a free $\mathbb{Z}$-module Z surjecting onto M. Letting K be the kernel of this surjection, we have that

$$Z/K \cong M.$$

On the other hand, Z canonically embeds into some free $\mathbb{Q}$-module, call it Q. If we denote this canonical embedding by $\eta : Z \to Q$, and set $D = Q/\operatorname{Im}(\eta|_K)$ we may write

$$M \cong Z/K \cong \operatorname{Im}(\eta)/\operatorname{Im}(\eta|_K) \subseteq D.$$

Since D is divisible, we have completed Step 1.

Step 2. We will now embed M into $\operatorname{Hom}_{\mathbb{Z}}(A, D)$ where D is defined as in Step 1. We will denote the embedding of M into D by

$$\iota : M \hookrightarrow D.$$

Applying $\operatorname{Hom}_{\mathbb{Z}}(A, -)$, we get an injective $\mathbb{Z}$-module homomorphism

$$\begin{aligned} \iota_* : \operatorname{Hom}_{\mathbb{Z}}(A, M) &\hookrightarrow \operatorname{Hom}_{\mathbb{Z}}(A, D), \\ \varphi &\mapsto \iota \circ \varphi. \end{aligned}$$

Noting that there is a canonical injection of A-modules

$$\operatorname{Hom}_A(A, M) \hookrightarrow \operatorname{Hom}_{\mathbb{Z}}(A, M),$$

where the A-module structure on $\operatorname{Hom}_{\mathbb{Z}}(A, M)$ is given by

$$a \cdot f(x) := f(ax) \qquad \text{for } a \in A \text{ and } f \in \operatorname{Hom}_{\mathbb{Z}}(A, M),$$

we see that we have an embedding of A-modules

$$M \cong \operatorname{Hom}_A(A, M) \hookrightarrow \operatorname{Hom}_{\mathbb{Z}}(A, M) \hookrightarrow \operatorname{Hom}_{\mathbb{Z}}(A, D).$$

Step 3. We will show that if D is a divisible $\mathbb{Z}$-module, then $\operatorname{Hom}_{\mathbb{Z}}(A, D)$ is an injective A-module. Note that this step completes the proof of the theorem. Consider an ideal $\mathfrak{a}$ of A. By Baer's Criterion, Theorem 5.14, we need to show that any A-module homomorphism

$$\begin{aligned} \psi &: \mathfrak{a} \to \operatorname{Hom}_{\mathbb{Z}}(A, D), \qquad && \text{extends to} \\ \Psi &: A \to \operatorname{Hom}_{\mathbb{Z}}(A, D). \end{aligned}$$

Now consider the $\mathbb{Z}$-module homomorphism:

$$\begin{aligned} \varphi : \mathfrak{a} &\to D \\ a &\mapsto \psi(a)(1_A) \end{aligned}$$

One should check that this is indeed a $\mathbb{Z}$-module homomorphism. Since D is a divisible $\mathbb{Z}$-module, by Corollary 5.15, we see that it is an injective $\mathbb{Z}$-module, and so we write

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathfrak{a} & \xrightarrow{\iota} & A \\ & & \downarrow{\scriptstyle \varphi} & \swarrow{\scriptstyle \widetilde{\varphi}} & \\ & & D & & \end{array}$$

and obtain a $\mathbb{Z}$-module homomorphism $\widetilde{\varphi}$ such that the diagram above commutes. Now define

$$\begin{aligned} \Psi : A &\to \mathrm{Hom}_{\mathbb{Z}}(A, D), \\ a &\mapsto f, \end{aligned}$$

where $f(x) = \widetilde{\varphi}(ax)$. One should check that this defines an A-module homomorphism. For $a \in \mathfrak{a}$ and $x \in A$, we have

$$\Psi(a)(x) = f(x) = \widetilde{\varphi}(ax) = \varphi(ax) = \psi(ax)(1_A).$$

Since ψ is an A-module homomorphism, we have

$$\psi(ax)(1_A) = x\psi(a)(1_A) = \psi(a)(x),$$

where the right-most equality is due to the A-module structure on $\mathrm{Hom}_{\mathbb{Z}}(A, D)$. Hence we have $\Psi : A \to \mathrm{Hom}_{\mathbb{Z}}(A, D)$ and $\Psi|_{\mathfrak{a}} = \psi$. Thus we see $\mathrm{Hom}_{\mathbb{Z}}(A, D)$ is an injective A-module. ■

Definition If M is an A-module, an **injective resolution** of M is a cocomplex of injective modules $E^\bullet$ and a map $\iota : M \to E_0$ such that

$$0 \longrightarrow M \xrightarrow{\iota} E^0 \xrightarrow{d^0} E^1 \xrightarrow{d^1} E^2 \longrightarrow \cdots$$

is exact.

If A is a ring and M is an A-module, we can use Theorem 5.17 to construct an injective resolution as follows. Set

$$\begin{aligned} E^0 &:= \{\text{a module which } M \text{ embeds into}\}, \\ C^1 &:= \mathrm{Coker}(M \hookrightarrow E^0), \end{aligned}$$

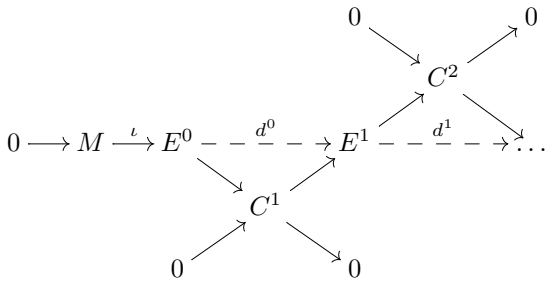
and inductively define

$$\begin{aligned} E^i &:= \{\text{a module which } C^i \text{ embeds into}\}, \\ C^{i+1} &:= \mathrm{Coker}(C^i \hookrightarrow E^i). \end{aligned}$$

Now we may inductively write the exact sequences:

$$\begin{aligned} 0 \to M \to E^0 \to C^1 \to 0, \\ 0 \to C^i \to E^i \to C^{i+1} \to 0. \end{aligned}$$

Putting the above exact sequences together we obtain:



The d^i's above are formed by taking the composition of the relevant maps, while ι is the canonical injection. Hence we obtain an injective resolution of M.

We now include the corresponding results for injective resolutions that we had for projective resolutions. The statements and proofs are precisely the duals of the projective case.

Lemma 5.18 *Let $f : M \to N$ be a homomorphism of A-modules. If $I^\bullet$ is a cocomplex of injective A-modules such that $H^0(I^\bullet) = M$ and $J^\bullet$ is an exact cocomplex with $H^0(J^\bullet) = N$, then there exists a map of cocomplexes $f^\bullet : I^\bullet \to J^\bullet$ lifting f.*

Lemma 5.19 (Horseshoe Lemma) *Let*

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

is an exact sequence of A-modules, and $M_1 \to I_1^\bullet$ and $M_3 \to I_3^\bullet$ be injective resolutions. Then, there exists an injective resolution $M_2 \to I_2^\bullet$ such that the rows in the diagram below are exact:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I_1^\bullet & \longrightarrow & I_2^\bullet & \longrightarrow & I_3^\bullet & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \end{array}$$

Exercise 5.20 *Show that given the following commutative diagram of A-modules with exact rows:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & 0 \end{array}$$

Then there exist associated injective resolutions that form a commutative dia-

gram of A-complexes with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I_1^\bullet & \longrightarrow & I_2^\bullet & \longrightarrow & I_3^\bullet & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & J_1^\bullet & \longrightarrow & J_2^\bullet & \longrightarrow & J_3^\bullet & \longrightarrow & 0 \end{array}$$

Exercise 5.21 *Consider the short exact sequence:*

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0.$$

Note that this is an injective resolution of $\mathbb{Z}$. Is $\mathbb{Q}/\mathbb{Z}$ indecomposable? That is, is $\mathbb{Q}/\mathbb{Z}$ a direct sum of $\mathbb{Z}$-modules? If so, what are the summands? If not, why not?

5.2 Tor and Ext

5.2.1 Tor

Construction of Tor

Definition Given a ring A and an A-module N, $\mathbf{Tor_i^A(-, N)}$ is the left derived functor of the right exact covariant functor $- \otimes_A N$.

To be more explicit, consider **any** projective resolution of an A-module M:

$$\cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0$$

Apply the functor $- \otimes_A N$ to get the complex $P_\bullet \otimes_A N$:

$$\cdots \to P_2 \otimes_A N \to P_1 \otimes_A N \to P_0 \otimes_A N \to 0$$

We now define

$$\mathrm{Tor}_i^A(M, N) := H_i(P_\bullet \otimes_A N) = \frac{\mathrm{Ker}(d_i \otimes 1)}{\mathrm{Im}(d_{i+1} \otimes 1)}$$

Note that since

$$P_1 \to P_0 \to M \to 0$$

is exact,

$$P_1 \otimes_A N \to P_0 \otimes_A N \to M \otimes_A N \to 0$$

is also exact. Hence

$$\mathrm{Tor}_0^A(M, N) \cong M \otimes_A N.$$

Proposition 5.22 *$\mathrm{Tor}_i^A(M, N)$ does not depend on the choice of projective resolution used. Hence it is well-defined.*

Proof Let $P_\bullet$ and $Q_\bullet$ be two projective resolutions of M. So we may write:

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & P_i & \longrightarrow & \cdots & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \varphi_i} & & & & \downarrow{\scriptstyle \varphi_0} & & \downarrow{\scriptstyle \mathbb{1}_M} & & \\
\cdots & \longrightarrow & Q_i & \longrightarrow & \cdots & \longrightarrow & Q_0 & \longrightarrow & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \psi_i} & & & & \downarrow{\scriptstyle \psi_0} & & \downarrow{\scriptstyle \mathbb{1}_M} & & \\
\cdots & \longrightarrow & P_i & \longrightarrow & \cdots & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0
\end{array}$$

Note that the lifts $\varphi_\bullet$ and $\psi_\bullet$ of $\mathbb{1}_M$ are guaranteed to exist by Lemma 5.9. Thus $\psi_\bullet \circ \varphi_\bullet : P_\bullet \to P_\bullet$ is a lift of $\mathbb{1}_M$. But clearly $\mathbb{1}_{P_\bullet}$ is another such lift. Thus $\psi_\bullet \circ \varphi_\bullet \sim \mathbb{1}_{P_\bullet}$. Similarly, $\varphi_\bullet \circ \psi_\bullet \sim \mathbb{1}_{Q_\bullet}$. Applying $- \otimes_A N$ to everything we obtain that

$$(\psi_\bullet \circ \varphi_\bullet) \otimes (\mathbb{1}_N) \sim (\mathbb{1}_{P_\bullet}) \otimes (\mathbb{1}_N) \qquad \text{and} \qquad (\varphi_\bullet \circ \psi_\bullet) \otimes (\mathbb{1}_N) \sim (\mathbb{1}_{Q_\bullet}) \otimes (\mathbb{1}_N)$$

and so

$$H_i(P_\bullet \otimes_A N) \cong H_i(Q_\bullet \otimes_A N).$$

Thus $\operatorname{Tor}_i^A(M, N)$ is well-defined. ■

Properties of Tor

Exercise 5.23 *If N is A-flat or if M is A-flat, show that*

$$\operatorname{Tor}_i^A(M, N) = 0$$

for all A-modules M and $i > 0$. Hint: For the second part, first show that if

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

is exact and M_2 and M_3 are flat, so is M_1.

Proposition 5.24 *Given an exact sequence of A-modules,*

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

we obtain a long exact sequence of Tor*:*

$$\begin{array}{l}
\cdots \longrightarrow \operatorname{Tor}_{n+1}^A(M', N) \longrightarrow \operatorname{Tor}_{n+1}^A(M, N) \longrightarrow \operatorname{Tor}_{n+1}^A(M'', N) \xrightarrow{\partial_{n+1}} \\
\longrightarrow \operatorname{Tor}_n^A(M', N) \longrightarrow \operatorname{Tor}_n^A(M, N) \longrightarrow \operatorname{Tor}_n^A(M'', N) \xrightarrow{\partial_n} \\
\longrightarrow \operatorname{Tor}_{n-1}^A(M', N) \longrightarrow \cdots\cdots\cdots\cdots \longrightarrow \operatorname{Tor}_1^A(M'', N) \xrightarrow{\partial_1} \\
\longrightarrow M' \otimes_A N \longrightarrow M \otimes_A N \longrightarrow M'' \otimes_A N \longrightarrow 0
\end{array}$$

Proof Let $P'_\bullet$ and $P''_\bullet$ be projective resolutions of M' and M'' respectively. By the Horseshoe Lemma there exists a projective resolution $P'_\bullet$ of M such that

$$0 \to P'_\bullet \to P_\bullet \to P''_\bullet \to 0$$

is an exact sequence of complexes. Since $P''_\bullet$ is projective, we have following short exact sequence of complexes:

$$0 \to P'_\bullet \otimes_A N \to P_\bullet \otimes_A N \to P''_\bullet \otimes_A N \to 0$$

By Lemma 5.3, we obtain a long exact sequence of homologies, and hence the result. ■

Proposition 5.25 *Given an exact sequence of A-modules,*

$$0 \to N' \to N \to N'' \to 0$$

we obtain a long exact sequence of Tor*:*

$$\cdots \longrightarrow \mathrm{Tor}^A_{n+1}(M,N') \longrightarrow \mathrm{Tor}^A_{n+1}(M,N) \longrightarrow \mathrm{Tor}^A_{n+1}(M,N'') \xrightarrow{\partial_{n+1}}$$
$$\mathrm{Tor}^A_n(M,N') \longrightarrow \mathrm{Tor}^A_n(M,N) \longrightarrow \mathrm{Tor}^A_n(M,N'') \xrightarrow{\partial_n}$$
$$\mathrm{Tor}^A_{n-1}(M,N') \longrightarrow \cdots\cdots\cdots\cdots \longrightarrow \mathrm{Tor}^A_1(M,N'') \xrightarrow{\partial_1}$$
$$M \otimes_A N' \longrightarrow M \otimes_A N \longrightarrow M \otimes_A N'' \longrightarrow 0$$

Proof Let $Q_\bullet$ be a projective resolutions of M. Since projective modules are flat, applying successively $N' \otimes_A -$, $N \otimes_A -$ and $N'' \otimes_A -$, we get a short exact sequence of complexes:

$$0 \to Q_\bullet \otimes_A N' \to Q_\bullet \otimes_A N \to Q_\bullet \times_A N'' \to 0$$

By Lemma 5.3, we obtain a long exact sequence of homologies, and hence the result. ■

One may also define $\mathrm{Tor}^A_i(M,N)$ as the left derived functor of $M \otimes_A -$. We leave it as an exercise to show that this definition does not depend on the choice of projective resolution of N and that there are corresponding long exact sequences as well. Let us temporarily set $\underline{\mathrm{Tor}}^A_i(M,N) = H_i(M \otimes_A P_\bullet)$, where $P_\bullet$ is a projective resolution of N.

Theorem 5.26 (Balancing of Tor) *Let M, N be A-modules. Then*

$$\mathrm{Tor}^A_i(M,N) \cong \underline{\mathrm{Tor}}^A_i(M,N)$$

for all $i \geq 0$.

Proof We proceed by induction on i. When $i = 0$, the right exactness of both $M \otimes_A -$ and $- \otimes_A N$ show that $\mathrm{Tor}_0^A(M,N) \cong M \otimes_A N \cong \underline{\mathrm{Tor}}_0^A(M,N)$.

Assume the result for all M and N and for $i < n$. Take a short exact sequence of the form

$$0 \to K \to F \to M \to 0,$$

where F is free. Since all free modules are projective, $\mathrm{Tor}_i^A(F,N) = 0$ for $i > 0$. If $n = 1$, we have exact sequences of the form

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Tor}_1^A(M,N) & \longrightarrow & K \otimes_A N & \longrightarrow & F \otimes_A N & \longrightarrow & M \otimes_A N & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow \cong & & \downarrow \cong & & \downarrow \cong & & \\
0 & \longrightarrow & \underline{\mathrm{Tor}}_1^A(M,N) & \longrightarrow & K \otimes_A N & \longrightarrow & F \otimes_A N & \longrightarrow & M \otimes_A N & \longrightarrow & 0
\end{array}$$

It follows that $\mathrm{Tor}_1^A(M,N) \cong \underline{\mathrm{Tor}}_1^A(M,N)$. If $n > 1$, we have exact sequences of the form

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Tor}_n^A(M,N) & \longrightarrow & \mathrm{Tor}_{n-1}^A(K,N) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow \cong & & \\
0 & \longrightarrow & \underline{\mathrm{Tor}}_n^A(M,N) & \longrightarrow & \underline{\mathrm{Tor}}_{n-1}^A(K,N) & \longrightarrow & 0
\end{array}$$

from which the claimed isomorphism follows. ■

The symmetry of tensor product leads to the following isomorphism.

Proposition 5.27 *Given a ring A and two A-modules M and N, we then have*

$$\mathrm{Tor}_i^A(M,N) \cong \mathrm{Tor}_i^A(N,M).$$

Proof First note that

$$\mathrm{Tor}_0^A(M,N) \cong M \otimes_A N \qquad \text{and} \qquad \mathrm{Tor}_0^A(N,M) \cong N \otimes_A M.$$

Since

$$\begin{gathered} M \otimes_A N \cong N \otimes_A M \\ m \otimes n \mapsto n \otimes m \end{gathered}$$

we have that $\mathrm{Tor}_0^A(M,N) \cong \mathrm{Tor}_0^A(N,M)$. Consider

$$0 \to S \to P \to M \to 0$$

where P is a free module and S is the kernel of the surjection. Note that since P is a free module, it is flat, and so

$$\begin{aligned} \mathrm{Tor}_i^A(P,N) &= 0 && \text{for } i > 0 \text{ and} \\ \mathrm{Tor}_i^A(N,P) &= 0 && \text{for } i > 0. \end{aligned}$$

Hence by Proposition 5.25 we now have two long exact sequences of Tor's:

$$\cdots \longrightarrow \operatorname{Tor}_{i+1}^A(S,N) \longrightarrow 0 \longrightarrow \operatorname{Tor}_{i+1}^A(M,N) \xrightarrow{\partial_{i+1}} \operatorname{Tor}_i^A(S,N) \longrightarrow 0 \longrightarrow \operatorname{Tor}_i^A(M,N) \xrightarrow{\partial_i} \operatorname{Tor}_{i-1}^A(S,N) \longrightarrow 0 \longrightarrow \operatorname{Tor}_{i-1}^A(M,N) \longrightarrow \cdots$$

And:

$$\cdots \longrightarrow \operatorname{Tor}_{i+1}^A(N,S) \longrightarrow 0 \longrightarrow \operatorname{Tor}_{i+1}^A(N,M) \xrightarrow{\partial_{i+1}} \operatorname{Tor}_i^A(N,S) \longrightarrow 0 \longrightarrow \operatorname{Tor}_i^A(N,M) \xrightarrow{\partial_i} \operatorname{Tor}_{i-1}^A(N,S) \longrightarrow 0 \longrightarrow \operatorname{Tor}_{i-1}^A(N,M) \longrightarrow \cdots$$

Thus we see that

$$\begin{aligned} \operatorname{Tor}_i^A(M,N) &\cong \operatorname{Tor}_{i-1}^A(S,N) && \text{if } i > 1, \\ \operatorname{Tor}_i^A(N,M) &\cong \operatorname{Tor}_{i-1}^A(N,S) && \text{if } i > 1. \end{aligned}$$

We see now that it is enough to show that $\operatorname{Tor}_1^A(M,N) \cong \operatorname{Tor}_1^A(N,M)$. Consider the commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{Tor}_1^A(M,N) & \longrightarrow & S \otimes_A N & \longrightarrow & P \otimes_A N & \longrightarrow & M \otimes_A N & \longrightarrow & 0 \\ & & & & \| & & \| & & \| & & \\ 0 & \longrightarrow & \operatorname{Tor}_1^A(N,M) & \longrightarrow & N \otimes_A S & \longrightarrow & N \otimes_A P & \longrightarrow & N \otimes_A M & \longrightarrow & 0 \end{array}$$

Note that the left-most terms are 0 because M and N are projective. And so we see that $\operatorname{Tor}_1^A(M,N) \cong \operatorname{Tor}_1^A(N,M)$. ■

Exercise 5.28 $\operatorname{Tor}_i(M, \bigoplus_\alpha N_\alpha) \cong \bigoplus_\alpha \operatorname{Tor}_i(M, N_\alpha)$.

Exercise 5.29 *Let B be a flat A-algebra. Then*

$$B \otimes_A \operatorname{Tor}_i^A(M,N) \cong \operatorname{Tor}_i^B(M \otimes_A B, N \otimes_A B).$$

In particular, if U is a multiplicatively closed set in A, then

$$U^{-1} \operatorname{Tor}_i^A(M,N) \cong \operatorname{Tor}_i^{U^{-1}}(U^{-1}M, U^{-1}N).$$

5.2.2 Ext

First Construction

Definition Given a ring A and an A-module N, $\mathbf{Ext}^{\boldsymbol{i}}_{\boldsymbol{A}}\boldsymbol{(-,N)}$ is the left derived functor of the left exact contravariant functor $\mathrm{Hom}_A(-,N)$.

To be more explicit, consider **any** projective resolution of an A-module M:

$$\cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0$$

Apply the functor $\mathrm{Hom}_A(-,N)$ to get the complex $\mathrm{Hom}_A(P_\bullet, N)$:

$$0 \xrightarrow{d_0^*} \mathrm{Hom}_A(P_0,N) \xrightarrow{d_1^*} \mathrm{Hom}_A(P_1,N) \xrightarrow{d_2^*} \mathrm{Hom}_A(P_2,N) \longrightarrow \cdots$$

where $d_0^* := 0$. We now define:

$$\mathrm{Ext}^i_A(M,N) := H^i(\mathrm{Hom}_A(P_\bullet,N)) = \frac{\mathrm{Ker}(d_{i+1}^*)}{\mathrm{Im}(d_i^*)}$$

The shift in degrees of the differentials in the quotient above, compared to the definition of cohomology, is due to the fact that d_i^* is the $(i-1)$th differential in the cocomplex $\mathrm{Hom}_A(P_\bullet, N)$. Since

$$P_1 \to P_0 \to M \to 0$$

is exact,

$$0 \longrightarrow \mathrm{Hom}_A(M,N) \longrightarrow \mathrm{Hom}_A(P_0,N) \xrightarrow{d_1^*} \mathrm{Hom}_A(P_1,N)$$

is also exact. Hence

$$\mathrm{Ext}^0_A(M,N) = \frac{\mathrm{Ker}(d_1^*)}{0} \cong \mathrm{Hom}_A(M,N).$$

Proposition 5.30 *$\mathrm{Ext}^i_A(M,N)$ does not depend on the choice of projective resolution of M used to compute it. Hence it is well-defined.*

Proof Let $P_\bullet$ and $Q_\bullet$ be two projective resolutions of M. We can lift $\mathbb{1}_M$ to maps of complex $\varphi_\bullet$ and $\psi_\bullet$ and write:

$$\begin{array}{ccccccccc}
\cdots \longrightarrow & P_i & \longrightarrow \cdots \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0 \\
& \downarrow{\scriptstyle \varphi_i} & & \downarrow{\scriptstyle \varphi_0} & & \downarrow{\scriptstyle \mathbb{1}_M} & & \\
\cdots \longrightarrow & Q_i & \longrightarrow \cdots \longrightarrow & Q_0 & \longrightarrow & M & \longrightarrow & 0 \\
& \downarrow{\scriptstyle \psi_i} & & \downarrow{\scriptstyle \psi_0} & & \downarrow{\scriptstyle \mathbb{1}_M} & & \\
\cdots \longrightarrow & P_i & \longrightarrow \cdots \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0
\end{array}$$

Since $\mathbb{1}_{P_\bullet}$ and $\psi_\bullet \circ \varphi_\bullet$ are both lifts of $\mathbb{1}_M$, we have $\psi_\bullet \circ \varphi_\bullet \sim (\mathbb{1}_{P_\bullet})$. Similarly, $\varphi_\bullet \circ \psi_\bullet \sim (\mathbb{1}_{Q_\bullet})$. Applying $(-)^* = \mathrm{Hom}_A(-, N)$ to everything we obtain that

$$(\psi_\bullet \circ \varphi_\bullet)^* \sim (\mathbb{1}_{P_\bullet})^* \qquad \text{and} \qquad (\varphi_\bullet \circ \psi_\bullet)^* \sim (\mathbb{1}_{Q_\bullet})^*$$

and so

$$H^i(\mathrm{Hom}_A(P_\bullet, N)) \cong H^i(\mathrm{Hom}_A(Q_\bullet, N)).$$

Thus $\mathrm{Ext}^A_i(M, N)$ is well-defined. ■

Second Construction

Definition Given a ring A and an A-module N, $\mathbf{Ext}^{\boldsymbol{i}}_{\boldsymbol{A}}\boldsymbol{(M, -)}$ is the left derived functor of the left exact covariant functor $\mathrm{Hom}_A(M, -)$.

To be more explicit, consider **any** injective resolution of an A-module N:

$$0 \longrightarrow N \xrightarrow{\iota} E^0 \xrightarrow{d^0} E^1 \xrightarrow{d^1} E^2 \longrightarrow \cdots$$

Apply the functor $\mathrm{Hom}_A(M, -)$ and chop off the $\mathrm{Hom}_A(M, N)$ term to get the complex $\mathrm{Hom}_A(M, E^\bullet)$:

$$0 \xrightarrow{d^{-1}_*} \mathrm{Hom}_A(M, E^0) \xrightarrow{d^0_*} \mathrm{Hom}_A(M, E^1) \xrightarrow{d^1_*} \mathrm{Hom}_A(M, E^2) \longrightarrow \cdots$$

where $d^{-1}_* := 0$. We now define:

$$\mathrm{Ext}^i_A(M, N) := H^i(\mathrm{Hom}_A(M, E^\bullet)) = \frac{\mathrm{Ker}(d^i_*)}{\mathrm{Im}(d^{i-1}_*)}$$

Note that since

$$0 \to N \to E^0 \to E^1$$

is exact,

$$0 \longrightarrow \mathrm{Hom}_A(M, N) \longrightarrow \mathrm{Hom}_A(M, E^0) \xrightarrow{d^0_*} \mathrm{Hom}_A(M, E^1)$$

is also exact. Hence

$$\mathrm{Ext}^0_A(M, N) = \frac{\mathrm{Ker}(d^0_*)}{0} \cong \mathrm{Hom}_A(M, N).$$

Proposition 5.31 *$\mathrm{Ext}^i_A(M, N)$ does not depend on the choice of injective resolution of N used to compute it. Hence it is well-defined.*

Proof Let $I^\bullet$ and $J^\bullet$ be two injective resolutions of N. So we may write:

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & N & \longrightarrow & I^0 & \longrightarrow & \cdots & \longrightarrow & I^i & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle \mathbb{1}_N} & & \downarrow{\scriptstyle \varphi^0} & & & & \downarrow{\scriptstyle \varphi^i} & & \\
0 & \longrightarrow & N & \longrightarrow & J^0 & \longrightarrow & \cdots & \longrightarrow & J^i & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle \mathbb{1}_N} & & \downarrow{\scriptstyle \psi^0} & & & & \downarrow{\scriptstyle \psi^i} & & \\
0 & \longrightarrow & N & \longrightarrow & I^0 & \longrightarrow & \cdots & \longrightarrow & I^i & \longrightarrow & \cdots
\end{array}$$

Thus we see that $\psi^\bullet \circ \varphi^\bullet \sim (\mathbb{1}_{I^\bullet})$. Similarly, $\varphi^\bullet \circ \psi^\bullet \sim (\mathbb{1}_{J^\bullet})$. Applying $(-)^* = \mathrm{Hom}_A(M, -)$ to everything we obtain that

$$(\psi^\bullet \circ \varphi^\bullet)^* \sim (\mathbb{1}_{I^\bullet})^* \qquad \text{and} \qquad (\varphi^\bullet \circ \psi^\bullet)^* \sim (\mathbb{1}_{J^\bullet})^*$$

and so

$$H^i(\mathrm{Hom}_A(M, I^\bullet)) \cong H^i(\mathrm{Hom}_A(M, J^\bullet)).$$

Thus $\mathrm{Ext}^A_i(M, N)$ is well-defined. ■

Properties of Ext

Proposition 5.32 *The two constructions of* $\mathrm{Ext}^i_A(M, N)$ *given above produce isomorphic modules and hence are equivalent.*

Proof We omit the proof of this result, though it is similar to the proof that the two definitions of Tor are the same. Readers who are familiar with spectral sequences can see the result easily by taking a projective resolution $P_\bullet \to M$ of M and an injective resolution $N \to I^\bullet$ and considering the double complex $\mathrm{Hom}_A(P_\bullet, I^\bullet)$. ■

Proposition 5.33 *Given an exact sequence of A-modules,*

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

we obtain a long exact sequence of Ext*'s:*

$$\begin{array}{l}
0 \longrightarrow \mathrm{Hom}_A(M'', N) \longrightarrow \mathrm{Hom}_A(M, N) \longrightarrow \mathrm{Hom}_A(M', N) \xrightarrow{\partial_1} \\
\quad \longrightarrow \mathrm{Ext}^1_A(M'', N) \longrightarrow \cdots\cdots\cdots\cdots \longrightarrow \mathrm{Ext}^{n-1}_A(M', N) \xrightarrow{\partial_{n-1}} \\
\quad \longrightarrow \mathrm{Ext}^n_A(M'', N) \longrightarrow \mathrm{Ext}^n_A(M, N) \longrightarrow \mathrm{Ext}^n_A(M', N) \xrightarrow{\partial_n} \\
\quad \longrightarrow \mathrm{Ext}^{n+1}_A(M'', N) \longrightarrow \mathrm{Ext}^{n+1}_A(M, N) \longrightarrow \mathrm{Ext}^{n+1}_A(M', N) \longrightarrow \cdots
\end{array}$$

Proof By the Horseshoe Lemma, there are projective resolutions $P'_\bullet$, $P_\bullet$, and $P''_\bullet$ of M', M, and M'' respectively, yielding a short exact sequence of complexes:

$$0 \to P'_\bullet \to P_\bullet \to P''_\bullet \to 0$$

Since $P''_\bullet$ is projective, we have following short exact sequence of complexes:

$$0 \to \mathrm{Hom}_A(P''_\bullet, N) \to \mathrm{Hom}_A(P_\bullet, N) \to \mathrm{Hom}_A(P'_\bullet, N) \to 0$$

By Lemma 5.3, we obtain a long exact sequence of homologies, and hence the result. ■

Proposition 5.34 *Given an exact sequence of A-modules,*

$$0 \to N' \to N \to N'' \to 0$$

we obtain a long exact sequence of Ext*'s:*

$$\cdots \longrightarrow \mathrm{Ext}_A^{n-1}(M,N') \longrightarrow \mathrm{Ext}_A^{n-1}(M,N) \longrightarrow \mathrm{Ext}_A^{n-1}(M,N'') \xrightarrow{\partial_{n-1}}$$
$$\mathrm{Ext}_A^{n}(M,N') \longrightarrow \mathrm{Ext}_A^{n}(M,N) \longrightarrow \mathrm{Ext}_A^{n}(M,N'') \xrightarrow{\partial_{n}}$$
$$\mathrm{Ext}_A^{n+1}(M,N') \longrightarrow \mathrm{Ext}_A^{n+1}(M,N) \longrightarrow \mathrm{Ext}_A^{n+1}(M,N'') \longrightarrow \cdots$$

Proof Note, one could dualize the above proof or one could take a projective resolution $P_\bullet$ of M and look at the short exact sequence of complexes:

$$0 \to \mathrm{Hom}_A(P_\bullet, N') \to \mathrm{Hom}_A(P_\bullet, N) \to \mathrm{Hom}_A(P_\bullet, N'') \to 0$$

By Lemma 5.3, we obtain a long exact sequence of homologies, and hence the result. ■

Proposition 5.35 *If A is a ring, the following are equivalent:*

(1) *M is projective.*

(2) *$\mathrm{Ext}_A^i(M,N) = 0$ for all A-modules N and for all $i > 0$.*

(3) *$\mathrm{Ext}_A^1(M,N) = 0$ for all A-modules N.*

Proof All that needs to be shown is (3) $\Rightarrow$ (1). We must show that given any short exact sequence

$$0 \to N' \to N \to N'' \to 0$$

of A modules, we have

$$\mathrm{Hom}_A(M,N) \twoheadrightarrow \mathrm{Hom}_A(M,N'').$$

But by the long exact sequence of Ext and the fact that $\mathrm{Ext}_A^1(M,N) = 0$ for all A-modules N, we have

$$0 \to \mathrm{Hom}_A(M,N') \to \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(M,N'') \to 0$$

is exact, which shows M is projective. ■

Proposition 5.36 *If A is a ring, the following are equivalent:*

(1) *N is injective.*

(2) $\operatorname{Ext}^i_A(M,N) = 0$ *for all* A*-modules* M *and for all* $i > 0$.

(3) $\operatorname{Ext}^1_A(M,N) = 0$ *for all* A*-modules* M.

(4) $\operatorname{Ext}^1_A(M,N) = 0$ *for all finitely generated* A*-modules* M.

(5) $\operatorname{Ext}^1_A(A/I,N) = 0$ *for all ideals* $I \subseteq A$.

Proof All that needs to be shown is (5) $\Rightarrow$ (1). By Baer's Criterion, Theorem 5.14, we must show that given any ideal I of A, a module homomorphism $\varphi : I \to N$ can be extended to a module homomorphism $\Phi : A \to N$. This amounts to saying that

$$\operatorname{Hom}_A(A,N) \twoheadrightarrow \operatorname{Hom}_A(I,N).$$

Write

$$0 \to I \to A \to A/I \to 0$$

and apply the functor $\operatorname{Hom}_A(-,N)$, and note that $\operatorname{Ext}^1_A(A/I,N) = 0$ for all ideals $I \subseteq A$, to obtain the exact sequence

$$0 \to \operatorname{Hom}_A(A/I,N) \to \operatorname{Hom}_A(A,N) \to \operatorname{Hom}_A(I,N) \to 0$$

Hence N must be injective. ■

Exercise 5.37

(1) $\operatorname{Ext}^i_A(\bigoplus_\alpha M_\alpha, N) \cong \prod_\alpha \operatorname{Ext}^i_A(M_\alpha, N)$.

(2) $\operatorname{Ext}^i_A(M, \prod_\alpha N_\alpha) \cong \prod_\alpha \operatorname{Ext}^i_A(M, N_\alpha)$.

In particular, finite direct sums in either variable pass through Ext.

Exercise 5.38 *Let* B *be an* A*-algebra that is finitely generated and projective as an* A*-module or let* B *be a flat* A*-algebra where* A *is Noetherian and* M *is finitely generated. Then*

$$B \otimes_A \operatorname{Ext}^i_A(M,N) \cong \operatorname{Ext}^i_B(M \otimes_A B, N \otimes_A B).$$

If U *is a multiplicatively closed set in* A, A *is Noetherian and* M *is finitely generated, then*

$$U^{-1} \operatorname{Ext}^i_A(M,N) \cong \operatorname{Ext}^i_{U^{-1}A}(U^{-1}M, U^{-1}N).$$

5.3 Homological Notions of Dimension

5.3.1 Projective Dimension

Definition Given a ring A and an A-module M, the **projective dimension** of M is defined to be:

$$\operatorname{pd}_A(M) := \inf\{n : \text{there exists a projective resolution of } M \text{ of length } n\}.$$

Recall that

$$0 \to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to M \to 0$$

is a resolution of length n if it is an exact complex and each P_i is projective.

Remark Sometimes projective dimension is called **homological dimension**.

Proposition 5.39 *If A is a ring and M is an A-module, then the following are equivalent:*

(1) $\mathrm{pd}_A(M) \leq n$.

(2) $\mathrm{Ext}^i_A(M, N) = 0$ *for all A-modules N and for all $i > n$.*

(3) $\mathrm{Ext}^{n+1}_A(M, N) = 0$ *for all A-modules N.*

Proof All that needs to be shown is (3) $\Rightarrow$ (1). Write

$$P_\bullet : \qquad 0 \to S_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to M \to 0$$

where S_n is the kernel of d_{n-1}. We'll show that S_n is projective. By Proposition 5.35, we need only show that $\mathrm{Ext}^1_A(S_n, N) = 0$ for all A-module N. Break up $P_\bullet$ into short exact sequences as follows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & S_n & \longrightarrow & P_{n-1} & \longrightarrow & S_{n-1} & \longrightarrow & 0 \\
0 & \longrightarrow & S_{n-1} & \longrightarrow & P_{n-2} & \longrightarrow & S_{n-2} & \longrightarrow & 0 \\
 & & \vdots & & \vdots & & \vdots & & \\
0 & \longrightarrow & S_1 & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0
\end{array}$$

Apply $\mathrm{Hom}_A(-, N)$ and from the corresponding long exact sequences for Ext we see

$$\mathrm{Ext}^1_A(S_n, N) \cong \mathrm{Ext}^2_A(S_{n-1}, N) \cong \cdots \cong \mathrm{Ext}^n_A(S_1, N) \cong \mathrm{Ext}^{n+1}_A(M, N) = 0.$$

Hence we see that S_n is projective. ■

As immediate corollaries to this proposition we have two more characterizations of projective dimension:

Corollary 5.40 *If A is a ring and M is an A-module, then:*

$$\mathrm{pd}_A(M) := \inf \left\{ n : \begin{array}{l} \textit{Given any projective resolution } (P_\bullet, d_\bullet) \textit{ of } M, \\ \mathrm{Ker}(d_{n-1}) \textit{ is projective} \end{array} \right\}$$

Corollary 5.41 *If A is a ring and M is an A-module, then*

$$\mathrm{pd}_A(M) = \sup_N \{ n : \mathrm{Ext}^n_A(M, N) \neq 0 \},$$

where N varies over all A-modules.

Example 5.42 *For arbitrary modules, projective dimension is not always finite. Consider the local ring* $A = k[\![x, y]\!]/(x^2)$ *and the* A*-module* $M = A/(x)$*, where* k *is a field. Then*

$$P_\bullet : \quad \cdots \to A \xrightarrow{x} A \xrightarrow{x} A \xrightarrow{x} A$$

is a projective resolution of M*. If apply* $\mathrm{Hom}_A(-, M)$*, then all the differential maps become* 0 *(since* $x \in \mathrm{Ann}_A(M)$*) and so* $\mathrm{Ext}^i_A(M, M) \cong M$ *for all* $i \geq 0$*. By the previous proposition,* $\mathrm{pd}_A(M) = \infty$*.*

On the other hand, the A*-module* $N = A/(y)$ *has the following finite free resolution*

$$0 \to A \xrightarrow{y} A$$

and so $\mathrm{pd}_A(N) \leq 1$*. A similar argument shows that in fact* $\mathrm{pd}_A(N) = 1$*.*

Exercise 5.43 *If* $A \to B$ *is a ring homomorphism and* P *is a projective* A*-module, then* $P \otimes_A B$ *is a projective* B*-module.*

Proposition 5.44 *Given an* A*-module* M*, suppose that* $x \in A$ *is a nonzerodivisor on both* A *and* M*. If* $\mathrm{pd}_A(M) < \infty$*, then* $\mathrm{pd}_{A/xA}(M/xM) < \infty$*.*

Proof Consider the following projective resolution of M

$$P_\bullet : \qquad 0 \to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0$$

We would be done if we knew that

$$0 \to P_n/xP_n \to \cdots \to P_0/xP_0 \to M/xM \to 0$$

was exact; this follows from the above exercise. But we can also prove this directly.

Now note that

$$H_i(P_\bullet \otimes_A A/xA) = \mathrm{Tor}^A_i(M, A/xA).$$

Since

$$0 \longrightarrow A \xrightarrow{x} A \longrightarrow A/xA \longrightarrow 0 \qquad (\bigstar)$$

is a free resolution of A/xA, we see that

$$\mathrm{Tor}^A_i(M, A/xA) = 0 \qquad \text{for } i \geq 2.$$

We must show that $\mathrm{Tor}^A_1(M, A/xA) = 0$. Applying $- \otimes_A M$ to $(\bigstar)$ above we obtain the exact sequence

$$0 \longrightarrow \mathrm{Tor}^A_1(M, A/xA) \longrightarrow M \xrightarrow{x} M \longrightarrow M/xM \longrightarrow 0.$$

But we see that $\mathrm{Tor}^A_1(M, A/xA) = 0$ as the above complex is exact and multiplication by x is injective. Thus $P_\bullet \otimes_A A/xA$ is a projective resolution of M/xM. ■

Proposition 5.45 *Let $0 \to M \to N \to T \to 0$ be an exact sequence of A-modules. Then*

(1) $\mathrm{pd}_A(N) \leq \max\{\mathrm{pd}_A(M), \mathrm{pd}_A(T)\}$

(2) $\mathrm{pd}_A(M) \leq \max\{\mathrm{pd}_A(N), \mathrm{pd}_A(T) - 1\}$

(3) $\mathrm{pd}_A(T) \leq \max\{\mathrm{pd}_A(N), \mathrm{pd}_A(M) + 1\}$

Proof This follows easily from the long exact sequence of Tor. ■

Exercise 5.46 *With notation in the previous proposition, show that*

(1) *If* $\mathrm{pd}_A(M) > \mathrm{pd}_A(N)$, *then* $\mathrm{pd}_A(T) = \mathrm{pd}_A(M) + 1$.

(2) *If* $\mathrm{pd}_A(M) < \mathrm{pd}_A(N)$, *then* $\mathrm{pd}_A(T) = \mathrm{pd}_A(N)$.

(3) *If* $\mathrm{pd}_A(N) > \mathrm{pd}_A(T)$, *then* $\mathrm{pd}_A(M) = \mathrm{pd}_A(N)$.

(4) *If* $\mathrm{pd}_A(N) < \mathrm{pd}_A(T)$, *then* $\mathrm{pd}_A(M) = \mathrm{pd}_A(T) - 1$.

(5) *If* $\mathrm{pd}_A(M) > \mathrm{pd}_A(T) - 1$, *then* $\mathrm{pd}_A(N) = \mathrm{pd}_A(M)$.

(6) *If* $\mathrm{pd}_A(M) < \mathrm{pd}_A(T) - 1$, *then* $\mathrm{pd}_A(N) = \mathrm{pd}_A(T)$.

5.3.2 Injective Dimension

Definition Given a ring A and an A-module M, the **injective dimension** of M is defined to be:

$$\mathrm{id}_A(M) := \inf\{n : \text{there exists an injective resolution of } M \text{ of length } n\}.$$

Recall that

$$0 \to M \to E^0 \to E^1 \to \cdots \to E^{n-1} \to E^n \to 0$$

is a resolution of length n if it is an exact cocomplex and each E^i is injective.

Proposition 5.47 *If A is a ring and N is an A-module, then the following are equivalent:*

(1) $\mathrm{id}_A(N) \leq n$.

(2) $\mathrm{Ext}^i_A(M, N) = 0$ *for all A-modules M and for all $i > n$.*

(3) $\mathrm{Ext}^{n+1}_A(M, N) = 0$ *for all A-modules M.*

(4) $\mathrm{Ext}^{n+1}_A(M, N) = 0$ *for all finitely generated A-modules M.*

(5) $\mathrm{Ext}^{n+1}_A(A/I, N) = 0$ *for all ideals $I \subseteq A$.*

Proof This proof is left as an exercise for the reader. Hint: See the proof of Proposition 5.39. ■

As immediate corollaries to this proposition we have two more characterizations of injective dimension:

Corollary 5.48 *If A is a ring and N is an A-module, then:*

$$\mathrm{id}_A(M) := \inf\left\{n : \begin{array}{l}\textit{Given any injective resolution } (E^\bullet, d^\bullet) \textit{ of } M,\\ \mathrm{Im}(d^{n-1}) \textit{ is injective}\end{array}\right\}$$

Corollary 5.49 *If A is a ring and N is an A-module, then*

$$\mathrm{id}_A(N) = \sup_M\{n : \mathrm{Ext}^n_A(M, N) \neq 0\},$$

where M varies over all finitely generated A-modules.

Exercise 5.50 *State and prove the analogous statements to Proposition 5.45 and Exercise 5.46 for injective dimension.*

Example 5.51 *The earlier exact sequence*

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

shows that $\mathrm{id}_{\mathbb{Z}}(\mathbb{Z}) \leq 1$. *One can show that, in fact,* $\mathrm{id}_{\mathbb{Z}}(\mathbb{Z}) = 1$.

Rings which have finite injective dimension as modules over themselves are called ***Gorenstein****. These rings are covered in a later chapter. An example of an Artinian non-Gorenstein ring is* $A = k[\![x, y]\!]/(x^2, xy, y^2)$. *It follows then that* $\mathrm{id}_A(A) = \infty$.

5.3.3 Global Dimension

Definition Given a ring A, the **global dimension** of A is defined to be:

$$\mathrm{gd}(A) := \sup_M \mathrm{pd}_A(M)$$

where the M varies over all A-modules.

We now have the following corollary to Proposition 5.39 and Proposition 5.47:

Corollary 5.52 *Given a ring A we have that:*

$$\begin{aligned}\mathrm{gd}(A) &= \sup_{M\in\mathbf{Mod}_A} \mathrm{pd}_A(M)\\ &= \sup_{M\in\mathbf{Mod}_A} \mathrm{id}_A(M)\\ &= \sup_{M\in\mathbf{Mod}_A} \mathrm{pd}_A(M) \qquad \textit{such that } M \textit{ is finitely generated.}\end{aligned}$$

5.4 The Local Case

Let $(A, \mathfrak{m}, k)$ be a local ring. Recall Corollary 2.35 which states that if M is a finitely generated A-module, then

$$\begin{aligned}\boldsymbol{\mu}(M) :=& \{\text{the minimal number of generators of } M\} \\ =& \dim_k(M/\mathfrak{m}M).\end{aligned}$$

The above fact will be used extensively.

The next theorem is very important as it shows that projective modules and flat modules are **locally free**. This means that when you localize a finitely generated flat or projective module at a prime ideal, you get a free module.

Theorem 5.53 *If A is a local ring and M is a finitely generated A-module, then the following are equivalent:*

(1) *M is free.*

(2) *M is projective.*

(3) *M is flat.*

(4) *$\operatorname{Tor}_i^A(M, N) = 0$ for all A-modules N and for all $i > 0$.*

(5) *$\operatorname{Tor}_1^A(M, k) = 0$.*

Proof All that needs to be shown is (5) $\Rightarrow$ (1). Let F be a free module mapping onto the minimal generators of M and obtain the short exact sequence

$$0 \to S \to F \to M \to 0.$$

Applying $- \otimes_A k$ we obtain the short exact sequence

$$0 \to S/\mathfrak{m}S \to F/\mathfrak{m}F \to M/\mathfrak{m}M \to 0$$

since $\operatorname{Tor}_1^A(M, k) = 0$. However, since we map a basis of F onto a minimal set of generators of M, we see $F/\mathfrak{m}F \cong M/\mathfrak{m}M$ and so $S/\mathfrak{m}S$ is 0. Hence by Corollary 0.29, Nakayama's Lemma, we see that $S = 0$ and so $M \cong F$. ■

5.4.1 Minimal Free Resolutions

Let $(A, \mathfrak{m}, k)$ be a local ring and M be a finitely generated A-module. We are going to discuss the construction of a minimal free resolution of M. Recalling Corollary 2.35, set

$$\begin{aligned}\beta_0 &:= \operatorname{rank}_k(M/\mathfrak{m}M), \\ S_1 &:= \operatorname{Ker}(A^{\beta_0} \to M),\end{aligned}$$

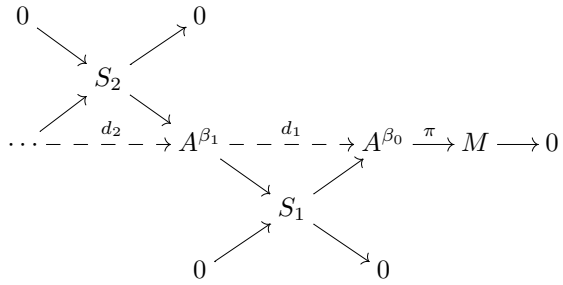
where the map $A^{\beta_0} \to M$ is defined by mapping a basis of A^{β_0} onto a minimal set of generators of M. Inductively define

$$\beta_i := \text{rank}_k(S_i/\mathfrak{m}S_i),$$
$$S_{i+1} := \text{Ker}(A^{\beta_i} \to S_i),$$

where at each step, the map $A^{\beta_i} \to S_i$ is defined by mapping a basis of A^{β_i} onto a minimal set of generators of S_i. Now we may inductively write the exact sequences:

$$0 \to S_1 \to A^{\beta_0} \to M \to 0,$$
$$0 \to S_{i+1} \to A^{\beta_i} \to S_i \to 0.$$

The integer β_i is sometimes called the ith **Betti number** of M and S_i is referred to as the ith **syzygy** of M. The rather mysterious word *syzygy* means *yoke*. After putting the above exact sequences together, we can see why *syzygy* is a good term to use for the S_i's, as each S_i is connecting two free modules via A-module homomorphisms:



The d_i's above are formed by taking the composition $A^{\beta_i} \to S_i \to A^{\beta_{i-1}}$, while π is the canonical surjection. Hence we obtain a **free resolution** of M, that is a long exact sequence of free modules ending at M:

$$\cdots \longrightarrow A^{\beta_3} \xrightarrow{d_3} A^{\beta_2} \xrightarrow{d_2} A^{\beta_1} \xrightarrow{d_1} A^{\beta_0} \xrightarrow{\pi} M \longrightarrow 0$$

A resolution of this form is called a **minimal free resolution**. Note that the condition that A is local, and hence Noetherian, is critical for this construction. By Corollary 5.57, we see that the projective dimension of M is given by

$$\text{pd}_A(M) = \sup\{n : \text{Tor}_i^A(M, k) \neq 0\}.$$

Since the entries of the matrices defining the d_i's in a minimal free resolution live in $\mathfrak{m}$, they become zero maps when tensored by k. Hence

$$\text{Tor}_i^A(M, k) = \frac{\text{Ker}(d_i \otimes 1)}{\text{Im}(d_{i+1} \otimes 1)} = A^{\beta_i} \otimes_A k \cong k^{\beta_i}.$$

Thus we see that if the projective dimension of M is finite, then the degree of the final nonzero term in the minimal free resolution is equal to $\text{pd}_A(M)$. Hence a minimal free resolution is truly a resolution of minimal length.

Proposition 5.54 *Let $(A, \mathfrak{m}, k)$ be a local ring, M a finitely generated A-module, and $F_\bullet$ be any free resolution of M where each F_i has finite rank and such that:*

(1) $\pi : F_0 \twoheadrightarrow M$ *and* $\mathrm{Ker}(\pi) \subseteq \mathfrak{m}F_0$.

(2) $\mathrm{Im}(d_i) = \mathrm{Ker}(d_{i-1}) \subseteq \mathfrak{m}F_{i-1}$.

Then $F_\bullet$ is a minimal free resolution of M.

Proof Consider the exact sequences:

$$0 \to S_1 \to F_0 \to M \to 0$$
$$0 \to S_{i+1} \to F_i \to S_i \to 0$$

Where S_i is the ith syzygy as defined above. Now apply $- \otimes_A k$ to obtain

$$F_0 \otimes_A k \cong M \otimes_A k,$$
$$F_i \otimes_A k \cong S_i \otimes_A k.$$

Thus by Corollary 2.35, we see that the rank of F_0 is the minimum number of generators of M. Similarly, we see that F_i is a free module of rank equal to the minimum number of generators of S_i. ■

Exercise 5.55 *Let M be a finitely generated module over a local ring A. Then the minimal free resolution of M is unique up to isomorphism of complexes.*

Proposition 5.56 *If $(A, \mathfrak{m}, k)$ is a local ring and M is a finitely generated A-module, then the following are equivalent:*

(1) $\mathrm{pd}_A(M) \leq n$.

(2) $\mathrm{Tor}_i^A(M, N) = 0$ *for all A-modules N and for all $i > n$.*

(3) $\mathrm{Tor}_{n+1}^A(M, k) = 0$.

Proof The only nontrivial implication is (3) $\Rightarrow$ (1). Let $F_\bullet$ be a minimal free resolution of M. After tensoring by k, all the differentials become 0 maps and so $\mathrm{Tor}_{n+1}^A(M, k) = F_{n+1} \otimes_A k = 0$. This means $F_{n+1} = 0$ and so $\mathrm{pd}_A(M) \leq n$. ■

Later on we will be able to remove the condition that A is a local ring for the above proposition.

Corollary 5.57 *If $(A, \mathfrak{m}, k)$ is a local ring and M is a finitely generated A-module, then*

$$\mathrm{pd}_A(M) = \sup\{n : \mathrm{Tor}_i^A(M, k) \neq 0\}.$$

Proposition 5.58 *If $(A, \mathfrak{m}, k)$ is a local ring, the following are equivalent:*

(1) $\mathrm{gd}(A) \leq n$.

(2) $\mathrm{Tor}_i^A(M,N) = 0$ *for* $i > n$ *and all* A*-modules* M *and* N.

(3) $\mathrm{Tor}_{n+1}^A(k,k) = 0$.

Proof All that needs to be shown is (3) $\Rightarrow$ (1). If $\mathrm{Tor}_{n+1}^A(k,k) = 0$, then $\mathrm{pd}_A(k) \leq n$. So by Proposition 5.56, $\mathrm{Tor}_{n+1}^A(M,k) = 0$ for all A-modules M. In particular, $\mathrm{Tor}_{n+1}^A(M,k) = 0$ for all finitely generated A-modules M. Again by Proposition 5.56 we have that $\mathrm{pd}_A(M) \leq n$ for all finitely generated A-modules M. Thus $\mathrm{gd}(A) \leq n$ by Corollary 5.52. ■

Corollary 5.59 *If* $(A, \mathfrak{m}, k)$ *is a local ring,*

$$\mathrm{gd}(A) = \mathrm{pd}_A(k).$$

There is an analogous result to Corollary 5.57 for injective dimension over local rings.

Theorem 5.60 *Let* $(A, \mathfrak{m}, k)$ *be a local ring and* M *a finitely generated* A*-module. Then*

$$\mathrm{id}_A(M) = \sup\{i : \mathrm{Ext}_A^i(k, M) \neq 0\}.$$

Proof We refer the reader to [3, Proposition 3.1.14]. ■

5.5 Regular Rings and Global Dimension

5.5.1 Regular Local Rings

Definition If $(A, \mathfrak{m})$ is local, A is a **regular local ring** if

$$\dim(A) = \boldsymbol{\mu}(\mathfrak{m}) = \{\text{the minimal number of generators of } \mathfrak{m}\}.$$

Example 5.61 *Examples of regular local rings:*

(1) *Consider* $A = k[\![X_1, \ldots, X_n]\!]$ *where* k *is a field. Here* $\dim(A) = n$ *and* $\mathfrak{m} = (X_1, \ldots, X_n)$. *Thus* A *is a regular local ring.*

(2) *Any DVR is a regular local ring of dimension* 1 *since its maximal ideal is principal. In particular,* $\mathbb{Z}_{(p)}$ *and* $k[X]_{(X)}$ *are regular local rings.*

Example 5.62 *A nonexample of a regular local ring:*

$$A = \frac{k[\![X,Y,U,V]\!]}{(XY - UV)} \qquad \text{or} \qquad A = \frac{k[X,Y,U,V]_{\mathfrak{m}}}{(XY - UV)}$$

In either case $\mathfrak{m} = (X, Y, U, V)$ *but* $\dim(A) = 3$.

Exercise 5.63 *Consider*

$$A = \frac{k[X,Y,U,V]_{\mathfrak{m}}}{(XY - UV)}.$$

Letting $\mathfrak{p} = (X, U)$, *write down a free resolution of* $A/\mathfrak{p}$ *over* A. *Can you get a finite free resolution of* $A/\mathfrak{p}$ *over* A?

Definition If $(A, \mathfrak{m})$ is a regular local ring, a system of parameters $x_1, \ldots, x_d$ is called a **regular system of parameters** if $\mathfrak{m} = (x_1, \ldots, x_d)$.

Proposition 5.64 *Let $(A, \mathfrak{m})$ be a regular local ring of dimension n and*

$$x_1, \ldots, x_j \in \mathfrak{m}.$$

Then $x_1, \ldots, x_j$ form part of a regular system of parameters for A if and only if for all i, $1 \leq i \leq j$, $A/(x_1, \ldots, x_i)$ is a regular local ring of dimension $n - i$.

Proof Throughout this proof set $A_i = A/(x_1, \ldots, x_i)$ and thus

$$\mathfrak{m}_{A_i} = \mathfrak{m}/(x_1, \ldots, x_i).$$

($\Rightarrow$) By the definition of A_i we have that $\dim(A_i) \geq n - i$. The maximal ideal $\mathfrak{m}_{A_i}$ of A_i is generated by $n - i$ elements since you can extend $x_1, \ldots, x_i$ to a regular system of parameters. Thus $\dim(A_i) \leq n - i$ and so we see that $\dim(A_i) = n - i$.

($\Leftarrow$) If $\dim(A_i) = n - i$ and A_i is a regular local ring, then $\mathfrak{m}_{A_i}$ can be generated by $n - i$ elements. Since A is a regular local ring, $x_1, \ldots, x_i$ must form part of a regular system of parameters. ■

Definition Given a ring A and an A-module M, $x_1, \ldots, x_n \in A$ is called an ***M*-sequence** or a **regular sequence on *M*** if the following hold:

(1) $(x_1, \ldots, x_n)M \neq M$.

(2) For each $i > 0$,

$$\frac{M}{(x_1, \ldots, x_{i-1})M} \xrightarrow{x_i} \frac{M}{(x_1, \ldots, x_{i-1})M}$$

is an injective map; that is, x_i is a nonzerodivisor on $M/(x_1, \ldots, x_{i-1})M$ for $1 \leq i \leq n$.

Example 5.65 *If $A = k[X_1, \ldots, X_n]$, then $X_1, \ldots, X_n$ form an A-sequence.*

Exercise 5.66 *If $A = k[X, Y, Z]$, $x_1 = X$, $x_2 = Y(X-1)$, and $x_3 = Z(X-1)$, then x_1, x_2, x_3 form an A-sequence, but x_3, x_2, x_1 does not.*

The next lemma tells us the relationship between an M-sequence and a system of parameters:

Lemma 5.67 *If A is a local ring, every M-sequence is part of a system of parameters for M.*

Proof This follows by repeatedly applying the exercise after Corollary 3.42. ■

Corollary 5.68 *If A is local and M is finitely generated A-module with $x_1, \ldots, x_i$ an M-sequence, then $i \leq \dim(M)$.*

It should be pointed out here that unless the ring is nice, the inequality above is strict.

Lemma 5.69 *If $(A, \mathfrak{m})$ is local ring and $a \in \mathfrak{m} - \mathfrak{m}^2$, then the exact sequence*

$$0 \longrightarrow aA/a\mathfrak{m} \xrightarrow{\iota} \mathfrak{m}/a\mathfrak{m} \longrightarrow \mathfrak{m}/aA \longrightarrow 0$$

splits.

Proof We must define $\eta : \mathfrak{m}/a\mathfrak{m} \to aA/a\mathfrak{m}$ such that $\eta \circ \iota = \mathbb{1}_{aA/a\mathfrak{m}}$. Take η to be the composite

$$\mathfrak{m}/a\mathfrak{m} \longrightarrow \mathfrak{m}/\mathfrak{m}^2 \xrightarrow{\varphi} A/\mathfrak{m} \xrightarrow{\cong} aA/a\mathfrak{m}$$

where $\varphi(\overline{a}) = \overline{1}$ and φ sends the rest of a k-basis for $\mathfrak{m}/\mathfrak{m}^2$ to 0. ■

Lemma 5.70 *Suppose that $(A, \mathfrak{m})$ is local and $\mathrm{gd}(A)$ is finite. Let $a \in \mathfrak{m} - \mathfrak{m}^2$ such that a is a nonzerodivisor on A. Then $\mathrm{gd}(A/aA)$ is finite.*

Proof First note that by Corollary 5.59 we have that $\mathrm{gd}(A) = \mathrm{pd}_A(A/\mathfrak{m})$. Thus if $\mathrm{gd}(A) = 0$, we have that A is a field implying that $\mathfrak{m}$ is zero, and hence we are done.

Assuming that $\mathrm{gd}(A) > 0$, write

$$0 \to \mathfrak{m} \to A \to A/\mathfrak{m} \to 0$$

and so we see that if $\mathrm{pd}_A(A/\mathfrak{m})$ is finite, then $\mathrm{pd}_A(\mathfrak{m})$ is finite. If a is a nonzerodivisor on A, then it is also a nonzerodivisor on $\mathfrak{m}$. Hence $\mathrm{pd}_{A/aA}(\mathfrak{m}/(a\mathfrak{m}))$ is finite by Proposition 5.44. By Lemma 5.69, we have that

$$\mathfrak{m}/a\mathfrak{m} \cong A/\mathfrak{m} \bigoplus \mathfrak{m}/aA.$$

By considering the Tor characterization of projective dimension we see that $\mathrm{pd}_{A/aA}(A/\mathfrak{m})$ is finite. Hence $\mathrm{gd}(A/aA)$ is finite. ■

Lemma 5.71 *If A is local and M is a finitely generated A-module with finite projective dimension, and $a \in \mathfrak{m}$ is a nonzerodivisor on M, then*

$$\mathrm{pd}_A(M/aM) = \mathrm{pd}_A(M) + 1.$$

Proof Write

$$0 \longrightarrow M \xrightarrow{a} M \longrightarrow M/aM \longrightarrow 0$$

apply the functor $- \otimes_A k$ and consider the long exact sequence for Tor. Since $a \in \mathfrak{m}$, the map $\mathrm{Tor}_i^A(M,k) \xrightarrow{a} \mathrm{Tor}_i^A(M,k)$ is in fact the zero map for all i and so we have the exact sequence

$$0 \to \mathrm{Tor}_i^A(M,k) \to \mathrm{Tor}_i^A(M/aM,k) \to \mathrm{Tor}_{i-1}^A(M,k) \to 0$$

for $i \geq 1$. Since $\mathrm{Tor}_{i-1}^A(M,k) = 0$ implies that $\mathrm{Tor}_i^A(M,k) = 0$, we must conclude that

$$\mathrm{Tor}_i^A(M/aM,k) = 0 \qquad \text{whenever} \qquad \mathrm{Tor}_{i-1}^A(M,k) = 0.$$

The theorem now follows from Theorem 5.56. ■

Exercise 5.72 *If A is a ring and $\mathfrak{a}$ is an ideal such that*

$$\mathfrak{a} \subseteq I_0 \cup I_1 \cup \cdots \cup I_n$$

where I_0 is a prime ideal. Show that there exists a proper subset S of $\{0, \ldots, n\}$ such that

$$\mathfrak{a} \subseteq \bigcup_{i \in S} I_i.$$

Lemma 5.73 *Let A be a local ring and suppose every element $\mathfrak{m} - \mathfrak{m}^2$ is a zerodivisor. Then every finitely generated module of finite projective dimension is free.*

Proof To start note that

$$\mathfrak{m} - \mathfrak{m}^2 \subseteq \bigcup_{\mathfrak{p} \in \mathrm{Ass}(A)} \mathfrak{p}$$

and so

$$\mathfrak{m} \subseteq \left(\bigcup_{\mathfrak{p} \in \mathrm{Ass}(A)} \mathfrak{p} \right) \cup \mathfrak{m}^2$$

Repeatedly applying the previous exercise we see that either $\mathfrak{m} \in \mathrm{Ass}(A)$ or that $\mathfrak{m} \subseteq \mathfrak{m}^2$. If the latter is the case, then

$$\mathfrak{m} = \mathfrak{m}^2$$

which implies that $\mathfrak{m} = 0$ by Corollary 0.29, Nakayama's Lemma. Hence A must be a field, and every finitely generated module over a field is free as it is a vector space.

So now suppose that $\mathfrak{m} \in \mathrm{Ass}(A)$. Thus A contains an element x annihilated by $\mathfrak{m}$ and we may write, setting $k = A/\mathfrak{m}$, the exact sequence:

$$0 \longrightarrow k \xrightarrow{x} A \longrightarrow A/xA \longrightarrow 0$$

Suppose that there exists some finitely generated A-module M of positive projective dimension. Applying the functor $- \otimes_A M$ to the above exact sequence and considering the long exact sequence for Tor we see that for all $i \geq 1$

$$\mathrm{Tor}_i^A(k, M) \cong \mathrm{Tor}_{i+1}^A(A/xA, M).$$

However now we see by Proposition 5.56 that if $\mathrm{pd}_A(M) = n$, then

$$\mathrm{Tor}_n^A(k, M) \neq 0 \qquad \text{and} \qquad \mathrm{Tor}_{n+1}^A(A/xA, M) = 0$$

which is impossible. Thus M must be free. ■

Theorem 5.74 *$(A, \mathfrak{m}, k)$ is a regular local ring if and only if $\mathrm{gd}(A)$ is finite. In this case*

$$\mathrm{gd}(A) = \dim(A).$$

Proof ($\Rightarrow$) Suppose that A is a regular local ring with $\mathfrak{m} = (x_1, \ldots, x_n)$. Setting $\mathbf{x}_i = x_1, \ldots, x_i$, we see that $\mathbf{x}_n$ is a regular system of parameters for A and thus $\mathbf{x}_n$ forms an A-sequence by Proposition **??**. Consider the following short exact sequences:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{x_1} & A & \longrightarrow & A/(x_1) & \longrightarrow & 0 \\
0 & \longrightarrow & A/(x_1) & \xrightarrow{x_2} & A/(x_1) & \longrightarrow & A/(\mathbf{x}_2) & \longrightarrow & 0 \\
 & & \vdots & & \vdots & & \vdots & & \\
0 & \longrightarrow & A/(\mathbf{x}_{n-1}) & \xrightarrow{x_n} & A/(\mathbf{x}_{n-1}) & \longrightarrow & A/(\mathbf{x}_n) & \longrightarrow & 0
\end{array}$$

By Lemma 5.71 we have that

$$\begin{aligned}
\mathrm{pd}_A(A) &= 0, \\
\mathrm{pd}_A(A/(x_1)) &= 1, \\
\mathrm{pd}_A(A/(\mathbf{x}_2)) &= 2, \\
&\vdots \\
\mathrm{pd}_A(A/(\mathbf{x}_n)) &= n.
\end{aligned}$$

But $A/(\mathbf{x}_n) = A/\mathfrak{m}$, and hence by Corollary 5.59, $\mathrm{gd}(A) = n$.

($\Leftarrow$) Now suppose that $\mathrm{gd}(A)$ is finite. Let $n = \mathrm{rank}_k(\mathfrak{m}/\mathfrak{m}^2)$, and proceed by induction on n. If $n = 0$, then $\mathfrak{m} = \mathfrak{m}^2$ and by Corollary 0.29, Nakayama's Lemma, we see $\mathfrak{m} = 0$ and so A must be a field, and hence regular.

Suppose that the statement is true up to n. We must check the case when $\mathrm{rank}_k(\mathfrak{m}/\mathfrak{m}^2) = n+1$. We claim that some element of $\mathfrak{m}-\mathfrak{m}^2$ is a nonzerodivisor. Suppose to the contrary that every element of $\mathfrak{m} - \mathfrak{m}^2$ is a zerodivisor. Now by Lemma 5.73 we see that every module of finite projective dimension is free. But if $\mathrm{gd}(A)$ is finite, then $\mathrm{pd}_A(k)$ is finite, and hence free, and so we must conclude that A is a field, a contradiction. Thus there is $a \in \mathfrak{m} - \mathfrak{m}^2$ which is a nonzerodivisor on A.

Now by Lemma 5.70, $\mathrm{gd}(A/aA)$ is finite and if we set $\overline{\mathfrak{m}} = \mathfrak{m}/aA$, then we have $n = \mathrm{rank}_k(\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2)$. Thus $\dim(A/aA) = n$, and so $\dim(A) = n + 1$. ■

Now we turn to the question which we started with in this section: If

$$A = \mathbb{C}[\![X_1, \ldots, X_n]\!]$$

and $\mathfrak{p}$ is a prime ideal in A, is $A_\mathfrak{p}$ a regular local ring? We answer this question in the affirmative with the following corollary:

Corollary 5.75 *If A is a regular local ring and $\mathfrak{p}$ is a prime ideal of A, then $A_\mathfrak{p}$ is a regular local ring.*

Proof Since A is a regular local ring, $\mathrm{gd}(A)$ is finite and hence $\mathrm{pd}_A(A/\mathfrak{p})$ is finite. Consider a free resolution of $A/\mathfrak{p}$:

$$F_\bullet : \qquad 0 \to F_i \to \cdots \to F_1 \to F_0 \to A/\mathfrak{p} \to 0$$

Apply the functor $- \otimes_A A_\mathfrak{p}$ to get:

$$(F_\bullet)_\mathfrak{p}: \qquad 0 \to (F_i)_\mathfrak{p} \to \cdots \to (F_1)_\mathfrak{p} \to (F_0)_\mathfrak{p} \to A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \to 0$$

Since $A_\mathfrak{p}$ is a flat A-module, $(F_\bullet)_\mathfrak{p}$ is an exact complex. Thus $\mathrm{pd}_{A_\mathfrak{p}}(A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p})$ is finite, and so $\mathrm{gd}(A_\mathfrak{p})$ is finite, and hence $A_\mathfrak{p}$ is a regular local ring. ■

Theorem 5.76 *A regular local ring is a domain.*

Proof Let $(R, \mathfrak{m})$ be a regular local ring with $\dim(R) = n$. Proceed by induction on n. If $n = 0$, then $\mathfrak{m}$ is an ideal generated by 0 elements, so $\mathfrak{m} = (0)$ and R is a field.

If $n = 1$, then $\mathfrak{m} = xR$ is principal. It follows that R is a DVR and in particular a domain.

When $n > 1$, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ be the minimal primes of R. Since $\mathfrak{m} \not\subseteq \mathfrak{m}^2$ and $\mathfrak{m} \not\subseteq \mathfrak{p}_i$ for all i, there exists $x \in \mathfrak{m}$ that is not contained in $\mathfrak{m}^2, \mathfrak{p}_1, \ldots, \mathfrak{p}_t$. So $\overline{x} \in \mathfrak{m}/\mathfrak{m}^2$ is a regular parameter. By Proposition 5.64, R/xR is a regular local ring of dimension $n-1$. By induction, R/xR is a domain and so xR is a height one prime ideal of R. Suppose $\mathfrak{p}_1$ is one of the minimal primes contained in xR. Let $y \in \mathfrak{p}_1 \subseteq xR$. Then we may write $y = rx$ for some $r \in R$. Since $x \notin \mathfrak{p}_1$, $r \in \mathfrak{p}_1$. Therefore $\mathfrak{p}_1 = x\mathfrak{p}_1$. By Nakayama's Lemma, Corollary 0.29, $\mathfrak{p}_1 = (0)$. Thus R is a domain.

■

Theorem 5.77 (Nagata) *Let A be a Noetherian domain, S a set of prime elements, and U the multiplicatively closed set generated by S. If $U^{-1}A$ is a UFD, then so is A.*

Proof Let $\mathfrak{p}$ be a height one prime ideal of A. If $\mathfrak{p} \cap U \neq \varnothing$, then $\mathfrak{p}$ contains an element $x \in S$, and since xA is a nonzero prime ideal, $\mathfrak{p} = xA$. If $\mathfrak{p} \cap U = \varnothing$, then $\mathfrak{p}U^{-1}A$ is a height one prime ideal of $U^{-1}A$. Since $U^{-1}A$ is a UFD, $\mathfrak{p}U^{-1}A = aU^{-1}A$ is principal for some $a \in \mathfrak{p}$. Among such a choose one such that aA is maximal under containment. Then a is not divisible by any $s \in S$. If $x \in \mathfrak{p}$, then $sx = ay$ for some $s \in S$ and some $y \in A$. Let $s = s_1 \cdots s_r$ with $s_i \in S$. By the choice of a, $a \notin s_iA$ for any i and so $y \in s_iA$ for all i. It follows that $y \in sA$ so that $x \in aA$. Hence $\mathfrak{p} = aA$.

■

Theorem 5.78 (Auslander-Buchsbaum) *If $(A, \mathfrak{m})$ is regular local, then A is a UFD.*

Proof We refer the reader to [12] for a proof. ■

5.5.2 Regular Rings

Definition A Noetherian ring A is **regular** if $\mathrm{gd}(A)$ is finite.

Exercise 5.79 *If A is Noetherian and M is a finitely generated A-module, then show the following:*

(1) $\mathrm{pd}_A(M) = \sup_{\mathfrak{m}\in \mathrm{MaxSpec}(A)} \mathrm{pd}_{A_\mathfrak{m}}(M_\mathfrak{m})$.

(2) *Suppose that* $\mathrm{pd}_{A_\mathfrak{m}}(M_\mathfrak{m})$ *is finite for all* $\mathfrak{m} \in \mathrm{MaxSpec}(A)$. *Then* $\mathrm{pd}_A(M)$ *is finite.*

Proposition 5.80 *If A is a Noetherian ring and M is a finitely generated A-module, then the following are equivalent:*

(1) $\mathrm{pd}_A(M) \leq n$.

(2) $\mathrm{Tor}_i^A(M, N) = 0$ *for all A-modules N and all $i > n$.*

(3) $\mathrm{Tor}_{n+1}^A(M, A/\mathfrak{m}) = 0$ *for all* $\mathfrak{m} \in \mathrm{MaxSpec}(A)$.

Proof Follows from the above exercise and Proposition 5.56. ■

Proposition 5.81 *If A is Noetherian, the following are equivalent:*

(1) $\mathrm{gd}(A) \leq n$.

(2) *For all finitely generated A-modules M and N,* $\mathrm{Tor}_{n+1}^A(M, N) = 0$.

(3) *For all finitely generated A-modules M and all maximal ideals $\mathfrak{m} \subseteq A$,* $\mathrm{Tor}_{n+1}^A(M, A/\mathfrak{m}) = 0$.

(4) $\mathrm{Tor}_{n+1}^A(A/\mathfrak{m}, A/\mathfrak{m}) = 0$ *for all maximal ideals $\mathfrak{m} \subseteq A$.*

Proof Follows from the above exercise and Proposition 5.58. ■

Corollary 5.82 *If A is a ring then A is regular if and only if* $\mathrm{pd}_A(A/\mathfrak{m}) < \infty$ *for all maximal ideals $\mathfrak{m} \subseteq A$.*

Corollary 5.83 *If A is a regular ring, then $A_\mathfrak{p}$ is regular local for all $\mathfrak{p} \in \mathrm{Spec}(A)$.*

Exercise 5.84 *Consider*

$$A = \frac{\mathbb{R}[X, Y, Z]}{(X^2 + Y^2 - Z^2 - 1)}.$$

Show that A is a regular ring but not a UFD. Conclude that the previous theorem is false if the local condition is dropped.

Example 5.85 *If A is regular, then $A[x]$ is regular. Moreover*

$$\mathrm{gd}(A[x]) = \mathrm{gd}(A) + 1.$$

Example 5.86 *The following are examples of regular rings.*

(1) *If k is a field, then $k[X_1, \ldots, X_n]$ is regular.*

(2) *$\mathbb{Z}[X_1, \ldots, X_n]$ is regular.*

(3) *If A is a Dedekind domain, then $A[X_1, \ldots, X_n]$ is regular.*

(4) *If k is a field, then $k[\![X_1, \ldots, X_n]\!][Y_1, \ldots, Y_m]$ is regular.*

Chapter 6

Depth and Cohen-Macaulay Modules

6.1 Depth

Definition Given a ring A and an A-module M, $x_1, \ldots, x_n \in A$ is called **M-regular** or an **M-sequence** if the following hold:

(1) $(x_1, \ldots, x_n)M \neq M$.

(2) For each $i > 0$,

$$\frac{M}{(x_1, \ldots, x_{i-1})M} \xrightarrow{x_i} \frac{M}{(x_1, \ldots, x_{i-1})M}$$

is an injective map; that is, x_i is a nonzerodivisor on $M/(x_1, \ldots, x_{i-1})M$ for $1 \leq i \leq n$.

Example 6.1 *If $A = k[X_1, \ldots, X_n]$, then $X_1, \ldots, X_n$ form an A-sequence.*

Exercise 6.2 *If $A = k[X, Y, Z]$, $x_1 = X$, $x_2 = Y(X-1)$, and $x_3 = Z(X-1)$, then x_1, x_2, x_3 form an A-sequence, but x_3, x_2, x_1 does not.*

Remark By the exercise we see that a permutation of an M-sequence is not in general another M-sequence.

Lemma 6.3 *If $x_1, \ldots, x_n$ is an M-sequence and*

$$x_1\xi_1 + \cdots + x_n\xi_n = 0,$$

with $\xi_i \in M$ for all i, then $\xi_i \in (x_1, \ldots, x_n)M$ for all i.

Proof Proceed by induction on n. If $n = 1$, then we have $x_1\xi_1 = 0$ which implies that $\xi_1 = 0 \in (x_1)M$.

Now suppose the lemma is true for $1, \ldots, n-1$. Since

$$x_1\xi_1 + \cdots + x_{n-1}\xi_{n-1} + x_n\xi_n = 0,$$

we have that $x_n\xi_n = 0$ in $M/(x_1, \ldots, x_{i-1})$. However, since x_n is a nonzerodivisor on $M/(x_1 \ldots, x_{n-1})$, we see that in fact $\xi_n \in (x_1, \ldots, x_{n-1})M$. Hence for some $m_1, \ldots, m_{n-1}$ we have

$$\xi_n = x_1m_1 + \cdots + x_{n-1}m_{n-1}.$$

Thus

$$\begin{aligned} x_1\xi_1 + \cdots + x_{n-1}\xi_{n-1} + x_n(x_1m_1 + \cdots + x_{n-1}m_{n-1}) = 0, \\ x_1(\xi_1 + x_nm_1) + x_2(\xi_2 + x_nm_2) + \cdots + x_{n-1}(\xi_{n-1} + x_nm_{n-1}) = 0. \end{aligned}$$

By induction, $(\xi_i + x_nm_i) \in (x_1, \ldots, x_{n-1})M$ and so we see that

$$\xi_i \in (x_1, \ldots, x_n)M \qquad \text{for } i = 1 \text{ to } n-1$$

and so we are done. ■

Lemma 6.4 *If $x_1, \ldots, x_n$ is an M-sequence, then $x_1^{r_1}, \ldots, x_n^{r_n}$ is an M-sequence for any positive integers $r_1, \ldots, r_n$.*

Proof It is enough to show $x_1^r, x_2, \ldots, x_n$ is an M-sequence as then we may consider $M' = M/x_1^rM$ with M'-sequence $x_2, \ldots, x_n$ and work inductively. Note that it is clear that

$$(x_1^r, \ldots, x_n)M \neq M,$$

since

$$(x_1, \ldots, x_n)M \neq M.$$

Now proceed by induction on r. The case of $r = 1$ is trivial. So let's assume that our theorem is true for $r = 1, \ldots, r-1$. Since

$$\frac{M}{(x_1, \ldots, x_{i-1})M} \xrightarrow{x_1} \frac{M}{(x_1, \ldots, x_{i-1})M}$$

is injective, so is

$$\frac{M}{(x_1, \ldots, x_{i-1})M} \xrightarrow{x_1^r} \frac{M}{(x_1, \ldots, x_{i-1})M}.$$

We must now show that $\mathbf{x}_i$ is a nonzerodivisor on $M/(x_1^r, x_2, \ldots, x_{i-1})M$ for $i = 2, \ldots, n$. Suppose for some $m \in M$ and for $\xi_1, \ldots, \xi_{i-1} \in M$ that

$$x_im = x_1^r\xi_1 + x_2\xi_2 + \cdots + x_{i-1}\xi_{i-1}.$$

Since we assume $x_1^{r-1}, \ldots, x_{i-1}$ is an M-sequence by induction, we have

$$m = x_1^{r-1}m_1 + x_2m_2 + \cdots + x_{i-1}m_{i-1}$$

where $m_1, \ldots, m_{i-1} \in M$. Hence

$$0 = x_1(x_1^{r-1}\xi_1 - x_i m_1) + x_2(\xi_2 - x_i m_2) + \cdots + x_{n-1}(\xi_{i-1} - x_i m_{n-1}).$$

Thus by Lemma 6.3, we see that $(x_1^{r-1}\xi_1 - x_i m_1) \in (x_1, \ldots, x_{n-1})M$. Thus, $(x_i m_1) \in (x_1, \ldots, x_{i-1})M$ and so we see $m_1 \in (x_1, \ldots, x_{i-1})M$, because $x_1, \ldots, x_i$ is an M-sequence. Hence

$$m \in (x_1^r, \ldots, x_{i-1})M$$

and so we see that x_i is an injective map on $M/(x_1, \ldots, x_{i-1})$. Hence $x_1^r, \ldots, x_n$ is an M-sequence. This proves the theorem. ■

Definition Let A be a ring and let M be an A-module. Then $x_1, \ldots, x_n$ is called an ***M*-quasi-regular sequence** if given a ring A, an A-module M, $x_1, \ldots, x_n \in M$ such that if $(x_1, \ldots, x_n) = I$, $IM \neq M$, and a module homomorphism $\psi : M[\mathbf{X}] \to M$ via

$$\psi : \sum m_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n} \to \sum m_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n},$$

the following condition holds for each r:

($\bigstar$) Given $f \in M[\mathbf{X}]$, a homogeneous polynomial of degree r, $\psi(f) = f(x_1, \ldots, x_n) \in I^{r+1}M$ implies that the coefficients of f are in IM.

Proposition 6.5 *In the above definition the condition ($\bigstar$) is actually equivalent to each of the following:*

($\bigstar\bigstar$) *Given $f \in M[\mathbf{X}]$, a homogeneous polynomial, $\psi(f) = 0$ implies that the coefficients of f are in IM.*

($\bigstar\bigstar\bigstar$) *The map*

$$\Phi : \frac{M}{IM}[\mathbf{X}] \to \frac{M}{IM} \oplus \frac{IM}{I^2M} \oplus \frac{I^2M}{I^3M} \oplus \cdots$$

defined by sending a homogeneous polynomial f of degree r to the residue class of $f(x_1, \ldots, x_n)$ in $I^rM/I^{r+1}M$ is an isomorphism.

Proof ($\bigstar$) $\Rightarrow$ ($\bigstar\bigstar$) Clear.

($\bigstar\bigstar$) $\Rightarrow$ ($\bigstar$) Suppose that $\psi(f) \in I^{r+1}M$. Now there exits a homogeneous polynomial $g(X) \in M[\mathbf{X}]$ of degree r such that $\psi(f) = \psi(g)$ with the coefficients of g in IM. Since ψ is a homomorphism, $\psi(f - g) = 0$, and so we see the coefficients of $f - g$ are in IM. Hence the coefficients of f are in IM.

The equivalence of ($\bigstar\bigstar$) and ($\bigstar\bigstar\bigstar$) is left to the reader. ■

Remark Let $x_1, \ldots, x_n$ be an M-quasi-regular sequence. Then $x_1, \ldots, x_i$ for $i < n$ is not necessarily M-quasi-regular. This is in contrast with the case for M-sequences.

Theorem 6.6 *Given a ring A, M an A-module with $I = (x_1, \ldots, x_n)$ an ideal of A, we have the following*

(1) *Suppose that $x_1, \ldots, x_n$ is an M-quasi-regular sequence. If $x \in A$ is such that $(IM :_M x) = IM$, then $(I^r M :_M x) = I^r M$, where*

$$(IM :_M x) := \{m \in M : xm \in IM\}.$$

(2) *If $x_1, \ldots, x_n$ is an M-sequence, then $x_1, \ldots, x_n$ is an M-quasi-regular sequence.*

(3) *If the I-adic topologies on $M, M/x_1M, \ldots, M/(x_1, \ldots, x_{n-1})M$ are all Hausdorff and if $x_1, \ldots, x_n$ is an M-quasi-regular sequence, then $x_1, \ldots, x_n$ is an M-sequence.*

Proof (1) Proceed by induction on r. The statement is trivial if $r = 1$. Assume that $(I^{r-1}M :_M x) = I^{r-1}M$. Then

$$m \in (I^r M :_M x) \Rightarrow xm \in I^r M \subseteq I^{r-1}M.$$

Thus $m \in (I^{r-1}M :_M x) = I^{r-1}M$ by induction. Hence there is a homogeneous form $F(x_1, \ldots, x_n) \in M[x_1, \ldots, x_n]$ of degree $r-1$, which we can write as

$$F(x_1, \ldots, x_n) = \sum m_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n},$$

such that

$$m = F(a_1, \ldots, a_n).$$

By above,

$$xm = \sum x m_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n} \in I^r M.$$

By quasi-regularity, $xm_{i_1,\ldots,i_n} \in IM$ for all tuples $(i_1, \ldots, i_n)$. Since each $m_{i_1,\ldots,i_n} \in (IM :_M x) = IM$, we have that

$$m = F(a_1, \ldots, a_n) \in I^r M.$$

(2) Let $x_1, \ldots, x_n$ be an M-sequence. We proceed by induction on n. If $n = 1$, then a degree r form $F(X)$ in $M[X]$ must be of the form mX^r for some $m \in M$. If $F(x_1) = 0$, then $mx_1^r = 0$. Since x_1 is an M-sequence, x_1 is a nonzerodivisor on M and so $m = 0$. In particular $m \in IM$. Therefore by ($\bigstar\bigstar$), x_1 is an M-quasi-regular sequence.

Now assume that (2) is true up to $n-1$. So we can assume that $x_1, \ldots, x_{n-1}$ is M-quasi-regular. Let $F(X_1, \ldots, X_n)$ be a form in $M[X_1, \ldots, X_n]$ of degree r such that $F(x_1, \ldots, x_n) = 0$. We prove by induction on r that the coefficients of F lie in IM. The case $r = 1$ is proved by Lemma 6.3. Assume (2) holds for forms of degree less than r. Write

$$F(X_1, \ldots, X_n) = G(X_1, \ldots, X_{n-1}) + X_n H(X_1, \ldots, X_n),$$

where $\deg G = r$ and $\deg H = n-1$. Therefore

$$x_n H(x_1, \ldots, x_n) = -G(x_1, \ldots, x_{n-1}) \in (x_1, \ldots, x_{n-1})M.$$

Since $x_1, \ldots, x_n$ form an M-sequence, we have

$$((x_1, \ldots, x_{n-1})M :_M x_n) = (x_1, \ldots, x_{n-1})M.$$

Thus by (1), $H(x_1, \ldots, x_n) \in (x_1, \ldots, x_{n-1})^r M \subseteq (x_1, \ldots, x_n)M$. Since $\deg H = r-1$ by induction we have that the coefficients of G are in IM. In addition we can write $H(x_1, \ldots, x_n) = H'(x_1, \ldots, x_{n-1})$ where H' is a form of degree r in $M[X_1, \ldots, X_{n-1}]$. Now set

$$F'(X_1, \ldots, X_{n-1}) = G(X_1, \ldots, X_{n-1}) + x_n H'(X_1, \ldots, X_{n-1}).$$

Then F' is a form of degree r in $M[X_1, \ldots, X_{n-1}]$. Further, we have

$$\begin{aligned} F'(x_1, \ldots, x_{n-1}) &= G(x_1, \ldots, x_{n-1}) + x_n H'(x_1, \ldots, x_{n-1}), \\ &= G(x_1, \ldots, x_{n-1}) + x_n H(x_1, \ldots, x_n), \\ &= 0. \end{aligned}$$

Since $x_1, \ldots, x_{n-1}$ is M-quasi-regular, the coefficients of F' are in IM. Therefore the coefficients of H are in IM, and hence those of F are in IM. This proves that $x_1, \ldots, x_n$ is M-quasi-regular.

(3) Suppose that $x_1, \ldots, x_n$ is an M-quasi-regular sequence and that the I-adic topologies on each of $M, M/x_1M, M/(x_1, x_2)M, \ldots, M/IM$ are Hausdorff. We first show that x_1 is an M-sequence. Suppose $x_1 m = 0$ for some $m \in M$. Then since x_1 is a quasi-regular sequence, $m \in IM$. Thus we can write

$$m = x_1 m_1 + \cdots x_n m_n$$

where $m_1, \ldots, m_n \in M$. Thus

$$x_1^2 m_1 + x_1 x_2 m_2 + \cdots + x_1 x_n m_n = 0.$$

Again, since $x_1, \ldots, x_n$ is a quasiregular sequence, $m \in I^2 M$. Continuing in this way we get that $m \in \bigcap I^n M$, which is (0) by hypothesis. Thus x_1 is a nonzerodivisor on M.

It suffices now to show that $x_2, \ldots, x_n$ is an M/x_1M-quasi-regular sequence, since by induction then $x_2, \ldots, x_n$ is an M/x_1M-sequence and hence $x_1, \ldots, x_n$ is an M-sequence. Using the ($\bigstar\bigstar$) criterion, we must show that if $F(X_2, \ldots, X_n)$ is a form of degree v in $M[X_2, \ldots, X_n]$ such that $F(x_2, \ldots, x_n) \in x_1 M$, then the coefficients of F are in IM. This is true for $v = 1$, since $x_1, \ldots, x_n$ is M-quasi-regular. Assume the statement is true for forms of degree less than v. We can write

$$F(x_2, \ldots, x_n) = x_1 m$$

for some $m \in M$. Since $\bigcap I^n M = 0$, there is some integer i such that $m \in I^i M - I^{i+1} M$. Thus we can write

$$F(x_2, \ldots, x_n) = x_1 H(x_1, \ldots, x_n)$$

where $H(X_1, \ldots, X_n)$ is a form of degree i in $M[X_1, \ldots, X_n]$. Suppose $i < v-1$. Then $X_1 H(X_1, \ldots, X_n)$ is a form of degree at most v. Since $F(x_2, \ldots, x_n) - x_1 H(x_1, \ldots, x_n) = 0$, the coefficients of H are in IM. But then $m \in I^{i+1} M$, a contradiction. Therefore $i \geq v - 1$. We may assume then that $\deg(H) = v - 1$. Then

$$F'(X_1, \ldots, X_n) = F(X_2, \ldots, X_n) - X_1 H(X_1, \ldots, X_n)$$

is a form of degree v such that $F'(x_1, \ldots, x_n) = 0$. Thus the coefficients of F', and hence those of F, are in IM. ■

Corollary 6.7 *If (3) in the above theorem is satisfied, then the sequence can be permuted; that is, any permutation of an M-sequence $x_1, \ldots, x_n$ is again an M-sequence, because any permutation of an M-quasi-regular sequence is again M-quasi-regular.*

Remark Now consider the Noetherian case. Let A be a Noetherian ring and M a finitely generated A-module. Let $x_1, x_2, \ldots$ be an M-sequence. Then we get a strictly increasing sequence of submodules

$$(x_1)M \subsetneq (x_1, x_2)M \subsetneq (x_1, x_2, x_3)M \subsetneq \cdots .$$

By assumption this chain must terminate. Hence any M-sequence must be of finte length. The natural question then is do all M-sequences have the same length. The next couple results will answer that question in the affirmative.

Lemma 6.8 *If A is a Noetherian ring with M a finitely generated A-module and N any A-module, then* $\mathrm{Ass}_A(\mathrm{Hom}_A(M, N)) = \mathrm{Supp}_A(M) \cap \mathrm{Ass}_A(N)$.

Proof ($\subseteq$) Recall that $\mathfrak{p} \in \mathrm{Ass}_A(T)$ if and only if $\mathfrak{p}A_\mathfrak{p} \in \mathrm{Ass}_{A_\mathfrak{p}}(T_\mathfrak{p})$. So take $\mathfrak{p} \in \mathrm{Ass}_A(\mathrm{Hom}_A(M, N))$. Then $\mathfrak{p}A_\mathfrak{p} \in \mathrm{Ass}_{A_\mathfrak{p}}(\mathrm{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}))$. Since $\mathrm{Ass}_{A_\mathfrak{p}}(\mathrm{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})) \neq \varnothing$, $\mathrm{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}) \neq 0$ and hence $M_\mathfrak{p} \neq 0$. Thus $\mathfrak{p} \in \mathrm{Supp}(M)$. Further, we have an injection $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \hookrightarrow \mathrm{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})$. Therefore

$$\mathrm{Hom}_{A_\mathfrak{p}}(A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \otimes_{A_\mathfrak{p}} M_\mathfrak{p}, N_\mathfrak{p}) \cong \mathrm{Hom}_{A_\mathfrak{p}}(A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}, \mathrm{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})) \neq 0.$$

Since $M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p} = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \otimes_{A_\mathfrak{p}} M_\mathfrak{p}$ is a vector space over $A_\mathfrak{p}/pA_\mathfrak{p}$, there is a nonzero map from $A_p/\mathfrak{p}A_\mathfrak{p} \to M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p}$. Therefore $\mathrm{Hom}_{A_\mathfrak{p}}(A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}, N_p) \neq 0$ and so we have an injection $A_p/\mathfrak{p}A_\mathfrak{p} \hookrightarrow N_p$. Therefore $\mathfrak{p}A_\mathfrak{p} \in \mathrm{Ass}_{A_p}(N_p)$ and hence $\mathfrak{p} \in \mathrm{Ass}_A(N)$.

($\supseteq$) Working backwards, take $\mathfrak{p} \in \mathrm{Supp}_A(M) \cap \mathrm{Ass}_A(N)$. Then we have that $M_\mathfrak{p} \neq 0$ and there is an injection $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \hookrightarrow N_\mathfrak{p}$. By Nakayama's Lemma,

$$M_p \otimes_{A_\mathfrak{p}} A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \cong M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p} \neq 0.$$

Since $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ is a field, $M_p \otimes_{A_\mathfrak{p}} A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ is a nonzero vector field over $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. Hence there is a nonzero map $M_\mathfrak{p} \otimes_{A_\mathfrak{p}} A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \to A_p/\mathfrak{p}A_p$. Composing with the injection above yields a nonzero map in $\mathrm{Hom}_{A_\mathfrak{p}}(M_p \otimes_{A_\mathfrak{p}} A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}, N_\mathfrak{p})$. Therefore

$$\mathrm{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p}, \mathrm{Hom}_{A_\mathfrak{p}}(A_p/\mathfrak{p}A_\mathfrak{p}, N_\mathfrak{p})) \cong \mathrm{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p} \otimes_{A_\mathfrak{p}} A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}, N_\mathfrak{p})) \neq 0.$$

Therefore $\mathfrak{p}A_\mathfrak{p} \in \mathrm{Ass}_{A_\mathfrak{p}}(\mathrm{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}))$, and so $\mathfrak{p} \in \mathrm{Ass}_A(\mathrm{Hom}_A(M, N))$. ■

Theorem 6.9 *If A is a Noetherian ring and M is a finitely generated A-module and I is an ideal of A such that $IM \neq M$. Then the following are equivalent:*

(1) $\mathrm{Ext}^i_A(N, M) = 0$ *for all $i < n$ and for all finitely generated A-modules N such that* $\mathrm{Supp}_A(N) \subseteq V(I) = \{\mathfrak{p} \in \mathrm{Spec}(A) : \mathfrak{p} \supseteq I\}$.

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

(3) $\mathrm{Ext}^i_A(N, M) = 0$ *for all $i < n$ for some finitely generated A-module N where* $\mathrm{Supp}_A(N) = V(I)$.

(4) *There exists $x_1, \ldots, x_n \in I$ which form an M-sequence.*

Proof (1) $\Rightarrow$ (2) $\Rightarrow$ (3) is obvious.

(3) $\Rightarrow$ (4) First we show that if $\mathrm{Hom}_A(N, M) = 0$, then there exists $a_1 \in I$ a nonzerodivisor on M. By the previous lemma, $\mathrm{Supp}_A(N) \cap \mathrm{Ass}_A(M) = \varnothing$. We prove by induction that there is an M-sequence of length n in I. Let $\mathfrak{p}$ be a prime ideal of A.

$$\begin{aligned} \mathfrak{p} \in \mathrm{Ass}_A(M) &\Rightarrow \mathfrak{p} \notin \mathrm{Supp}_A(N), \\ &\Rightarrow \mathfrak{p} \not\supseteq I. \end{aligned}$$

Hence, by prime avoidance,

$$I \not\subseteq \bigcup_{\mathfrak{p} \in \mathrm{Ass}_A(M)} \mathfrak{p}.$$

Since the union of associated primes are exactly the zerodivisors, there exists $a \in I$ such that a is a nonzerodivisor on M.

We now prove (3) $\Rightarrow$ (4) by induction on n. Observe that the $n = 0$ case is vacuous. Above we proved the $n = 1$ case. Now suppose that $Ext^i_A(N, M) = 0$ for $i < n$ for some finitely generated A-module N where $\mathrm{Supp}(A(N) = V(I)$. Since $\mathrm{Hom}_A(N, M) = 0$, there exists $a_1 \in I$ be a nonzerodivisor on M. Then we have an exact sequence

$$0 \to M \xrightarrow{a_1} M \to M/a_1M \to 0.$$

From the long exact sequence for Ext we have $\mathrm{Ext}^i_A(N, M/a_1M) = 0$ for $0 \leq i < n - 1$. By induction, there is an M/a_1M-sequence $a_2, \ldots, a_n$. Therefore $a_1, \ldots, a_n$ is an M-sequence.

(4) $\Rightarrow$ (1) Suppose $a_1, \ldots, a_n$ is an M-sequence in I. Let N be a finitely generated A-module with $\mathrm{Supp}_A(N) \subseteq V(I)$. Let $J = \mathrm{Ann}_A(N)$. Then $V(J) \subseteq V(I)$ and $\sqrt{I} \subseteq \sqrt{J}$. Hence there exists $t > 0$ such that $I^t \subseteq J$. Take any $f \in \mathrm{Hom}_A(N, M)$. Fix $n \in N$. Since $a_1^t \in \mathrm{Ann}_A(N)$, we have $a_1^t f(n) = f(a_1^t n) = f(0) = 0$. Since a_1^t is a nonzerodivisor on M, $f(n) = 0$ and so $\mathrm{Hom}_A(N, M) = 0$.

Now consider the exact sequence

$$0 \to M \xrightarrow{a_1^t} M \to M/a_1^t M \to 0.$$

Since $a_2, \ldots, a_n$ is an $M/a_1 M$-sequence, we may assume by induction that $\mathrm{Ext}_A^i(N, M/a_1^t M) = 0$ for $0 \leq i < n-1$. By the long exact sequence for Ext_A the map

$$\mathrm{Ext}_A^i(N, M) \xrightarrow{a_1^t} \mathrm{Ext}_A^i(N, M)$$

is an isomorphism for $0 \leq i < n-1$ and is injective for $i = n-1$. Since $a_1^t \in \mathrm{Ann}_A(N)$, the above map is the zero map for $0 \leq i < n$. Hence $\mathrm{Ext}_A^i(N, M) = 0$ for $0 \leq i < n$. ■

Definition Let A be a Noetherian ring, M a finitely generated A-module, and I an ideal of A such that $IM \neq M$. Then we define

$$\begin{aligned} \mathrm{depth}_I(M) &:= \inf\{i : \mathrm{Ext}^i(A/I, M) \neq 0\}, \\ &= \text{length of maximal } M\text{-sequence in } I. \end{aligned}$$

If A is a local ring with maximal ideal $\mathfrak{m}$, then $\mathrm{depth}_{\mathfrak{m}}(M)$ will be abbreviated by $\mathrm{depth}(M)$.

Exercise 6.10 *Suppose that A is a local ring and M is a finitely-generated A-module. Show that* $\mathrm{depth}(M) = 0$ *if and only if* $\mathfrak{m} \in \mathrm{Ass}_A(M)$.

Corollary 6.11 *If*

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

is a short exact sequence of finitely generated A-modules. Set $d_i = \mathrm{depth}_I(M_i)$. Then:

(1) $d_1 \geq \min\{d_2, d_3 + 1\}$.

(2) $d_2 \geq \min\{d_1, d_3\}$.

(3) $d_3 \geq \min\{d_1 - 1, d_2\}$.

Proof Use the long exact sequence for Ext and the previous theorem characterizing depth. ■

Exercise 6.12 *Suppose that A is Noetherian, M and N are A-modules, where* $\mathrm{depth}_{\mathrm{Ann}(M)}(N) = n$. *Show that*

$$\mathrm{Ext}_A^i(M, N) = \begin{cases} 0 & \text{if } i < n, \\ \mathrm{Hom}_A(M, N/(x_1, \ldots, x_n)N) & \text{if } i = n, \end{cases}$$

where $x_1, \ldots, x_n$ is a maximal N-sequence in $\mathrm{Ann}(M)$.

Exercise 6.13 *Suppose that A is local, M and N are A-modules, with* $\operatorname{depth}_{\operatorname{Ann}(M)}(N) = n$. *If $x_1, \ldots, x_n$ is both an A-sequence and an N-sequence, then setting $\overline{A} = A/\mathbf{x}A$ we have*

$$\operatorname{Ext}^i_A(M, N) = \operatorname{Ext}^{i-n}_{\overline{A}}(M, N/(x_1, \ldots, x_n)N)$$

for all $i > n$.

Definition If A is a Noetherian ring, and M is a finitely generated A-module, then the **grade** M is

$$\begin{aligned}\operatorname{grade}(M) &:= \inf\{i : \operatorname{Ext}^i_A(M, A) \neq 0\},\\ &= \operatorname{depth}_{\operatorname{Ann}(M)}(A),\\ &= \inf\{\operatorname{depth}(A_{\mathfrak{p}}) : \mathfrak{p} \in \operatorname{Supp}(M)\}.\end{aligned}$$

Exercise 6.14 *If A is a Noetherian ring with an ideal I, then*

$$\operatorname{depth}_I(A) \leq \operatorname{ht}(I).$$

Exercise 6.15 *If $x_1, \ldots, x_n$ is an A-sequence, then*

$$\operatorname{depth}_I(A) = \operatorname{ht}(I)$$

where $I = (x_1, \ldots, x_n)$.

Proposition 6.16 *Let A be a Noetherian ring and M, N be finitely generated A-modules where* $\operatorname{grade}(M) = m$ *and* $\operatorname{pd}_A(N) = n$. *Then for $i < m - n$*

$$\operatorname{Ext}^i_A(M, N) = 0.$$

Proof If $n = 0$, then N is projective and hence a direct summand of a free A-module. That is, there exists an A-module T such that $N \oplus T = A^t$ for some integer t. Since $\operatorname{grade}(M) = m$, $\operatorname{Ext}^i_A(M, A) = 0$ for $i < m$. Hence $\operatorname{Ext}^i_A(M, A^t) = 0$ for $i < m$. Thus $\operatorname{Ext}^i_A(M, N) = 0$ for $i < m$.

Now suppose $n > 0$. Then let

$$0 \to N' \to F \to N \to 0$$

be a short exact sequence where F is a finitely generated free A-module. Then $\operatorname{pd}(N') = n-1$ and so by induction $\operatorname{Ext}^i_A(M, N') = 0$ for $i < m-(n-1)$. Again we have $\operatorname{Ext}^i_A(M, F) = 0$ for $i < m$. Thus $\operatorname{Ext}^i_A(M, N) = 0$ for $i < m - n$. ■

Theorem 6.17 *Let $(A, \mathfrak{m})$ be a local ring, and M, N be finitely generated A-modules where* $\operatorname{depth}(M) = m$ *and* $\dim(N) = n$. *Then for $i < m - n$*

$$\operatorname{Ext}^i_A(N, M) = 0.$$

Proof If $n = 0$, then $\mathrm{Supp}_A(N) = \{\mathfrak{m}\}$. By assumption there exists an M-sequence of length m in $\mathfrak{m}$. By Theorem 6.9, $\mathrm{Ext}^i_A(N, M) = 0$ for $i < m$.

Now assume $n > 0$. By prime filtration theorem, N has a filtration

$$N = N_1 \supsetneq N_2 \supsetneq \cdots \supsetneq N_t = 0$$

such that $N_j/N_{j+1} \cong A/\mathfrak{p}_j$ for $j = 1, \ldots, t-1$. To show that $\mathrm{Ext}^i_A(N, M)$ vanishes for $i < m - n$, it is sufficient by the long exact sequence for Ext to show that $\mathrm{Ext}^i_A(A/\mathfrak{p}, M) = 0$ for $i < m - n$. By induction, it suffices to prove this for primes $\mathfrak{p}$ with $\dim(A/\mathfrak{p}) = n$. Pick $x \in \mathfrak{m} - \mathfrak{p}$ and consider the short exact sequence

$$0 \to A/\mathfrak{p} \xrightarrow{x} A/\mathfrak{p} \to A/(\mathfrak{p} + xA) \to 0.$$

Then $\dim(A/(\mathfrak{p} + xA)) = n - 1$. By induction, $\mathrm{Ext}^i_A(A/(\mathfrak{p} + xA), M) = 0$ for $i < m - n + 1$. By the long exact sequence for Ext,

$$\mathrm{Ext}^i_A(A/\mathfrak{p}, M) \xrightarrow{x} \mathrm{Ext}^i_A(A/\mathfrak{p}, M)$$

is an isomorphism for $i < m - n$. Since $x \in \mathfrak{m}$, by Nakayama's Lemma we have $\mathrm{Ext}^i_A(N, M) = 0$ for $i < m - n$. ■

Corollary 6.18 *Let A be a local ring and $N \subseteq M$ finitely generated A-modules. Then* $\dim(N) \geq \mathrm{depth}(M)$.

Proof Since $N \subseteq M$, there is a nonzero map $N \to M$. Thus $\mathrm{Hom}_A(N, M) \neq 0$. The conclusion follows from the previous Theorem. ■

Corollary 6.19 *Let A be a local ring and M be a finitely generated A-module. Then* $\mathrm{depth}(M) \leq \dim(M)$.

Proof Use the previous Corollary with $N = M$. ■

Exercise 6.20 *If A is a local ring and M is a finitely generated A-module with $x_1, \ldots, x_r$ an M-sequence, then*

$$\dim\left(\frac{M}{(x_1, \ldots, x_r)M}\right) = \dim(M) - r.$$

Exercise 6.21 *If A is a Noetherian ring and M is a finitely generated A-module, then*

$$\mathrm{depth}_I(M) \leq \inf_{\mathfrak{p} \supseteq I}\{\mathrm{depth}(M_\mathfrak{p})\}.$$

WARNING 6.22 *There exist local rings A such that* $\mathrm{depth}(A) < \mathrm{depth}(A_\mathfrak{p})$. *As an example consider*

$$A = \left(\frac{k[X, Y, Z]}{(XZ, YZ, Z^2)}\right)_{(X,Y,Z)}.$$

Now we see that the depth of A is zero as every element of $\mathfrak{m} = (X, Y, Z)$ is killed by the nonzero element Z. Moreover if we localize at $\mathfrak{p} = (Y, Z)$, X becomes a unit. So we get

$$A_{\mathfrak{p}} = \left(\frac{k[X,Y,Z]}{(XZ, YZ, Z^2)}\right)_{(Y,Z)} = \left(\frac{k[X,Y,Z]}{(Z)}\right)_{(Y,Z)} = k[X,Y]_{(Y)},$$

a ring of depth 1.

Exercise 6.23 *If $\varphi : R \to A$ is a homomorphism of Noetherian rings, M is a finitely generated A-module, and I is an ideal of R, prove that the following numbers are equal:*

(1) *The length of a maximal M-sequence in I.*

(2) $\operatorname{depth}_{IA}(M)$.

(3) $\inf\{i : \operatorname{Ext}^i_R(R/I, M) \neq 0\}$.

Hint: $\operatorname{Ass}_R(M) = \varphi^{-1}(\operatorname{Ass}_A(M))$.

As an application, suppose one wishes to calculate $\operatorname{depth}_I(M)$ where $I = (x_1, \ldots, x_d)$. Define a map $\varphi : \mathbb{Z}[X_1, \ldots, X_d] \to A$ via $X_i \mapsto x_i$. Then

$$\operatorname{depth}_I(M) = \inf\left\{i \,|\, \operatorname{Ext}^i_{\mathbb{Z}[X_1,\ldots,X_d]}(\mathbb{Z}, M) \neq 0\right\}$$

by the previous exercise. This is often easier to compute.

Minimal Free Resolutions

Let $(A, \mathfrak{m}, k)$ be a local ring and M a finitely generated A-module. We are going to discuss the construction of a minimal free resolution of M. First an exercise:

Exercise 6.24 *Let $(A, \mathfrak{m}, k)$ be a local ring, and M a finitely generated A-module. Show that*

$$\operatorname{rank}_k(M/\mathfrak{m}M) = \textit{the minimum number of generators of } M.$$

Hint: Use Nakayama's Lemma.

We are going to construct a minimal free resolution of M. Set

$$\begin{aligned} \beta_0 &:= \operatorname{rank}_k(M/\mathfrak{m}M), \\ S_1 &:= \operatorname{Ker}(A^{\beta_0} \to M), \end{aligned}$$

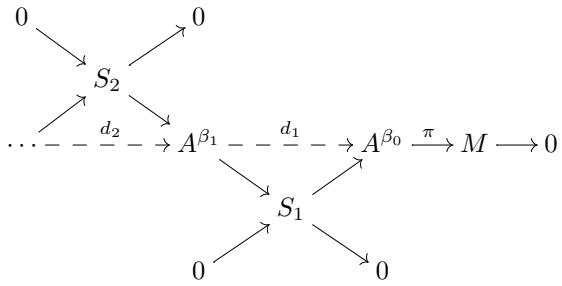
and inductively define

$$\begin{aligned} \beta_i &:= \operatorname{rank}_k(S_i/\mathfrak{m}S_i), \\ S_{i+1} &:= \operatorname{Ker}(A^{\beta_i} \to S_i). \end{aligned}$$

Now we may inductively write the exact sequences:

$$0 \to S_1 \to A^{\beta_0} \to M \to 0,$$
$$0 \to S_{i+1} \to A^{\beta_i} \to S_i \to 0.$$

The integer β_i is called the ith **Betti number** of M and S_i is referred to as the ith **syzygy** of M. The rather mysterious word *syzygy* means *yoke*. After putting the above exact sequences together, we can see why *syzygy* is a good term to use for the S_i's, as each S_i is connecting two free modules via A-module homomorphisms:



The d_i's above are formed by taking the composition of the relevant maps, while π is the canonical surjection. Hence we obtain a **free resolution** of M, that is a long exact sequence of free modules ending at M:

$$\cdots \longrightarrow A^{\beta_3} \xrightarrow{d_3} A^{\beta_2} \xrightarrow{d_2} A^{\beta_1} \xrightarrow{d_1} A^{\beta_0} \xrightarrow{\pi} M \longrightarrow 0$$

Moreover, since at each point we are mapping onto a minimal set of generators, a resolution of this form is called a **minimal free resolution**. Note that the condition that A is local, and hence Noetherian, is critical for this construction. We know that the projective dimension of M is given by:

$$\mathrm{pd}_A(M) = \sup\{i : \mathrm{Tor}_i^A(M, k) \neq 0\}$$

Since the entries of the matrices defining the d_i's in a minimal free resolution live in $\mathfrak{m}$, they become zero maps when tensored by k. Hence

$$\mathrm{Tor}_i^A(M, k) = A^{\beta_i} \otimes_A k.$$

Thus we see that if the projective dimension of M is finite, then the degree of the final nonzero term in the minimal free resolution is equal to $\mathrm{pd}(M)$. Hence a minimal free resolution is truly a resolution of minimal length.

Proposition 6.25 *Let $(A, \mathfrak{m}, k)$ be a local ring, M a finitely generated A-module, and $F_\bullet$ be any free resolution of M where each F_i has finite rank, such that:*

(1) $\pi : F_0 \twoheadrightarrow M$ *and* $\mathrm{Ker}(\pi) \subseteq \mathfrak{m}M$.

(2) $\mathrm{Im}(d_i) = \mathrm{Ker}(d_{i-1}) \subseteq \mathfrak{m}F_{i-1}$.

Then $F_\bullet$ is a minimal free resolution of M.

Proof Consider the exact sequences:

$$0 \to S_1 \to F_0 \to M \to 0$$
$$0 \to S_{i+1} \to F_i \to S_i \to 0$$

Where S_i is the ith syzygy as defined above. Now apply $- \otimes_A k$ to obtain

$$F_0 \otimes_A k \cong M \otimes_A k,$$
$$F_i \otimes_A k \cong S_i \otimes_A k.$$

Consider a basis $\{\overline{b}_1, \ldots, \overline{b}_n\}$ of $M \otimes_A k$. We claim that $\{b_1, \ldots, b_n\}$ is a minimal set of generators for M. Write

$$M = \sum_{i=1}^{n} Ab_i + \mathfrak{m}M$$

Setting $\overline{M} = M/\sum_{i=1}^{n} Ab_i$ we then have $\overline{M} = \mathfrak{m}\overline{M}$, and so by Nakayama's Lemma, we see that $M = \sum_{i=1}^{n} Ab_i$. To see that this is minimal, suppose that it is not, then we have $\sum_{i=1}^{n-1} Ac_i = M$. But now $\{\overline{c}_1, \ldots, \overline{c}_{n-1}\}$ form a basis for $M \otimes_A k$, a contradiction as $M \otimes_A k$ is a free module of rank n. Thus we see that the rank of F_0 is the minimum number of generators of M. Similarly, we see that F_i is a free module of rank equal to the minimum number of generators of S_i. ■

Exercise 6.26 *If A is local, M a finitely generated A-module, and $P_\bullet$ is a free resolution of M, then there exists a minimal free resolution $F_\bullet$ of M such that*

$$P_\bullet = F_\bullet \oplus H_\bullet.$$

Lemma 6.27 *Let $(A, \mathfrak{m})$ be local, $\mathrm{depth}(A) = 0$, M a finitely generated A-module of finite projective dimension. Then M is free.*

Proof Take a minimal free resolution of M

$$0 \to A^{t_n} \xrightarrow{\varphi_n} A^{t_{n-1}} \xrightarrow{\varphi_{n-1}} \cdots \xrightarrow{\varphi_1} A^{t_0} \to M \to 0,$$

where $\varphi_n = (a_{ij})$ for $a_{ij} \in \mathfrak{m}$. Since $\mathrm{depth}(A) = 0$, for all $x \in \mathfrak{m}$, there exists $a \in A$ with $xa = 0$. Thus $\mathrm{Ker}(\varphi_n) \neq 0$ since all entries in (a_{ij}) are in the maximal ideal $\mathfrak{m}$. Yet by exactness of the above sequence, $\mathrm{Ker}(\varphi_n) = 0$. Therefore $n = 0$ and M is free. ■

Lemma 6.28 *Let A be a local ring and let M be a finitely generated A-module with finite projective dimension. Suppose $x \in \mathfrak{m}$ is a nonzerodivisor on A and on M. Then*

$$\mathrm{pd}_A(M) = \mathrm{pd}_{A/xA}(M/xM).$$

Proof Take a minimal free resolution of M

$$0 \to A^{t_n} \to A^{t_{n-1}} \to \cdots \to A^{t_0} \to M \to 0.$$

Observe that since $A \xrightarrow{x} A$ is injective, tensoring by $\overline{A} = A/xA$ yields the complex

$$0 \to \overline{A}^{t_n} \to \overline{A}^{t_{n-1}} \to \cdots \to \overline{A}^{t_0} \to \overline{M} \to 0.$$

The homology of the truncated complex above is clearly $\operatorname{Tor}_i^A(M, \overline{A})$. Since x is a nonzerodivisor on A, $\operatorname{pd}_A(\overline{A}) = 1$, so $\operatorname{Tor}_i^A(M, \overline{A})$ vanish for $i > 1$. Furthermore, $\operatorname{Tor}_1^A(M, \overline{A}) = \operatorname{Ker}(M \xrightarrow{x} M) = (0)$ by assumption. Thus the above complex is exact and so forms a minimal free resolution of $\overline{M}$ over $\overline{A}$. Hence $\operatorname{pd}_A(M) = \operatorname{pd}_{A/xA}(M/xM)$. ■

Theorem 6.29 (Auslander-Buchsbaum) *Let A be local and M be a finitely generated A-module with finite projective dimension. Then*

$$\operatorname{pd}_A(M) + \operatorname{depth}(M) = \operatorname{depth}(A).$$

Proof We induct on $\operatorname{pd}(M)\operatorname{depth}(A)$. In the base case, $\operatorname{pd}(M)\operatorname{depth}(A) = 0$. If $\operatorname{pd}(M) = 0$, then M is free. Hence $\operatorname{depth}(M) = \operatorname{depth}(R)$ and we are done. Similarly if $\operatorname{depth}(A) = 0$ then by Lemma 6.27 M is free. Hence $\operatorname{pd}(M) = 0$ and $\operatorname{depth}(M) = \operatorname{depth}(A) = 0$.

Now suppose $\operatorname{pd}(M)\operatorname{depth}(A) > 0$.

Case 1: $\operatorname{depth}(M) > 0$.
Since $\operatorname{depth}(M) > 0$ and $\operatorname{depth}(A) > 0$ we have,

$$\mathfrak{m} \not\subseteq \bigcup_{\mathfrak{p} \in \operatorname{Ass}_A(A)} \mathfrak{p} \quad \text{and} \quad \mathfrak{m} \not\subseteq \bigcup_{\mathfrak{q} \in \operatorname{Ass}_A(M)} \mathfrak{q}.$$

So by prime avoidance

$$\mathfrak{m} \not\subseteq \bigcup_{\mathfrak{p} \in \operatorname{Ass}_A(M) \cup \operatorname{Ass}_A(A)} \mathfrak{p}.$$

So there is $x \in \mathfrak{m}$ that is a nonzerodivisor on both A and M. By the previous lemma, $\operatorname{pd}_A(M) = \operatorname{pd}_{A/xA}(M/xM)$. Clearly $\operatorname{depth}(M/xM) = \operatorname{depth}(M) - 1$ and $\operatorname{depth}(A/xA) = \operatorname{depth}(A) - 1$. Since

$$\operatorname{pd}_{A/xA}(M/xM)\operatorname{depth}(A/xA) < \operatorname{pd}(M)\operatorname{depth}(A),$$

by induction we have

$$\operatorname{pd}_{A/xA}(M/xM) + \operatorname{depth}(M/xM) = \operatorname{depth}(A/xA).$$

Therefore

$$\operatorname{pd}_A(M) + \operatorname{depth}(M) = \operatorname{depth}(A).$$

Case 2: $\operatorname{depth}(M) = 0$.
Take an exact sequence

$$0 \to N \to F \to M \to 0,$$

where F is a free A-module. Since $\operatorname{depth}(A) > 0$, we have $\operatorname{depth}(N) = \operatorname{depth}(M) + 1$ by Corollary 6.11. Clearly $\operatorname{pd}(N) = \operatorname{pd}(M) - 1$. Since

$$\operatorname{pd}_A(N) \operatorname{depth}(A) < \operatorname{pd}(M) \operatorname{depth}(A),$$

by induction we have

$$\operatorname{pd}_A(N) + \operatorname{depth}(N) = \operatorname{depth}(A).$$

Hence

$$\operatorname{pd}_A(M) + \operatorname{depth}(M) = \operatorname{depth}(A).$$

■

Corollary 6.30 *If A is a local ring, M a finitely generated A-module and $\operatorname{pd}_A(M) < \infty$, then $\operatorname{depth}(M) = \operatorname{depth}(A)$ if and only if M is free.*

Proof Over a local ring, $\operatorname{pd}_A(M) = 0$ if and only if M is projective if and only if M is free. ■

Corollary 6.31 *If A is a regular local ring with $\dim(A) = n$, then a finitely generated A-module M is free if and only if $\operatorname{depth}(M) = n$.*

Proof Over a regular local ring, all finitely generated modules have finite projective dimension. So we are done by the previous corollary. ■

6.2 The Koszul Complex

Construction of the Koszul Complex

Given a ring A and $x \in A$, then $K_\bullet(x)$ denotes the **Koszul complex** of A generated by x. We define $K_\bullet(x)$ as follows

$$K_0(x) := A$$
$$K_1(x) := A$$

and we have

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K_1(x) & \xrightarrow{d_1} & K_0(x) & \longrightarrow & 0 \\ & & \| & & \| & & \\ 0 & \longrightarrow & A & \xrightarrow{x} & A & \longrightarrow & 0 \end{array}$$

where we define d_1 to be multiplication by x. We can now define

$$K_\bullet(x; M) := K_\bullet(x) \otimes_A M.$$

Definition If $X_\bullet$ and $Y_\bullet$ are complexes with

$$X_n \xrightarrow{d_n^X} X_{n-1},$$
$$Y_n \xrightarrow{d_n^Y} Y_{n-1},$$

then we can form a complex $(X_\bullet \otimes Y_\bullet)_\bullet$ defined via

$$(X_\bullet \otimes Y_\bullet)_n := \bigoplus_{p+q=n} X_p \otimes Y_q$$

with the maps

$$(X_\bullet \otimes Y_\bullet)_n \xrightarrow{d_n} (X_\bullet \otimes Y_\bullet)_{n-1}$$

being defined as follows:

$$d_n(x_p \otimes y_q) := d_p^X(x_p) \otimes y_q + (-1)^p x_p \otimes d_q^Y(y_q)$$

where $p + q = n$.

Definition Given a ring A, $x_1, \ldots, x_n \in A$, and M a finitely generated A-module, the **Koszul complex** of A generated by $x_1, \ldots, x_n$ is

$$K_\bullet(x_1, \ldots, x_n) := K_\bullet(x_1) \otimes K_\bullet(x_2) \otimes \cdots \otimes K_\bullet(x_n).$$

Likewise, the Koszul complex of M generated by $x_1, \ldots, x_n$ is defined by

$$K_\bullet(x_1, \ldots, x_n; M) := K_\bullet(x_1, \ldots, x_n) \otimes_A M.$$

From the definition of the Koszul complex we see that $K_p(\mathbf{x})$ is a free A-module. Explicitly, we see that $K_0(x_1, \ldots, x_n) = A$ and for $p \neq 0$, we have

$$K_p(x_1, \ldots, x_n) = \bigoplus_{1 \leq i_1 < \cdots < i_p \leq n} Ae_{i_1} \otimes \cdots \otimes Ae_{i_p}$$

and moreover that

$$d_p(e_{i_1} \otimes \cdots \otimes e_{i_p}) = \sum_{k=1}^{p} (-1)^{k+1} x_{i_k} e_{i_1} \otimes \cdots \otimes \widehat{e}_{i_k} \otimes \cdots \otimes e_{i_p},$$

where the $\widehat{e}_{i_k}$ denotes that the element e_{i_k} is omitted.

We may also write the differential in the Koszul complex as a matrix. If d_p^n is the pth differential in a Koszul complex of n elements, and I denotes the $\binom{n}{p} \times \binom{n}{p}$ identity matrix, then it is not hard to show:

$$d_{p+1}^{n+1} = \begin{bmatrix} d_{p+1}^n & (-1)^p x_{n+1} I \\ 0 & d_p^n \end{bmatrix}$$

Exercise 6.32 *Let $x_1, \ldots, x_n \in A$. Let us construct the first several Koszul complexes. Starting with $K_\bullet(x_1)$, which we already know has the form:*

$$0 \to A \xrightarrow{\begin{bmatrix} x_1 \end{bmatrix}} A \to 0.$$

Using the notation above, we have

$$d_1^1 = \begin{bmatrix} x_1 \end{bmatrix},$$

and d_i^1 is the empty matrix for $i > 1$.

By above, we have

$$d_1^2 = \begin{bmatrix} d_1^1 & (-1)^0 x_2 I \end{bmatrix} = \begin{bmatrix} x_1 & x_2 \end{bmatrix}$$

and

$$d_2^2 = \begin{bmatrix} (-1)^1 x_2 I \\ d_1^1 \end{bmatrix} = \begin{bmatrix} -x_2 \\ x_1 \end{bmatrix}.$$

So $K_\bullet(x_1, x_2)$ is the complex

$$0 \to A \xrightarrow{\begin{bmatrix} -x_2 \\ x_1 \end{bmatrix}} A^2 \xrightarrow{\begin{bmatrix} x_1 & x_2 \end{bmatrix}} A \to 0.$$

Going one step further we have

$$d_1^3 = \begin{bmatrix} d_1^2 & (-1)^0 x_3 I \end{bmatrix} = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix}$$

$$d_2^3 = \begin{bmatrix} d_2^2 & (-1)^1 x_3 I \\ 0 & d_1^2 \end{bmatrix} = \begin{bmatrix} -x_2 & -x_3 & 0 \\ x_1 & 0 & -x_3 \\ 0 & x_1 & x_2 \end{bmatrix},$$

and

$$d_3^3 = \begin{bmatrix} (-1)^2 x_3 I \\ d_2^2 \end{bmatrix} = \begin{bmatrix} x_3 \\ -x_2 \\ x_1 \end{bmatrix}.$$

So $K_\bullet(x_1, x_2, x_3)$ is the complex

$$0 \to A \xrightarrow{\begin{bmatrix} x_3 \\ -x_2 \\ x_1 \end{bmatrix}} A^3 \xrightarrow{\begin{bmatrix} -x_2 & -x_3 & 0 \\ x_1 & 0 & -x_3 \\ 0 & x_1 & x_2 \end{bmatrix}} A^3 \xrightarrow{\begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix}} A \to 0.$$

At this point we may regroup, and note if $F = \bigoplus_{i=1}^n Ae_i$, then

$$K_p(x_1, \ldots, x_n) = \bigwedge^p F$$

where $\bigwedge^p F$ denotes the pth exterior power of the free A-module F. Thus we see that:

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & K_n(\mathbf{x}) & \longrightarrow & K_{n-1}(\mathbf{x}) & \longrightarrow & \ldots & \longrightarrow & K_1(\mathbf{x}) & \longrightarrow & K_0(\mathbf{x}) & \longrightarrow & 0 \\
 & & \| & & \| & & & & \| & & \| & & \\
0 & \longrightarrow & A & \longrightarrow & A^{\binom{n}{n-1}} & \longrightarrow & \ldots & \longrightarrow & A^{\binom{n}{1}} & \longrightarrow & A & \longrightarrow & 0
\end{array}$$

Koszul Homology

A common notational convenience is to set

$$H_p(\mathbf{x}) := H_p(K_\bullet(\mathbf{x})) \qquad \text{and} \qquad H_p(\mathbf{x}; M) := H_p(K_\bullet(\mathbf{x}; M)).$$

From the construction of the Koszul complex we have that:

$$\begin{aligned} H_0(K_\bullet(\mathbf{x})) &= A/\mathbf{x}A, & H_n(K_\bullet(\mathbf{x})) &= (0 :_A \mathbf{x}), \\ H_0(K_\bullet(\mathbf{x}; M)) &= M/\mathbf{x}M, & H_n(K_\bullet(\mathbf{x}; M)) &= (0 :_M \mathbf{x}). \end{aligned}$$

Proposition 6.33 (Serre) *Let $L_\bullet$ be a complex of A-modules and let $x \in A$. Then we have an exact sequence*

$$0 \to \frac{H_p(L_\bullet)}{xH_p(L_\bullet)} \to H_p(L_\bullet \otimes K_\bullet(x)) \to (0 :_{H_{p-1}(L_\bullet)} x) \to 0$$

for all p.

Proof Consider the complex $L_\bullet \otimes K_\bullet(x)$. Let $d_p : L_p \to L_{p-1}$ be the differential map in $L_\bullet$. In $L_\bullet \otimes K_\bullet(x)$, the pth degree part is

$$(L_\bullet \otimes K_\bullet(x))_p = L_p \oplus L_{p-1},$$

and the differential map is

$$\begin{aligned} d'_p : L_p \oplus L_{p-1} &\to L_{p-1} \oplus L_{p-2}, \\ (u, v) &\mapsto (d_p(u) + (-1)^{p-1}xv, d_{p-1}(v)). \end{aligned}$$

We have then the following exact sequence of complexes

$$\begin{array}{ccccccccc} & & \vdots & & \vdots & & \vdots & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & L_p & \longrightarrow & L_p \oplus L_{p-1} & \longrightarrow & L_{p-1} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_p} & & \downarrow{\scriptstyle d'_p} & & \downarrow{\scriptstyle d_{p-1}} & & \\ 0 & \longrightarrow & L_{p-1} & \longrightarrow & L_{p-1} \oplus L_{p-2} & \longrightarrow & L_{p-2} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & \vdots & & \vdots & & \vdots & & \end{array}$$

By the corresponding long exact sequence of homology we get that

$$H_p(L_\bullet) \xrightarrow{\pm x} H_p(L_\bullet) \to H_p(L \otimes K_\bullet(x)) \to H_{p-1}(L_\bullet) \xrightarrow{\pm x} H_{p-1}(L_\bullet)$$

is exact for all $p > 0$. Hence we get the

$$0 \to \frac{H_p(L_\bullet)}{xH_p(L_\bullet)} \to H_p(L_\bullet \otimes K_\bullet(x)) \to (0 :_{H_{p-1}(L_\bullet)} x) \to 0$$

is exact for $p > 0$. ■

Corollary 6.34 *If $F_\bullet \to M \to 0$ is a free resolution of M, and x is a nonzerodivisor on M, then*

$$F_\bullet \otimes K_\bullet(x) \to M/xM \to 0$$

is a free resolution of M/xM over A.

Corollary 6.35 *If $x_1, \ldots, x_n \in A$, where A is a local ring, and M an A-module, then the following sequence is exact*

$$0 \to \frac{H_p(x_1, \ldots, x_{n-1}; M)}{x_n H_p(x_1, \ldots, x_{n-1}; M)} \to H_p(x_1, \ldots, x_n; M) \to (0 :_{H_{p-1}(x_1, \ldots, x_{n-1}; M)} x_n) \to 0.$$

Proof Take $L_\bullet = K_\bullet(x_1, \ldots, x_{n-1})$ in the above proposition. ■

Corollary 6.36 *If $x_1, \ldots, x_n$ is an M-sequence, then $H_p(\mathbf{x}; M) = 0$ for $p > 0$.*

Proof Suppose $n = 1$. Then x is a nonzerodivisor on M. Hence

$$H_1(x_1; M) = (0 :_M x_1) = 0,$$

and we are done.

Now assume the result is true for M-sequences of length less than n. Then

$$H_p(x_1, \ldots, x_{n-1}; M) = 0$$

for $p > 0$ by induction. So by the previous corollary $H_p(x_1, \ldots, x_n) = 0$ for $p > 1$ and

$$H_1(x_1, \ldots, x_n; M) = (0 :_{H_0(x_1, \ldots, x_{n-1}; M)} x_n) = (0 :_{M/(x_1, \ldots, x_{n-1})M} x_n) = 0,$$

since x_n is a nonzerodivisor on $M/(x_1, \ldots, x_{n-1})M$. ■

Corollary 6.37 *If $x_1, \ldots, x_n$ is an A-sequence, then $K_\bullet(\mathbf{x})$ is a free resolution of $A/(\mathbf{x})$.*

Remark Take an A-sequence $x_1, \ldots, x_n$, M an A-module and set:

$$B = \mathbb{Z}[X_1, \ldots, X_n] \to A$$
$$X_i \mapsto x_i$$

Since $X_1, \ldots, X_n$ form a B-sequence, $K_\bullet(\mathbf{X}; B)$ is a free resolution of $B/\mathbf{X}$. Moreover,

$$K_\bullet(\mathbf{X}; B) \otimes_B A = K_\bullet(\mathbf{x}; A)$$

and hence

$$K_\bullet(\mathbf{X}; B) \otimes_B M = K_\bullet(\mathbf{x}; M).$$

Thus

$$H_p(\mathbf{x}; M) = \operatorname{Tor}_B^p(B/\mathbf{X}, M).$$

From this we see that $\mathbf{x} + \operatorname{Ann}_A(M)$ kills $H_p(\mathbf{x}; M)$.

Proposition 6.38 *Let A be Noetherian, M a finitely generated A-module, and let $x_1, \ldots, x_n \in \mathfrak{J}(A)$, the Jacobson radical of A. The following are equivalent:*

(1) *$x_1, \ldots, x_n$ is an M-sequence.*

(2) *$H_p(\mathbf{x}; M) = 0$ for $p > 0$.*

(3) *$H_1(\mathbf{x}; M) = 0$.*

Proof (1) $\Rightarrow$ (2) $\Rightarrow$ (3) is clear.

(3) $\Rightarrow$ (1) For $n = 1$, we have that $H_1(x_1; M) = (0 :_M x_1) = 0$. Thus x_1 is a nonzerodivisor on M. Now suppose $n > 1$. By Corollary 6.35 we have the following short exact sequence:

$$0 \to \frac{H_1(x_1, \ldots, x_{n-1}; M)}{x_n H_1(x_1, \ldots, x_{n-1}; M)} \to H_1(x_1, \ldots, x_n; M) \to (0 :_{H_0(x_1, \ldots, x_{n-1}; M)} x_n) \to 0.$$

By assumption,

$$H_1(x_1, \ldots, x_n; M) = H_1(\mathbf{x}; M) = 0.$$

Thus

$$\frac{H_1(x_1, \ldots, x_{n-1}; M)}{x_n H_1(x_1, \ldots, x_{n-1}; M)} = 0 \quad \text{and} \quad (0 :_{H_0(x_1, \ldots, x_{n-1}; M)} x_n) = 0.$$

Since $x_n \in \mathfrak{J}(A)$ and since $H_1(x_1, \ldots, x_{n-1}; M)$ is a finitely generated A-module, $H_1(x_1, \ldots, x_{n-1}; M) = 0$ by Nakayama's Lemma. So by induction, $x_1, \ldots, x_{n-1}$ is an M-sequence. Since

$$(0 :_{H_0(x_1, \ldots, x_{n-1}; M)} x_n) = 0,$$

x_n is a nonzerodivisor on $M/(x_1, \ldots, x_{n-1})M$. Hence $x_1, \ldots, x_n$ is an M-sequence. ■

Koszul Cohomology

We start this section off with an exercise!

Exercise 6.39 *If P is a finitely generated projective A-module, and M is any A-module, then show that*

$$\mathrm{Hom}_A(P, M) \cong \mathrm{Hom}_A(P, A) \otimes_A M.$$

To define Koszul cohomology, we must first have a cochain complex. Define:

$$K^\bullet(\mathbf{x}; A) := \mathrm{Hom}_A(K_\bullet(\mathbf{x}; A), A),$$
$$K^\bullet(\mathbf{x}; M) := \mathrm{Hom}_A(K_\bullet(\mathbf{x}; A), M).$$

By the exercise above we have that

$$K^\bullet(\mathbf{x}; M) \cong K^\bullet(\mathbf{x}; A) \otimes_A M.$$

There is a strong connection between $K_\bullet(\mathbf{x})$ and $K^\bullet(\mathbf{x})$, namely

$$K_p(\mathbf{x}) \cong K^{n-p}(\mathbf{x}).$$

To see this, first note that from the symmetry of the Koszul complex we can see that

$$\begin{aligned} K_p(\mathbf{x}) \otimes_A K_{n-p}(\mathbf{x}) \cong K_n(\mathbf{x}) &\cong A, \\ u \otimes v &\mapsto u \wedge v. \end{aligned}$$

Now we may define an isomorphism

$$\varphi_p : K_p(\mathbf{x}) \to K^{n-p}(\mathbf{x}) = \mathrm{Hom}_A(K_{n-p}(\mathbf{x}), A)$$

via

$$e_{i_1} \wedge \cdots \wedge e_{i_p} \mapsto \pm\{v \mapsto (e_{i_1} \wedge \cdots \wedge e_{i_p}) \wedge v\} = \pm(j_1 \wedge \cdots \wedge j_{p-n})^*,$$

where $(-)^*$ signifies the application of the $\mathrm{Hom}_A(-, A)$ functor and the the sign comes from the sign of the permutation

$$\begin{pmatrix} 1 & 2 & \dots & p & p+1 & \dots & n \\ i_1 & i_2 & \dots & i_p & j_1 & \dots & j_{n-p} \end{pmatrix}.$$

By our choice of φ_p, it can be shown that

$$\begin{array}{ccc} K_p(\mathbf{x}) & \xrightarrow{\varphi_p} & K^{n-p}(\mathbf{x}) \\ {\scriptstyle d_p}\downarrow & & \downarrow{\scriptstyle d^*_{n-p+1}} \\ K_{p-1}(\mathbf{x}) & \xrightarrow{\varphi_{p-1}} & K^{n-p+1}(\mathbf{x}) \end{array}$$

commutes, and so we have that

$$H_p(\mathbf{x}; M) \cong H^{n-p}(\mathbf{x}; M).$$

Moreover,

$$H^0(\mathbf{x}; M) \cong H_n(\mathbf{x}; M) = (0 :_M \mathbf{x})$$

and

$$H^n(\mathbf{x}; M) \cong H_0(\mathbf{x}; M) = M/\mathbf{x}M.$$

The Koszul Complex and Depth

Let A be Noetherian, I an ideal of A, M a finitely generated A-module. We can use the Koszul complex to study $\mathrm{depth}_I(M)$. Recall

$$\mathrm{depth}_I(M) = \inf\{i : \mathrm{Ext}^i_A(A/I, M) \neq 0\}.$$

Suppose that $I = (x_1, \ldots, x_n)$ and consider

$$B = \mathbb{Z}[X_1, \ldots, X_n] \to A,$$
$$X_i \mapsto x_i.$$

Then by a previous exercise,

$$\begin{aligned}\operatorname{depth}_I(M) &= \inf\{i : \operatorname{Ext}^i_B(B/\mathbf{X}, M) \neq 0\},\\ &= \inf\{i : \operatorname{Ext}^i_B(\mathbb{Z}, M) \neq 0\}.\end{aligned}$$

Since $K_\bullet$ is a free resolution of $B/\mathbf{X} = \mathbb{Z}$ over B, we have

$$\begin{aligned}\operatorname{depth}_I(M) &= \inf\{i : H^i(\mathbf{x}; M) \neq 0\},\\ &= \inf\{i : H_{n-i}(\mathbf{x}; M) \neq 0\},\\ &= n - \sup\{i : H_i(\mathbf{x}; M) \neq 0\}.\end{aligned}$$

6.3 Cohen-Macaulay Modules and Rings

Definition If A is a local ring and M finitely generated A-module, then M is called **Cohen-Macaulay** if $\dim(M) = \operatorname{depth}(M)$. A is called **Cohen-Macaulay** if it is Cohen-Macaulay as a module over itself.

Theorem 6.40 (Properties of Cohen-Macaulay Modules) *If $(A, \mathfrak{m})$ is a local ring and M is a finitely generated A-module, then the following are true:*

(1) *M is Cohen-Macaulay implies that for every prime ideal $\mathfrak{p} \in \operatorname{Ass}_A(M)$, $\dim(A/\mathfrak{p}) = \operatorname{depth}(M)$. Note that this shows us that A has no embedded primes.*

(2) *Given a nonzero $x \in \mathfrak{m}$ such that x is a nonzerodivisor on M, M is Cohen-Macaulay if and only if M/xM is Cohen-Macaulay.*

(3) *M is Cohen-Macaulay if and only if $M_\mathfrak{p}$ is Cohen-Macaulay for every $\mathfrak{p} \in \operatorname{Supp}(M)$. In this case, $\operatorname{depth}_\mathfrak{p}(M) = \operatorname{depth}(M_\mathfrak{p})$.*

(4) *M is Cohen-Macaulay if and only if every system of parameters of M form a M-sequence if and only if some system of parameters form a M-sequence.*

(5) *Let $x_1, \ldots, x_n$ be a system of parameters of M. M is Cohen-Macaulay if and only if*

$$H_1(\mathbf{x}; M) = 0$$

if and only if

$$M/\mathbf{x}M[X_1, \ldots, X_n] \to \bigoplus_{t=0}^{\infty} \frac{I^t M}{I^{t+1} M}$$

is an isomorphism, where $I = (x_1, \ldots, x_n)$, if and only if

$$e_I(M) = \lambda(M/IM)$$

where $e_I(M)$ is the Hilbert-Samuel multiplicity of M with respect to I.

(6) *If M is Cohen-Macaulay and $\mathfrak{p} \in \operatorname{Supp}(M)$, then*

$$\dim(M_\mathfrak{p}) + \dim(A/\mathfrak{p}) = \dim(M).$$

(7) *If M is Cohen-Macaulay and $\mathfrak{p}, P \in \operatorname{Supp}(M)$, then any two saturated chains from*

$$\mathfrak{p} \subsetneq \cdots \subsetneq P$$

have the same length. In other words, $A/\operatorname{Ann}_A(M)$ is catenary.

Proof (1) For all $\mathfrak{p} \in \operatorname{Ass}_A(M)$, one has

$$\operatorname{depth}(M) \leq \dim(A/\mathfrak{p}) \leq \dim(M).$$

Since M is Cohen-Macaulay, $\dim(M) = \operatorname{depth}(M)$. Hence, $\dim(A/\mathfrak{p}) = \dim(M)$ for all $\mathfrak{p} \in \operatorname{Ass}_A(M)$ and so M has no embedded primes.

(2) Let x be a nonzerodivisor on M. Then

$$\dim(M/xM) = \dim(M) - 1 \quad \text{and} \quad \operatorname{depth}(M/xM) = \operatorname{depth}(M) - 1.$$

Hence M is Cohen-Macaulay if and only if M/xM is Cohen-Macaulay.

(3) One can show that for any finitely generated module M,

$$\operatorname{depth}_\mathfrak{p}(M) \leq \operatorname{depth}(M_\mathfrak{p}) \leq \dim(M_\mathfrak{p}).$$

We show that $\operatorname{depth}_\mathfrak{p}(M) = \dim(M_\mathfrak{p})$ if and only if M is Cohen-Macaulay. That this condition is sufficient to force M to be Cohen-Macaulay is clear, so assume M is Cohen-Macaulay. We prove the above equality by induction on $\operatorname{depth}_\mathfrak{p}(M)$. If $\operatorname{depth}_\mathfrak{p}(M) = 0$, then $\mathfrak{p} \in \operatorname{Ass}_A(M)$. Since M has no embedded primes, $\dim(M_\mathfrak{p}) = 0$. Now assume $\operatorname{depth}_\mathfrak{p}(M) > 0$. Then let $x \in \mathfrak{p}$ be a nonzerodivisor on M. Then

$$\operatorname{depth}_\mathfrak{p}(M/xM) = \operatorname{depth}_p(M) - 1 \quad \text{and} \quad \dim(M_p/xM_p) = \dim(M_p) - 1.$$

Since M/xM is Cohen-Macaulay by (2), we are done by induction.

(4) Suppose M is Cohen-Macaulay and let $x_1, \ldots, x_n$ be a system of parameters for M. Then for $1 \leq i \leq n$,

$$\dim(M/(x_1, \ldots, x_i)M) = \dim(M) - i.$$

Observe that it suffices to show that if $x \in \mathfrak{m}$ and $\dim(M/xM) = \dim(M) - 1$, then x is regular on M. If $x \in \mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Ass}_A(M)$, then $\dim(M) = \dim(M/xM)$ since M has no embedded primes. Therefore

$$x \notin \bigcup_{\mathfrak{p} \in \operatorname{Ass}_A(m)} \mathfrak{p}.$$

It follows that x is a nonzerodivisor on M and that $M/xM \neq 0$. Hence x is regular on M and we are done. That is, all systems of parameters are M-regular sequences.

Now suppose M is Cohen-Macaulay and that $x_1, \ldots, x_n$ is a system of parameters that is also M-regular. Then

$$\dim(M) = s(M) \leq \operatorname{depth}(M) \leq \dim(M).$$

Hence $\dim(M) = \operatorname{depth}(M)$ and so M is Cohen-Macaulay.

(5) Let $x_1, \ldots, x_n$ be a system of parameters for M. Then $H_1(\mathbf{x}; M) = 0$ implies that $x_1, \ldots, x_n$ forms an M-regular sequence. Thus $\operatorname{depth}(M) = \dim(M)$. In particular, $x_1, \ldots, x_n$ is an M-quasi-regular sequence. Hence

$$M/IM[X_1, \ldots, X_n] \cong \bigoplus I^t M/I^{t+1}M.$$

By Serre's Theorem on dimension, the previous isomorphism is equivalent to the equality

$$e_I(M) = \lambda(M/IM).$$

(6) Suppose M is Cohen Macaulay. If $\dim(M) = 0$, there is nothing to prove. If $\dim(M) > 0$, then if $\mathfrak{p} \in \operatorname{Ass}_A(M)$ we have $\mathfrak{p} \in \operatorname{Supp}(M)$. Hence $\dim(M_\mathfrak{p}) = 0$ and $\dim(A/\mathfrak{p}) = \dim(M)$, since M has no embedded primes. If $\mathfrak{p} \notin \operatorname{Ass}_A(M)$, then there exists a nonzerodivisor $x \in \mathfrak{p}$ on M. Thus

$$\dim(M/xM) = \dim(M) - 1 \quad \text{and} \quad \dim(M_\mathfrak{p}/xM_\mathfrak{p}) = \dim(M_\mathfrak{p}) - 1.$$

The result then follows from induction on $\dim(M)$.

(7) Suppose M is Cohen-Macaulay and let $\mathfrak{p} \subseteq \mathfrak{p}'$ be two primes in $\operatorname{Supp}(M)$. Let

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

be a saturated chain of prime ideals. We'll prove that

$$\dim(A/\mathfrak{p}) - \dim(A/\mathfrak{p}') = r.$$

It is enough to show that

$$\dim(A/\mathfrak{p}_0) - \dim(A/\mathfrak{p}_1) = 1.$$

By (6),

$$\dim(A_{\mathfrak{p}_0}) + \dim(A/\mathfrak{p}_0) = \dim(A) \quad \text{and} \quad \dim(A_{\mathfrak{p}_1}) + \dim(A/\mathfrak{p}_1) = \dim(A).$$

Also by (6),

$$\dim(A_{\mathfrak{p}_0}) + \dim(A_{\mathfrak{p}_1}/\mathfrak{p}_0 A_{\mathfrak{p}_1}) = \dim(A_{\mathfrak{p}_1}).$$

Since there are no primes strictly between $\mathfrak{p}_0$ and $\mathfrak{p}_1$, $\dim(A_{\mathfrak{p}_1}/\mathfrak{p}_0 A_{\mathfrak{p}_1}) = 1$. Thus

$$\dim(A/\mathfrak{p}_0) - \dim(A/\mathfrak{p}_1) = \dim(A_{\mathfrak{p}_1}) - \dim(A_{\mathfrak{p}_0}) = \dim(A_{\mathfrak{p}_1}/\mathfrak{p}_0 A_{\mathfrak{p}_1}) = 1.$$

■

Theorem 6.41 (Properties of local Cohen-Macaulay Rings) *If $(A, \mathfrak{m})$ is a local ring, then the following are true:*

(1) *A is Cohen-Macaulay implies that for every prime ideal $\mathfrak{p} \in \mathrm{Ass}_A(A)$, $\dim(A/\mathfrak{p}) = \mathrm{depth}(A)$. Note that this shows us that A has no embedded primes.*

(2) *Given a nonzero $x \in \mathfrak{m}$ such that x is a nonzerodivisor on A, A is Cohen-Macaulay if and only if A/x is Cohen-Macaulay.*

(3) *A is Cohen-Macaulay if and only if for every $A_\mathfrak{p}$ is Cohen-Macaulay for every $\mathfrak{p} \in \mathrm{Spec}(A)$. Moreover, $\mathrm{depth}_\mathfrak{p}(A) = \mathrm{depth}(A_\mathfrak{p})$.*

(4) *If A is Cohen Macaulay, $\mathrm{depth}_I(A) = \mathrm{ht}(I)$.*

(5) *A is Cohen-Macaulay if and only if every system of parameters of A form a A-sequence if and only if some system of parameters form a A-sequence.*

(6) *Let $x_1, \ldots, x_n$ be a system of parameters of A. A is Cohen-Macaulay if and only if*

$$H_1(\mathbf{x}) = 0$$

if and only if

$$A/\mathbf{x}[X_1, \ldots, X_n] \to \bigoplus_{t=0}^{\infty} \frac{I^t}{I^{t+1}}$$

is an isomorphism, where $I = (x_1, \ldots, x_n)$, if and only if

$$e_I(A) = \lambda(A/I)$$

where $e_I(A)$ is the Hilbert-Samuel multiplicity of A with respect to I.

(7) *If A is Cohen-Macaulay and I is an ideal of A, then*

$$\mathrm{ht}(I) + \dim(A/I) = \dim(A).$$

(8) *If A is Cohen-Macaulay and $\mathfrak{p}, P \in \mathrm{Spec}(A)$, then any two saturated chains from*

$$\mathfrak{p} \subsetneq \cdots \subsetneq P$$

have the same length.

Proof We leave it to the reader to translate the proof from the module case. ■

Corollary 6.42 *Suppose that A is the image of local Cohen-Macaulay ring. Then any saturated chain between two prime ideals $\mathfrak{p} \subsetneq P$ have the same length; that is, A is catenary.*

Corollary 6.43 *Suppose that A is a local domain which is the image of a local Cohen-Macaulay ring. Then for all $\mathfrak{p} \in \operatorname{Spec}(A)$,*

$$\operatorname{ht}(\mathfrak{p}) + \dim(A/\mathfrak{p}) = \dim(A).$$

Note that if A is a regular local ring, then $\mathfrak{m}$ is generated by an A-sequence. Hence A is Cohen-Macaulay. Consider for an example

$$B = k[\![X_1, \ldots, X_n]\!]$$

Letting $A = B/\mathfrak{q}$ where $\mathfrak{q} \in \operatorname{Spec}(B)$, we see that A satisfies the above corollary as follows. By Cohen's Structure Theorem, any complete local ring A has the form $B/\mathfrak{q}$ where

$$B = K[\![X_1, \ldots, X_n]\!]$$

and K is a field or a DVR. Hence any complete local domain satisfies the above corollary.

Theorem 6.44 *If $\varphi : A \to B$ is a homomorphism of Noetherian rings and M is a finitely generated A-module, N is an A-flat finitely generated B-module, then*

(1) *For every $P \in \operatorname{Spec}(B)$,*

$$\varphi^{-1}\left(\operatorname{Ass}_B(N/PN)\right) = \begin{cases} \varnothing & \text{if } N/PN = 0, \\ \mathfrak{p} & \text{if } N/PN \neq 0, \end{cases}$$

where $\mathfrak{p} = \varphi^{-1}(P)$.

(2) $\operatorname{Ass}_B(M \otimes_A N) = \bigcup_{\mathfrak{p} \in \operatorname{Ass}_A(M)} \operatorname{Ass}_B(N/PN)$

Proof (1) Suppose N is A-flat and let P be a prime in A. Suppose $N/PN \neq 0$. Then N/PN is A/P-flat. Since A/P is a domain, for every $a \in A - P$ the map $A/P \xrightarrow{a} A/P$ is injective. Hence $N/PN \xrightarrow{a} N/PN$ is injective. Hence if $\mathfrak{p} \in \operatorname{Ass}_B(N/PN)$, then $\varphi^{-1}(\mathfrak{p}) = P$.

(2) ($\supseteq$) Suppose $P \in \operatorname{Ass}_A(M)$. Then we have an injection $A/P \hookrightarrow M$. Since N is A-flat, we have an injection $N/PN = A/P \otimes_A N \hookrightarrow M \otimes_A N$. Hence $\operatorname{Ass}_B(N/PN) \subseteq \operatorname{Ass}_B(M \otimes_A N)$.

($\subseteq$). We prove this containment in two steps.

Case 1 First suppose M is P-coprimary, i.e. $\operatorname{Ass}_A(M) = \{P\}$.
Then every element of M is killed by a power of P. Hence every element of $M \otimes_A N$ is killed by a power of P. Thus every associated prime of $M \otimes_A N$ over B contains PB. Let $\mathfrak{q} \in \operatorname{Ass}_B(M \otimes_A N)$. Pick $x \in A - P$. Then $M \xrightarrow{x} M$ is injective. So $M \otimes_A N \xrightarrow{a} M \otimes_A N$ is injective. Thus $\varphi^{-1}(\mathfrak{q}) \subseteq P$. By above we also have $\varphi^{-1}(\mathfrak{q}) \supseteq P$, and so $\varphi^{-1}(\mathfrak{q}) = P$.

Now take a prime filtration of M:

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = (0),$$

where $M_i/M_{i+1} \cong A/P_i$ and each $P_i \in \mathrm{Ass}_A(M)$. In particular, $P_i = P$ for some i. Now since N is A-flat, we have a new filtration

$$M \otimes_A N = M_0 \otimes_A N \supsetneq M_1 \otimes_A N \supsetneq \cdots \supsetneq M_n \otimes_A N = (0)$$

satisfying $M_i/M_{i+1} \otimes_A N \cong N/P_iN$. Clearly

$$\mathrm{Ass}_B(M \otimes_A N) \subseteq \bigcup_{i=0}^{n-1} \mathrm{Ass}_B(N/P_iN).$$

But if $\mathfrak{q} \in \mathrm{Ass}_B(N/P_iN)$ for $P_i \neq P$, then $\varphi^{-1}(\mathfrak{q}) = P_i \neq P$. Hence, by (1), $\mathfrak{q} \notin \mathrm{Ass}_B(M \otimes_A N)$. Thus

$$\mathrm{Ass}_B(M \otimes_A N) \subseteq \mathrm{Ass}_B(N/PN).$$

Case 2 Now we prove the containment for arbitrary M.
Let $(0) = M_1 \cap \cdots \cap M_n$ be a primary decomposition of (0) in M where M_i is P_i-primary. We then have in injection

$$M = M/\bigcup_{i=1}^{n} M_i \hookrightarrow \bigoplus_{i=1}^{n} M/_i,$$

where each component map is the natural surjection. Since M/M_i is P_i-coprimary, by Case 1 we have $\mathrm{Ass}_B(M/M_i \otimes_A N) \subseteq \mathrm{Ass}_B(N/P_iN)$. Therefore,

$$\mathrm{Ass}_B(M \otimes_A N) \subseteq \bigcup_{i=1}^{n} \mathrm{Ass}_B(M/M_i) \subseteq \bigcup_{P \in \mathrm{Ass}_A(M)} \mathrm{Ass}_B(N/PN).$$

■

Corollary 6.45 *If $f : A \to B$ is a flat homomorphism of Noetherian rings, then*

$$\mathrm{Ass}_B(B) = \bigcup_{\mathfrak{p} \in \mathrm{Ass}_A(A)} \mathrm{Ass}_B(B/\mathfrak{p}B).$$

If f above is faithfully flat, then $f^{-1}(\mathrm{Ass}_B(B)) = \mathrm{Ass}_A(A)$.

Lemma 6.46 *Suppose $A \to B$ is a local homomorphism of local rings where $\mathfrak{m}$ and $\mathfrak{n}$ are the maximal ideals of A and B respectively, M is a finitely generated A-module, and N is a finitely generated A-flat module. If $x \in B$ is regular on $N/\mathfrak{m}N$, then x is regular on $M \otimes_A N$ and N/xN is flat over A.*

Proof Let $x \in B$ be regular on $N/\mathfrak{m}N$. Suppose we have $xz = 0$ for some $z \in M \otimes_A N$. If $z \neq 0$ then since $\bigcap_{i=1}^{\infty} \mathfrak{m}^i = (0)$, there is a largest integer i such that $z \in \mathfrak{m}^i(M \otimes_A N) - m^{i+1}(M \otimes_A N)$. We then have

$$m^i(M \otimes_A N)/\mathfrak{m}^{i+1}(M \otimes_A N) \cong (\mathfrak{m}^i M/\mathfrak{m}^{i+1}M) \otimes_A N \cong (A/\mathfrak{m})^t \otimes_A N \cong (N/\mathfrak{m}N)^t,$$

for some $t > 0$. Since x is regular on $(N/\mathfrak{m}N)$, x is regular on $\mathfrak{m}^i(M \otimes_A N)/\mathfrak{m}^{i+1}(M \otimes_A N)$. Thus $z \in \mathfrak{m}^{i+1}(M \otimes_A N)$, a contradiction. Hence $z = 0$, and x is regular on $M \otimes_A N$.

To show that N/xN is A-flat, consider an exact sequence

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

of finitely generated A-modules. In the following commutative diagram, the first two rows are exact since N is A-flat, and all columns are exact since x is a nonzero divisor on $M \otimes_A N$ for all finitely generated M.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M_1 \otimes_A N & \longrightarrow & M_2 \otimes_A N & \longrightarrow & M_3 \otimes_A N & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle x} & & \downarrow{\scriptstyle x} & & \downarrow{\scriptstyle x} & & \\
0 & \longrightarrow & M_1 \otimes_A N & \longrightarrow & M_2 \otimes_A N & \longrightarrow & M_3 \otimes_A N & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M_1 \otimes_A N/xN & \longrightarrow & M_2 \otimes_A N/xN & \longrightarrow & M_3 \otimes_A N/xN & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

A diagram chase argument shows that the bottom row is exact. ■

Theorem 6.47 *If $A \to B$ is a local homomorphism of local rings where $\mathfrak{m}$ and $\mathfrak{n}$ are the maximal ideals of A and B respectively, M is a finitely generated A-module, and N is a finitely generated A-flat module, then the following are true:*

(1) $\operatorname{depth}_{\mathfrak{n}}(M \otimes_A N) = \operatorname{depth}_{\mathfrak{m}}(M) + \operatorname{depth}_{\mathfrak{n}}(N/\mathfrak{m}N)$.

(2) $\dim_B(M \otimes_A N) = \dim_A(M) + \dim_B(N/\mathfrak{m}N)$.

Proof If $\operatorname{depth}_A(M) > 0$ then we have $x \in \mathfrak{m}$ which is regular on M. Hence $M \xrightarrow{x} M$ is injective. Since N is flat, $M \otimes_A N \xrightarrow{x} M \otimes_A N$ is injective. Since $x \in \mathfrak{m}$, $(M \otimes_A N)/x(M \otimes_A N) \neq 0$ by Nakayama's Lemma. So x is regular on $M \otimes_A N$. Since

$$\operatorname{depth}_{\mathfrak{n}}(M \otimes_A N) = \operatorname{depth}_{\mathfrak{n}}((M \otimes_A N)/x(M \otimes_A N)) + 1$$

and

$$\operatorname{depth}_{\mathfrak{m}}(M) = \operatorname{depth}_A(M/xM) + 1,$$

we may assume by induction that $\operatorname{depth}_{\mathfrak{m}}(M) = 0$.

If $\operatorname{depth}_B(N/\mathfrak{m}N) > 0$ then again we take $x \in \mathfrak{n}$ to be a regular element on $N/\mathfrak{m}N$. By the previous lemma, x is regular on $M \otimes_A N$ and N/xN is A-flat. So again by induction we may assume that $\operatorname{depth}_B(N/\mathfrak{m}N) = 0$.

We are now reduced to the case where $\operatorname{depth}_{\mathfrak{n}}(N/\mathfrak{m}N) = 0$ and $\operatorname{depth}_{\mathfrak{m}}(M) = 0$. Thus $\mathfrak{m} \in \operatorname{Ass}_A(M)$ and $\mathfrak{n} \in \operatorname{Ass}_B(N/\mathfrak{m}N)$. By Theorem 6.44, $\mathfrak{n} \in \operatorname{Ass}_B(M \otimes_A N)$. Thus $\operatorname{depth}_{\mathfrak{n}}(M \otimes_A N) = 0$ and we are done.

(2) Let $x_1, \ldots, x_s$ be a system of parameters for M and let $y_1, \ldots, y_t$ be a system of parameters for $N/\mathfrak{m}N$. It follows that $\lambda(M \otimes_A N)/(x_1, \ldots, x_s, y_1, \ldots, y_t)(M \otimes_A N) < \infty$. Thus $\dim(M \otimes_A N) \leq \dim(M) + \dim(N/\mathfrak{m}N)$.

For the other inequality, we may replace A by $\overline{A} = A/\operatorname{Ann}_A(M)$ so that $\operatorname{Supp}(M) = \operatorname{Spec}(\overline{A})$ since $M \otimes_A N \cong M \otimes_{\overline{A}} (N/\operatorname{Ann}_A(M)N)$. Further replacing B by $B/(\operatorname{Ann}_A(M)B + \operatorname{Ann}_B(N))$ and N by $N/\operatorname{Ann}_A(M)N$ allows us to assume that $\operatorname{Supp}_B(N) = \operatorname{Spec}(B)$. So proving that

$$\dim(M \otimes_A N) \geq \dim_A(M) + \dim_B(N/\mathfrak{m}N)$$

is equivalent to proving that

$$\dim(B) \geq \dim(A) + \dim(B/\mathfrak{m}B).$$

But since $A \to B$ is flat, it satisfies the going-down property. So choosing a prime ideal $\mathfrak{p}$ minimal over $\mathfrak{m}B$ gives $\operatorname{ht}(\mathfrak{p}) \geq \operatorname{ht}(\mathfrak{m})$. Thus

$$\begin{aligned} \dim(B) &\geq \operatorname{ht}(\mathfrak{m}B) + \dim(B/\mathfrak{m}B), \\ &\geq \operatorname{ht}(\mathfrak{m}) + \dim(B/\mathfrak{m}B), \\ &= \dim(A) + \dim(B/\mathfrak{m}B). \end{aligned}$$

■

Corollary 6.48 *If $A \to B$ is a local homomorphism of local rings where $\mathfrak{m}$ and $\mathfrak{n}$ are the maximal ideals of A and B respectively, M is a finitely generated A-module, and N is a finitely generated A-flat module, then $M \otimes_A N$ is Cohen-Macaulay if and only if M is Cohen-Macaulay and $N/\mathfrak{m}N$ is Cohen-Macaulay as a B-module.*

Corollary 6.49 *If $A \to B$ is a local homomorphism of local rings where $\mathfrak{m}$ is the maximal ideal of A, then B is Cohen-Macaulay if and only if A is Cohen-Macaulay and $B/\mathfrak{m}B$ is Cohen-Macaulay.*

Definition If A is Noetherian, and M is a finitely generated A-module, then M is called **Cohen-Macaulay** if for every maximal ideal of A, $M_{\mathfrak{m}}$ is Cohen-Macaulay. A Noetherian ring A is **Cohen-Macaulay** if it is a Cohen-Macaulay module over itself.

Definition Let A be a Noetherian ring and I an ideal of A of height r. We say I is **unmixed** if $\mathrm{ht}(\mathfrak{p}) = r$ for all $\mathfrak{p} \in \mathrm{Ass}_A(A/I)$.

Definition We say that the **unmixedness property** holds in A if for every $r \geq 0$ and every height r ideal I generated by r elements is unmixed.

Theorem 6.50 *If A is Noetherian, then the following are equivalent:*

(1) *A is Cohen-Macaulay.*

(2) *For every $\mathfrak{p} \in \mathrm{Spec}(A)$, $A_\mathfrak{p}$ is Cohen-Macaulay.*

(3) *For every ideal I in A, $\mathrm{ht}(I) = \mathrm{depth}_I(A)$.*

(4) *The unmixedness property holds in A.*

Proof (1) $\Rightarrow$ (2) Let $\mathfrak{p} \in \mathrm{Spec}(A)$ and take $\mathfrak{m}$ a maximal ideal containing $\mathfrak{p}$. Then $A_\mathfrak{m}$ is Cohen-Macaulay by definition. Thus $R_\mathfrak{p} = (R_\mathfrak{m})_{\mathfrak{p}R_\mathfrak{m}}$ is Cohen-Macaulay by by local theorem.

(2) $\Rightarrow$ (3) It is enough to show that for all prime ideals $\mathfrak{p}$, $\mathrm{ht}(\mathfrak{p}) = \mathrm{depth}_\mathfrak{p}(A)$. But

$$\mathrm{ht}(\mathfrak{p}) = \dim(A_\mathfrak{p}) = \mathrm{depth}(A_\mathfrak{p}) = \mathrm{depth}_\mathfrak{p}(A)$$

since $A_\mathfrak{p}$ is Cohen-Macaulay.

(3) $\Rightarrow$ (4) Let $I = (a_1, \ldots, a_r)$ be an ideal such that $\mathrm{ht}(I) = r$. Let $\mathfrak{p} \in \mathrm{Ass}_A(A/I)$. Since $\mathrm{ht}(J) = \mathrm{depth}_J(A)$ for every ideal in A and since $\mathfrak{p} \in \mathrm{Ass}_A(A/I)$, we have $r = \mathrm{depth}_{IA_\mathfrak{p}}(A_\mathfrak{p}) = \mathrm{depth}_{\mathfrak{p}A_\mathfrak{p}}(A_\mathfrak{p}) = \dim(A_\mathfrak{p}) = \mathrm{ht}(\mathfrak{p})$.

(4) $\Rightarrow$ (1) Suppose the unmixedness property holds in A. Let $\mathfrak{m}$ be a maximal ideal. Let $a_1, \ldots, a_r$ be a maximal A-sequence in $\mathfrak{m}$ and set $I = (a_1, \ldots, a_r)$. Then we have $\mathrm{ht}(\mathfrak{m}) = \dim(A_\mathfrak{m}) = r = \mathrm{depth}_\mathfrak{m}(A) = \mathrm{depth}(A_\mathfrak{m})$. Therefore $A_\mathfrak{m}$ is Cohen-Macaulay. Therefore ■

Example 6.51 *$A = k[\![X, Y]\!]/(X^2, XY)$ is not Cohen-Macaulay, as $\mathfrak{m} \in \mathrm{Ass}(A)$ and therefore $\mathrm{depth}(A) = 0$, but $\dim(A)$ is at least 1 as we have the chain of prime ideals*

$$(X) \subsetneq (X, Y).$$

Example 6.52 *Any ring of dimension zero is Cohen-Macaulay.*

Example 6.53 *Any domain of dimension one is Cohen-Macaulay.*

Definition A ring is called a **complete intersection** if it is of the form

$$A/(x_1, \ldots, x_r).$$

where A is a regular ring and $x_1, \ldots, x_r$ an A-sequence.

Exercise 6.54 *Show that if A is regular, then A is Cohen-Macaulay. Use this to show that any local complete intersection if Cohen-Macaulay.*

Exercise 6.55 *If A, B are Noetherian rings, $f : A \to B$ is faithfully flat, then B is Cohen-Macaulay if and only if A is Cohen-Macaulay and for all $\mathfrak{p} \in \operatorname{Spec}(A)$ such that $\mathfrak{p} = f^{-1}(P)$ where $P \in \operatorname{MaxSpec}(B)$, $\boldsymbol{\kappa}(\mathfrak{p}) \otimes_A B$ is Cohen-Macaulay.*

Exercise 6.56 *If A is local, M is finitely generated, then M is Cohen-Macaulay if and only if $\widehat{M}$ is Cohen-Macaulay. Similarly, A is Cohen-Macaulay if and only if $\widehat{A}$ is Cohen-Macaulay.*

Exercise 6.57 *$A[x]$ is Cohen-Macaulay if and only if A is Cohen-Macaulay. Moreover, A is Cohen-Macaulay if and only if $A[x_1, \ldots, x_n]$ is Cohen-Macaulay.*

Exercise 6.58 *Suppose $f : A \to A[\![x]\!]$ is the canonical injection.*

(1) *Is f faithfully flat?*

(2) *For $\mathfrak{p} \in \operatorname{Spec}(A)$, is $\boldsymbol{\kappa}(\mathfrak{p}) \otimes_A A[\![x]\!]$ local? Note that*

$$\boldsymbol{\kappa}(\mathfrak{p}) \otimes_A A[\![x]\!] \subsetneq \boldsymbol{\kappa}(\mathfrak{p})[\![x]\!].$$

(3) *Is $\boldsymbol{\kappa}(\mathfrak{p})[\![x]\!]$ the completion of $\boldsymbol{\kappa}(\mathfrak{p}) \otimes_A A[\![x]\!]$?*

Proposition 6.59 *If A is a regular local ring, and M is finitely generated A-module, M is free if and only if M is Cohen-Macaulay.*

Proof Use the Auslander-Buchsbaum formula and the fact that M is free over a local ring if and only if $\operatorname{pd}(M) = 0$. ■

Corollary 6.60 *Let A be a regular local ring where B is a local module finite extension of A. Then B is Cohen-Macaulay over A if and only if B is a free A-module.*

Example 6.61 *Let $R = k[\![X^2, Y^2]\!]$, $A = k[\![X^2, XY, Y^2]\!]$, and $B = k[\![X, Y]\!]$. Consider the canonical injections*

$$R \hookrightarrow A \hookrightarrow B.$$

Note R is a regular local ring. Since A is free over R with basis $\{1, XY\}$, A is Cohen-Macaulay as an R-module. Is B Cohen-Macaulay? Since B is regular, it is in fact Cohen-Macaulay as a module over itself. Moreover it is Cohen-Macaulay over R as we can have the basis $\{1, X, Y, XY\}$. But is B Cohen-Macaulay over A? Well it is clear that A is not regular as it is integral over R and thus $\dim(A) = 2$ while $\mathfrak{m}$ is generated by 3 elements. However B is regular, and so if B is flat over A, then for i sufficiently large

$$0 = \operatorname{Tor}_i^B(B/\mathfrak{m}, B/\mathfrak{m}) = \operatorname{Tor}_i^A(A/\mathfrak{m}, A/\mathfrak{m}) \otimes_A B.$$

Thus we would then see that $\operatorname{Tor}_i^A(A/\mathfrak{m}, A/\mathfrak{m}) = 0$ for i sufficiently large implying that A is regular, a contradiction. Hence B is not Cohen-Macaulay as an A-module.

Exercise 6.62 *Suppose that $f : A \to B$ is a local homomorphism of local rings, A is regular, $B/\mathfrak{m}B$ is regular, and*

$$\dim(B) = \dim(A) + \dim(B/\mathfrak{m}B).$$

Then show that:

(1) *B is regular.*

(2) *f is flat.*

Example 6.63 *Let $A = k[\![X^2, Y]\!]$ and $B = k[\![X^2, X^3, XY, Y]\!]$. Note that B is integral over A and hence $\dim(B) = 2$. Check that $\{1, XY, X^3\}$ form a minimal set of generators of B over A. Since A is regular, B is Cohen-Macaulay as an A-module if and only if B is free over A. However B is not free as*

$$X^2XY - YX^3 = 0.$$

Thus B is not Cohen-Macaulay as an A-module.

Theorem 6.64 (Hartshorne's Connectedness Theorem) *Let A be a local ring such that $\operatorname{depth}(A) \geq 2$. Let I and J be two ideals such that $I + J$ is $\mathfrak{m}$-primary and $I \cap J$ is nilpotent. Then either I or J is nilpotent.*

Proof Since $I \cap J$ is nilpotent, $(I \cap J)^t = 0$ for some $t > 0$. Thus $(IJ)^{t_0} = 0$ for some $t_0 > 0$. By the Artin-Rees Lemma, there exists $i > 0$ such that

$$I^{n+i} \cap J^{t_0} = I^n(J^{t_0} \cap I^i) \subseteq I^n J^{t_0}$$

for all $n > 0$. Thus for $n > t_0$ we have

$$I^n \cap J^{t_0} \subseteq I^{n-s} J^{t_0} \subseteq (IJ)^{t_0} = 0.$$

Thus by taking large powers of I and J, we can assume that $I \cap J = 0$ and $I + J$ is $\mathfrak{m}$-primary. Thus $\operatorname{depth}_{I+J}(A) = 2$, so we may pick $a, b \in I$ and $c, d \in J$ such that $a + c, b + d$ is an A-sequence. Then

$$a(b + d) - b(a + c) = ad + bc = 0$$

since $IJ = 0$. Thus $a = \lambda(a + c)$ for some $\lambda \in A$. Hence $(1 - \lambda)a = \lambda c$. Exactly one of $\lambda, 1 - \lambda$ is contained in $\mathfrak{m}$, otherwise $1 \in \mathfrak{m}$. Thus exactly one of $\lambda, 1 - \lambda$ is a unit. So either $a = \mu c$ or $c = \eta a$. Hence $a \in I \cap J$ or $c \in I \cap J$. Therefore $a = 0$ or $c = 0$. Since $a + c$ was the first element in an A-sequence, either a is a nonzerodivisor or c is. But since $aJ = Ic = 0$, either $I = 0$ or $J = 0$. ■

Remark Geometrically speaking, this is saying that $\operatorname{Spec}(A) - \{\mathfrak{m}\}$ is connected. If not then

$$\operatorname{Spec}(A) = V(I) \cup V(J) = V(I \cap J)$$

such that $V(I) \cap V(J) = V(I + J) = \{\mathfrak{m}\}$, that is $I + J$ is $\mathfrak{m}$-primary and $I \cap J$ is nilpotent. Then by the theorem, I or J is nilpotent and so $V(I) = \operatorname{Spec}(A)$ or $V(J) = \operatorname{Spec}(A)$. Hence either $V(I) = \{\mathfrak{m}\}$ or $V(J) = \{\mathfrak{m}\}$. Said otherwise, this means that $\operatorname{Spec}(A) - \{\mathfrak{m}\}$ is connected as a topological space.

Exercise 6.65 *If*

$$A = \frac{\mathbb{C}[X, Y, U, V]}{(X, Y) \cap (U, V)}$$

show that A is not Cohen-Macaulay.

Chapter 7

Injective Modules over Noetherian Rings

7.1 Essential Extensions and Injective Hulls

For the moment, we do not need A to be Noetherian.

Definition Let A be a ring and M, N, A-modules with $\alpha : M \hookrightarrow N$ an A-linear map. N is called an **essential extension** of M if for every nonzero submodule N_0 of N, $N_0 \cap M \neq 0$.

Equivalently, suppose M are N are A-modules. N is an essential extension of M if for all A-modules T and all A-linear maps $\beta : N \to T$, whenever the composition $\beta \circ \alpha$ is injective, β is also injective.

Exercise 7.1 *If A is a domain, show that $A \hookrightarrow \mathrm{Frac}(A)$ is an essential extension.*

Exercise 7.2 *If M is an injective A-module with $M \ncong N$, show that*

$$M \hookrightarrow N$$

is never an essential extension of M.

By the exercises above, we see that no integral domain is injective over itself unless it is a field.

Proposition 7.3 *If $\alpha : M \hookrightarrow N$ and $\beta : N \hookrightarrow T$ such that α and β are essential extensions, then*

$$\beta \circ \alpha : M \hookrightarrow N \hookrightarrow T$$

is an essential extension.

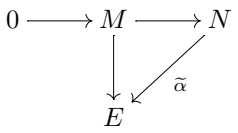
Proof Let T_0 be a nonzero submodule of T. Since $N \hookrightarrow T$ is essential, $N \cap T_0$ is nonzero. Since $M \hookrightarrow N$ is essential, $M \cap (N \cap T_0) = M \cap T_0$ is nonzero. Hence the composition is essential. ■

Theorem 7.4 *Let A be a ring, M and N be A-modules, then the following are equivalent:*

(1) *$\alpha : M \hookrightarrow N$ is a maximal essential extension; that is, there is no proper extension $\beta : N \hookrightarrow T$ such that $\beta \circ \alpha$ is an essential extension of M.*

(2) *$\alpha : M \hookrightarrow N$ is an essential extension of M and N is injective.*

Proof Let E be some injective module containing M. Since E is injective, we can lift an essential extension $M \hookrightarrow N$ to a map $\widetilde{\alpha} : N \to E$. See diagram.

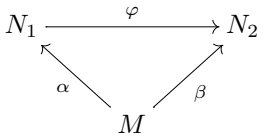


Since N is essential, $\widetilde{\alpha}$ is injective. So we may view all essential extensions as submodules of a chosen injetive module containing M. (1) $\Rightarrow$ (2) Suppose that $T \subseteq E$ is a maximal essential extension. By Zorn's Lemma, there is a maximal submodule N of E such that $N \cap T = 0$. We then have an injection $T \hookrightarrow E/N$. If this is not an isomorphism, then E/N is a proper essential extenion of T, a contradiction. Hence $E = T \oplus N$ and so T, being a summand of an injective, is itself injective.

(2) $\Rightarrow$ (1) Suppose now that $M \hookrightarrow E$ is essential and that E is injective. Take any other essential extension $M \hookrightarrow T \subseteq E$. If T were maximal essential, then $\widetilde{\alpha}$ must be an isomorphism. ■

Corollary 7.5 *N is a maximal essential extension of M if and only if N is an injective module which contains M minimally.*

Lemma 7.6 *Suppose that $\alpha : M \hookrightarrow N_1$ and $\beta : M \hookrightarrow N_2$ are both maximal essential extensions of M. Then there exists a (nonunique) isomorphism φ such that the diagram below commutes.*



Proof Since N_2 is maximal essential, it is injective. Hence the map φ above exists. Since β is injective and $M \hookrightarrow N_1$ is essential, φ is injective. But since N_1 is maximal essential, φ must be an isomorphism. ■

Definition If M is a A-module, a maximal essential extension of M is called the **injective hull** of M and will be denoted by $E_A(M)$.

Lemma 7.7 *Let $(A, \mathfrak{m})$ be a local ring and let M be an A-module such that every element of M is killed by some power of $\mathfrak{m}$. Then M is a module over $\widehat{A}$.*

Proof Exercise. ■

Lemma 7.8 *Let M be an A-module and let U be a multiplicatively closed set. If multiplication by u on M is an isomorphism for all $u \in U$, then M is a $U^{-1}A$-module.*

Proof Exercise. ■

Now we consider injective modules over Noetherian rings.

Theorem 7.9 *Let A be a Noetherian ring. Then:*

(1) *Any direct sum of injective modules is injective.*

(2) *For every $\mathfrak{p} \in \operatorname{Spec}(A)$, $E_A(A/\mathfrak{p})$ is indecomposable. Moreover, there exists a one-to-one correspondence between $\operatorname{Spec}(A)$ and the set of all (nonisomorphic) indecomposable injective modules over A.*

(3) *Every element of $E_A(A/\mathfrak{p})$ is annihilated by some power of $\mathfrak{p}$.*

(4) *For all $\mathfrak{p} \in \operatorname{Spec}(A)$:*

$$E_A(A/\mathfrak{p}) = E_{A_\mathfrak{p}}(\boldsymbol{\kappa}(\mathfrak{p})) = E_{\widehat{A}_\mathfrak{p}}(\boldsymbol{\kappa}(\mathfrak{p}))$$

(5) *Every injective module can be expressed as a direct sum of indecomposable injective modules.*

(6) *The number of copies of $E_A(A/\mathfrak{p})$ for any prime ideal $\mathfrak{p}$ in such a decomposition as described in 5 above, is independent of the decomposition. If E is an injective A-module, then the number of copies of $E_A(A/\mathfrak{p})$ in the decomposition is $\dim_{\boldsymbol{\kappa}(\mathfrak{p})}(\operatorname{Hom}_{A_\mathfrak{p}}(\boldsymbol{\kappa}(\mathfrak{p}), E_\mathfrak{p})$.*

Putting (5) and (6) together from the theorem above we see that given an A-module M, we have that:

$$E_A(M) = \bigoplus_{\mathfrak{p} \in \operatorname{Spec}(A)} E_A(A/\mathfrak{p})^{\dim_{\boldsymbol{\kappa}(\mathfrak{p})} \operatorname{Hom}_{A_\mathfrak{p}}(\boldsymbol{\kappa}(\mathfrak{p}), M_\mathfrak{p})}$$

Proof (1) Let $\{E_j\}_{j \in J}$ be a family of injective modules. By Baer's criterion, to check that $E = \bigoplus_{j \in J} E_j$ is injective, it suffices to check that any map $\varphi : \mathfrak{a} \to E$, where $\mathfrak{a}$ is an ideal of A, can be extended to a map $\widetilde{\varphi} : A \to E$. Let $\pi_j : E \to E_j$ be the jth projection map and let $\varphi_j = \pi_j \circ \varphi$. Since A is Noetherian, $\mathfrak{a}$ is finitely generated. Hence φ_j is the zero map for all but finitely many $j \in J$. For those indices, we can lift φ_j to $\widetilde{\varphi}_j : A \to E_j$ since each E_j is injective. Setting $\widetilde{\varphi}_j = 0$ for the remaining indices we obtain a lift $\widetilde{\varphi} = \bigoplus_{j \in J} \widetilde{\varphi}_j : A \to E$ of φ.

(2) Let $\mathfrak{p} \in \operatorname{Spec}(A)$. Suppose $E_A(A/\mathfrak{p}) = E_1 \oplus E_2$ with $E_1 \cap E_2 = 0$. Let $\alpha : A/\mathfrak{p} \hookrightarrow E_A(A/\mathfrak{p})$ be the injection. Then

$$(E_1 \cap \alpha(A/\mathfrak{p})) \cap (E_2 \cap \alpha(A/\mathfrak{p})) = (E_1 \cap E_2) \cap \alpha(A/\mathfrak{p}) = 0.$$

Since α is an essential extension,

$$I_1 = E_1 \cap \alpha(A/\mathfrak{p}) \neq 0 \quad \text{and} \quad I_2 = E_2 \cap \alpha(A/\mathfrak{p}) \neq 0.$$

Viewing I_1, I_2 as ideals in $A/\mathfrak{p}$, we have that $I_1 \cap I_2 \supseteq I_1 I_2$. Since $A/\mathfrak{p}$ is a domain, $I_1 I_2 \neq 0$. This contradicts $I_1 \cap I_2 = 0$. Thus $E_A(A/\mathfrak{p})$ is indecomposable for all primes $\mathfrak{p}$.

Now let E be any indecomposable injective A-module. Pick $0 \neq e \in E$. Take $\mathfrak{p} \in \mathrm{Ass}_A(Ae)$. Then $A/\mathfrak{p} \hookrightarrow Ae \hookrightarrow E$. Since E is injective, there exists a map $\varphi : E_A(A/\mathfrak{p}) \to E$ such that

$$\begin{array}{ccccc} 0 & \hookrightarrow & A/\mathfrak{p} & \hookrightarrow & E_A(A/\mathfrak{p}) \\ & & \downarrow & \swarrow_{\varphi} & \\ & & E & & \end{array}$$

commutes. Since $A/\mathfrak{p} \hookrightarrow E_A(A/\mathfrak{p})$ is an essential extension, φ is injective. Since $E_A(A/\mathfrak{p})$ is injective, it is a direct summand of E. Since E is indecomposable, $E = E_A(A/\mathfrak{p})$.

It remains to show that if $\mathfrak{p} \neq \mathfrak{q}$ then $E_A(A/\mathfrak{p}) \ncong E_A(A/\mathfrak{q})$. Let $x \in A$. We have the following commutative diagram:

$$\begin{array}{ccc} A/\mathfrak{p} & \xrightarrow{x} & A/\mathfrak{p} \\ \downarrow & & \downarrow \\ E_A(A/\mathfrak{p}) & \xrightarrow{x} & E_A(A/\mathfrak{p}). \end{array}$$

If $x \in \mathfrak{p}$, multiplication by x is the zero map on $A/\mathfrak{p}$ and so x must kill some nonzero elements (i.e. is not injective) in $E_A(A/\mathfrak{p})$. If $x \notin \mathfrak{p}$, then multiplication by x is injective on $A/\mathfrak{p}$. Since $E_A(A/\mathfrak{p})$ is an essential extension, multiplition by x is injective on $E_A(A/\mathfrak{p})$. Since $E_A(A/\mathfrak{p})$ is injective, multiplication by x is an isomorphism on $E_A(A/\mathfrak{p})$.

Now let $\mathfrak{p} \neq \mathfrak{q}$ be two prime ideals of A and pick $x \in \mathfrak{p} - \mathfrak{q}$. Then multiplication by x is an isomorphism on $E_A(A/\mathfrak{q})$ but is not injective on $E_A(A/\mathfrak{p})$. Therefore $E_A(A/\mathfrak{p}) \ncong E_A(A/\mathfrak{q})$.

(3) Let $0 \neq e \in E_A(A/\mathfrak{p})$ and let $\mathfrak{q} \in \mathrm{Ass}_A(Ae)$. Then $A/\mathfrak{q} \hookrightarrow Ae \hookrightarrow E_A(A/\mathfrak{p})$. Therefore $\mathfrak{q} = \mathfrak{p}$ and $\mathrm{Ass}_A(Ae) = \{\mathfrak{p}\}$. Thus $\mathfrak{p}^n e = 0$ for some integer n.

(4) First note that $A/\mathfrak{p} \hookrightarrow \boldsymbol{\kappa}(\mathfrak{p}) = \mathrm{Frac}(A/\mathfrak{p})$ is an essential extension. Thus $E_A(A/\mathfrak{p}) = E_A(\boldsymbol{\kappa}(\mathfrak{p}))$. Since multiplication by $x \in A - \mathfrak{p}$ induces is an isomorphism on $E_A(A/\mathfrak{p})$, $E_A(A/\mathfrak{p})$ is an $A_{\mathfrak{p}}$-module. The map $\boldsymbol{\kappa}(\mathfrak{p}) \hookrightarrow E_A(A/\mathfrak{p})$ is an essential extension over A, and hence an essential extension over $A_{\mathfrak{p}}$. Finally, since an $A_{\mathfrak{p}}$-module is A-injective if and only if it is $A_{\mathfrak{p}}$-injective, we have $E_A(A/\mathfrak{p}) = E_A(\boldsymbol{\kappa}(\mathfrak{p})) = E_{A_{\mathfrak{p}}}(\boldsymbol{\kappa}(\mathfrak{p}))$.

Now since every element in $E_A(A/\mathfrak{p})$ is killed by a power of $\mathfrak{p}$, $E_A(A/\mathfrak{p})$ is a module over $\widehat{A_\mathfrak{p}}$. By the same argument as for $A_\mathfrak{p}$, $E_A(A/\mathfrak{p}) = E_{\widehat{A}}(\boldsymbol{\kappa}(\mathfrak{p}))$.

(5) Let E be an injective module. As in (3), for any $0 \neq e \in E$, $A/\mathfrak{p} \hookrightarrow Ae \hookrightarrow E$ where $\mathfrak{p} \in \mathrm{Ass}_A(Ae)$ and so $E_A(A/\mathfrak{p})$ is a summand of E. Let $\mathcal{F}$ be the collection of families of indecomposable injective submodules $\{E_\lambda\}$ of E such that $\cap_\lambda E_\lambda = 0$. We have shown that this family is nonempty, so by Zorn's Lemma $\mathcal{F}$ has a maximal element, say $\{E_\alpha\}$. Set $E' = \oplus_\alpha E_\alpha$. If $E' \subsetneq E$, then $E = E' \oplus E''$ for some necessarily injective module E''. Pick a prime $\mathfrak{p}$ with $i : E_A(A/\mathfrak{p}) \hookrightarrow E''$ an injection. Then $\{E_\alpha\} \cup \{i(E_A(A/\mathfrak{p}))\}$ is a member of $\mathcal{F}$ strictly larger than $\{E_\alpha\}$, a contradiction. Hence $E = E'$.

(6) Let $E = \bigoplus_{\mathfrak{p}\in \mathrm{Spec}(A)} E_A(A/\mathfrak{p})^{i_\mathfrak{p}}$. For any prime $\mathfrak{q}$,

$$E_\mathfrak{q} = \bigoplus_{\mathfrak{p}\subseteq\mathfrak{q}} E_{A_\mathfrak{p}}(A/\mathfrak{p})^{i_\mathfrak{p}} = \bigoplus_{\mathfrak{p}\subseteq\mathfrak{q}} E_A(A/\mathfrak{p})^{i_\mathfrak{p}}.$$

For $\mathfrak{p} \subseteq \mathfrak{q}$,

$$\mathrm{Hom}_{A_\mathfrak{q}}(\boldsymbol{\kappa}(\mathfrak{q}), E_A(A/\mathfrak{p})) = \begin{cases} 0 & \text{if } \mathfrak{p} \neq \mathfrak{q} \\ \boldsymbol{\kappa}(\mathfrak{q}) & \text{if } \mathfrak{p} = \mathfrak{q}. \end{cases}$$

Thus

$$\mathrm{Hom}_{A_\mathfrak{q}}(\boldsymbol{\kappa}(\mathfrak{q}), E_\mathfrak{q}) = \mathrm{Hom}_{A_\mathfrak{p}}(\boldsymbol{\kappa}(\mathfrak{p}), \bigoplus_{\mathfrak{p}\subseteq\mathfrak{q}} E_A(A/\mathfrak{p})) = \mathrm{Hom}_{A_\mathfrak{q}}(\boldsymbol{\kappa}(\mathfrak{q}), E_A(A/\mathfrak{q}))^{i_\mathfrak{q}} = \boldsymbol{\kappa}(\mathfrak{q})^{i_\mathfrak{q}}.$$

Therefore the integers $i_\mathfrak{q}$ are independent of the decomposition and

$$i_\mathfrak{q} = \dim_{\boldsymbol{\kappa}(\mathfrak{q})}(\mathrm{Hom}_{A_\mathfrak{q}}(\boldsymbol{\kappa}(\mathfrak{q}), E_\mathfrak{q})).$$

■

Exercise 7.10 *Consider $\mathbb{Z}$ as a module over itself. What is $E_\mathbb{Z}(\mathbb{Z})$?*

Exercise 7.11 *Consider the $\mathbb{Z}$-module exact sequence:*

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

Is $\mathbb{Q}/\mathbb{Z}$ indecomposable? If not, find its factors.

Exercise 7.12 *If A is Noetherian, M is an A-module, and U is a multiplicatively closed set, then*

$$U^{-1}E_A(M) \cong E_{U^{-1}A}(U^{-1}M).$$

Exercise 7.13 *If we have $A \to B$ and M is injective over A, then $\mathrm{Hom}_A(B, M)$ is injective over B.*

Exercise 7.14 *What is $E_{k[\![x_1,\ldots,x_n]\!]}(k)$? What is $E_\mathbb{Z}(\mathbb{Z}/p\mathbb{Z})$?*

Remark If $(A, \mathfrak{m}, k)$ is a local ring, and we have an ideal $I \subseteq \mathfrak{m}$, then

$$\begin{aligned} E_{A/I}(k) &= \{x \in E_A(k) : I \cdot x = 0\}, \\ &= \mathrm{Hom}_A(A/I, E_A(k)). \end{aligned}$$

7.2 Matlis Duality

Definition If $(A, \mathfrak{m}, k)$ is a local ring, we define the **Matlis dual** as follows:

$$M^\vee := \mathrm{Hom}_A(M, E_A(k)).$$

Lemma 7.15 *Let $(A, \mathfrak{m}, k)$ be a local ring and let M be a finitely generated A-module. If $\lambda(M) < \infty$, then $\lambda(M) = \lambda(M^\vee)$.*

Proof By assumption, $\lambda(M) < \infty$. So M has a filtration

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_t = (0)$$

such that $M_i/M_{i+1} \cong k$ for all $0 \leq i < t$. Since $E = E_A(k)$ is injective, by applying the functor $\mathrm{Hom}(-, E) = (-)^\vee$, we get surjections

$$M^\vee = (M_0)^\vee \xrightarrow{\varphi_1} (M_1)^\vee \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_t} (M_t)^\vee = (0).$$

Since $\mathrm{Hom}(-, E)$ is contravariant and exact, $\mathrm{Ker}(\varphi_i) \cong k^\vee \cong k$ for $1 \leq i \leq t$. Set $K_i = \mathrm{Ker}(\varphi_{t-i} \circ \cdots \circ \varphi_1) \subseteq (M_0)^\vee$. Then

$$K_i/K_{i+1} \cong \mathrm{Ker}(\varphi_{t-i}) \subseteq (M_{t-i-1})^\vee.$$

Thus

$$M^\vee = K_0 \supsetneq K_1 \supsetneq \cdots \supsetneq K_t = (0)$$

is a filtration of length $t = \lambda(M)$ of $M^\vee$. ■

Theorem 7.16 *If $(A, \mathfrak{m}, k)$ is a local ring of dimension zero, then $E_A(k)$ is a module of finite length, with $\lambda(E_A(k)) \cong \lambda(A)$. Moreover*

$$\mu : A \to \mathrm{Hom}_A(E_A(k), E_A(k)), \qquad \textit{via}$$
$$a \mapsto \textit{map defined by multiplication by } a,$$

is an isomorphism.

Proof For the length assertion, we proceed by induction on $\lambda(A)$. If $\lambda(A) = 1$, then $A = k = E_A(k)$. So suppose $\lambda(A) > 1$. Since $\mathfrak{m} \in \mathrm{Ass}_A(A)$, we have a short exact sequence

$$0 \to k \to A \to A/xA \to 0$$

for some $x \in A$. Applying $(-)^\vee$ we have the short exact sequence

$$0 \to E_{A/xA}(k) \to E_A(k) \to k \to 0.$$

($\mathrm{Hom}_A(A/xA, E_A(k)) \cong E_{A/xA}(k)$ be a previous remark.) By induction

$$\lambda(E_{A/xA}(k) = \lambda(A/xA).$$

Thus

$$\lambda(E_A(k)) = \lambda(k) + \lambda(E_{A/xA}(k)) = 1 + \lambda(A/xA) = \lambda(A).$$

It remains to show that $\mu : A \to \mathrm{Hom}_A(E, E)$ is an isomorphism. Since

$$\lambda(\mathrm{Hom}_A(E, E) = \lambda(E^\vee) = \lambda(E) = \lambda(A^\vee) = \lambda(A),$$

it suffices to show that μ is injective. So suppose not. Take $0 \neq x \in A$ such that $\mu(x) = 0$. Then we have the exact sequence

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

Applying $(-)^\vee$ we have the exact sequence

$$0 \to E_{A/xA}(k) \to E_A(k) \xrightarrow{x} E_A(k) \to E_A(k)/xE_A(k) \to 0.$$

Since $\mu(x) = 0$, $E_{A/xA}(k) \cong E_A(k)$. This implies that

$$\lambda(A/xA) = \lambda(E_{A/xA}(k)) = \lambda(E_A(k)) = \lambda(A),$$

a contradiction since $x \neq 0$. Thus μ is injective, and hence, an isomorphism. ■

Corollary 7.17 *If A is a local ring, then*

$$\begin{aligned} &\mu : \widehat{A} \to \mathrm{Hom}_A(E_A(k)), E_A(k)) = E_A(k)^\vee, && \textit{via} \\ &\quad a \mapsto \textit{map defined by multiplication by } a, \end{aligned}$$

is an isomorphism.

Proof Let $E_n = (0 :_E \mathfrak{m}^n) \subseteq E = E_A(k)$. Then we have the commutative diagrams

$$\begin{array}{ccc} \widehat{A} & \xrightarrow{\quad\mu\quad} & \mathrm{Hom}_A(E, E) \\ \downarrow & & \downarrow \\ A/\mathfrak{m}^n & \xrightarrow{\quad\mu_n\quad} & \mathrm{Hom}_A(E_n, E_n) \end{array}$$

for each $n > 0$. (One checks that the restriction of a map $\varphi : E \to E$ to E_n has image inside E_n.) By the previous theorem, since $\dim(A/\mathfrak{m}^n) = 0$, the map μ_n is an isomorphism for each n. So let $0 \leq a \in \widehat{A}$. Then there exists $n > 0$ such that $a \notin \mathfrak{m}^n$. Thus $\mu_n(\overline{a}) \neq 0$. Hence $\mu_a \neq 0$ and μ is injective.

To show that μ is surjective pick $\alpha \in \mathrm{Hom}_A(E, E)$. Set $\alpha_n = \alpha|_{E_n} \in \mathrm{Hom}_A(E_n, E)$. Consider the following commutative diagram.

$$\begin{array}{ccc} A/\mathfrak{m}^{n+1} & \xrightarrow{\quad\mu_{n+1}\quad} & \mathrm{Hom}_A(E_{n+1}, E) \\ \downarrow & & \downarrow \\ A/\mathfrak{m}^n & \xrightarrow{\quad\mu_n\quad} & \mathrm{Hom}_A(E_n, E) \end{array}$$

Then α_n is just multiplication by a_n for some a_n such that $a_{n+1} - a_n \in \mathfrak{m}^n$. Thus $a = \lim a_n$ exists in $\widehat{A}$. It follows that α is just multiplication by a. Then μ is surjective; hence an isomorphism. ■

Remark Even if A is *not* complete, the map sending $a \in A$ to multiplication by a is still injective.

Lemma 7.18 *If $(A, \mathfrak{m}, k)$ is local and $M \neq 0$ is an A-module, then $M^\vee \neq 0$.*

Proof Let $0 \neq x \in M$. Set $I = \mathrm{Ann}_A(x)$. Then we have an injection $A/I \hookrightarrow M$ sending 1 to x. We also have a surjection $A/I \to A/\mathfrak{m} = k$ since I is a proper ideal. Recall that $(-)^\vee = \mathrm{Hom}_A(-, E_A(k))$ is an exact functor since $E_A(k)$ is injective. We then have exact sequences

$$M^\vee \to (A/I)^\vee \to 0 \quad \text{and} \quad 0 \to k^\vee \to (A/I)^\vee.$$

Since $k^\vee \cong k \neq 0$, $(A/I)^\vee \neq 0$. Thus $M^\vee \neq 0$. ■

Proposition 7.19 *If $(A, \mathfrak{m}, k)$ is local, then $E_A(k)$ is Artinian (satisfies DCC).*

Proof Let $E = E_A(k)$ and let

$$E = E_0 \supseteq E_1 \supseteq E_2 \supseteq \cdots$$

be any descending chain of submodules of E. Applying $(-)^\vee$ and noting that $\mathrm{Hom}_A(E, E) \cong \widehat{A}$, we have

$$\widehat{A} \twoheadrightarrow E_1^\vee \twoheadrightarrow E_2^\vee \twoheadrightarrow \cdots.$$

Set $\psi_n : \widehat{A} \to E_n^\vee$ to be the composition. Then

$$\mathrm{Ker}(\psi_1) \subseteq \mathrm{Ker}(\psi_2) \subseteq \mathrm{Ker}(\psi_3) \subseteq \cdots$$

is an ascending chain of ideals in $\widehat{A}$. Since $\widehat{A}$ is Noetherian, this chain stops so that $\mathrm{Ker}(\psi_n) = \mathrm{Ker}(\psi_{n+1}) = \cdots$ for some $n > 0$. Thus $E_n^\vee \cong E_{n+i}^\vee$ for $i > 0$. For all i we have the short exact sequence

$$0 \to E_{i+1} \to E_i \to E_i/E_{i+1} \to 0$$

and hence

$$0 \to (E_i/E_{i+1})^\vee \to E_i^\vee \to E_{i+1}^\vee \to 0$$

is exact. Since $E_n^\vee \cong E_{n+i}^\vee$ for $i > 0$, $(E_i/E_{i+1})^\vee = 0$ for $i \geq n$. By the previous lemma, $E_i/E_{i+1} = 0$ for $i \geq n$. Thus the descending chain stops with $E_n = E_{n+1} = \cdots$. ■

Theorem 7.20 *If $(A, \mathfrak{m}, k)$ is local and complete with M finitely generated, then*

$$\begin{aligned} \varphi : M \times M^\vee &\to E_A(k), \\ (x, f) &\mapsto f(x), \end{aligned}$$

induces an isomorphism $\Phi_M : M \to M^{\vee\vee}$ via $m \mapsto \varphi(m, -) \in M^{\vee\vee}$.

Proof First we show that Φ is injective for any A-module where A is merely a local (not necessarily complete) ring. Observe that Φ is injective if and only if for every $0 \neq x \in M$ there exists $f \in \mathrm{Hom}_A(M, E) = M^\vee$ such that $f(x) \neq 0$. Let $I = \mathrm{Ann}_A(x)$. Then we have an injection $A/I \hookrightarrow M$ sending $1 \to x$. Thus we have a surjection $M^\vee \twoheadrightarrow (A/I)^\vee$. By Lemma 7.18, $(A/I)^\vee \neq 0$. Hence $M^\vee \neq 0$ and there exists $f \in M^\vee$ such that $f(x) \neq 0$.

Now assume A is complete and M is finitely generated. Note that by Corollary 7.17, $\Phi_A : \widehat{A} \to E^\vee = A^{\vee\vee}$ is an isomorphism. Consider a finite presentation of M

$$A^s \to A^r \to M \to 0.$$

Applying $(-)^\vee$ we have the following exact sequence

$$0 \to M^\vee \to (A^r)^\vee \to (A^s)^\vee.$$

Applying $(-)^{\vee\vee}$ we have the following commutative diagram with exact rows

$$\begin{array}{ccccccc} A^s & \longrightarrow & A^r & \longrightarrow & M & \longrightarrow & 0\ . \\ \downarrow{\scriptstyle \Phi_{A^s}} & & \downarrow{\scriptstyle \Phi_{A^r}} & & \downarrow{\scriptstyle \Phi_M} & & \\ (A^s)^{\vee\vee} & \longrightarrow & (A^r)^{\vee\vee} & \longrightarrow & M^{\vee\vee} & \longrightarrow & 0 \end{array}$$

Since Φ_{A^s}, Φ_{A^r} are isomorphisms, so is Φ_M by the Five Lemma. ■

Corollary 7.21 *If $(A, \mathfrak{m}, k)$ is local and M is finitely generated, then $\widehat{M} \cong M^{\vee\vee}$.*

Proof This follows from the previous theorem. ■

Proposition 7.22 (Structure of Artinian Modules over Local Rings) *Let $(A, \mathfrak{m}, k)$ be local and M an A-module. The following are equivalent:*

(1) *M is Artinian (satisfies DCC).*

(2) $\mathrm{Supp}(M) = \{\mathfrak{m}\}$ *and* $\dim_k \mathrm{Hom}_A(k, M) < \infty$.

(3) $M \subseteq \bigoplus_{i=1}^r E_A(k)$.

Proof (1) $\Rightarrow$ (2) Suppose M satisifes DCC. Then since

$$\mathrm{Hom}_A(k, M) \hookrightarrow \mathrm{Hom}_A(A, M) \cong M,$$

$\mathrm{Hom}_A(k, M)$ has DCC. Since it is a vector space over k, $\mathrm{Hom}_A(k, M)$ is finite dimensional over k.

To show that $\mathrm{Supp}(M) = \{\mathfrak{m}\}$, take $0 \neq x \in M$. Set $I = \mathrm{Ann}_A(x)$. Then there is an injection $A/I \hookrightarrow M$. So A/I has DCC. Being Noetherian, this implies that $\lambda(A/I) < \infty$. Thus $\mathfrak{m}^n(A/I) = 0$ for some n. Hence $\mathfrak{m}^n \subseteq I$, which implies that $\mathfrak{m}^n x = 0$. Therefore $\mathrm{Supp}(M) = \{\mathfrak{m}\}$.

(2) $\Rightarrow$ (3) Now suppose $\mathrm{Supp}(M) = \{\mathfrak{m}\}$ and $\dim_k(\mathrm{Hom}_A(k, M)) < \infty$. Consider $\mathrm{Hom}_A(k, M) \hookrightarrow M$. Fix $0 \neq x \in M$. Then there exists a greatest integer t such that $\mathfrak{m}^t x \neq 0$. Taking $0 \neq y \in \mathrm{Hom}_A(k, M)$, we have that $\mathfrak{m}y = 0$. So the map $\varphi \in \mathrm{Hom}_A(k, M)$ sending $1 \mapsto y$ is well-defined and nonzero. Hence $Ax \cap \mathrm{Hom}_A(k, M) \neq 0$. Therefore $\mathrm{Hom}_A(k, M) \hookrightarrow M$ is an essential extension.

Now since $\mathrm{Hom}_A(k, M)$ is finite dimensional over A, we have $\mathrm{Hom}_A(k, M) \cong k^r$. Thus

$$E_A(M) = E_A(\mathrm{Hom}_A(k, M)) = E_A\left(k^r\right) = E_A(k)^r.$$

Therefore we have an injection

$$M \hookrightarrow E_A(M) = \bigoplus_{i=1}^{r} E_A(k).$$

(3) $\Rightarrow$ (1) This follows from Proposition 7.19. ■

Theorem 7.23 *Suppose that A is a complete local ring. The following are true:*

(1) *If M is Noetherian (satisifes ACC), then $M^\vee$ has DCC (is Artinian) and $M \cong M^{\vee\vee}$.*

(2) *If N is Artinian (satisfies DCC), then $N^\vee$ has ACC (is Noetherian) and $N \cong N^{\vee\vee}$.*

Proof (1) By assumption, M is finitely generated, so there is a surjection $A^n \twoheadrightarrow M$. Hence there is an injection $M^\vee \hookrightarrow \bigoplus_{i=1}^n E$. By the previous proposition, $M^\vee$ has DCC. That $M \cong M^{\vee\vee}$ was shown in Theorem 7.16.

(2) Now suppose N has DCC. By the previous proposition, we have an exact sequence of the form

$$0 \to N \to \bigoplus_{i=1}^{n} E \to \bigoplus_{i=1}^{m} E.$$

Applying the functor $(-)^\vee$ yields the exact sequence

$$A^m \to A^n \to N^\vee \to 0.$$

Then clearly $N^\vee$ has ACC. (It is a quotient of a free A-module.) Moreover, because we have the commuatative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & N & \longrightarrow & E^n & \longrightarrow & E^m \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & N^{\vee\vee} & \longrightarrow & E^n & \longrightarrow & E^m, \end{array}$$

we have that $N \to N^{\vee\vee}$ is an isomorphism.

■

We can restate the above theorem as follows:

Theorem 7.24 (Matlis Duality) *Let $(A, \mathfrak{m}, k)$ be a local ring, then there is a perfect duality between modules with DCC over A and modules with ACC over $\widehat{A}$, that is:*

$$\begin{aligned} \{\textit{Modules with DCC over } A\} &\longleftrightarrow \{\textit{Modules with ACC over } \widehat{A}\} \\ N &\longmapsto N^\vee \\ M^\vee &\longmapsfrom M \end{aligned}$$

Moreover, when A is complete, $A \cong \mathrm{Hom}_A(E_A(k), E_A(k))$.

Proof This follows from the above results. ■

7.3 Minimal Injective Resolutions

If A is Noetherian and M is an A-module, we can construct a minimal injective resolution as follows. Set

$$\begin{aligned} E^0 &= E_A(M), \\ C^1 &= \mathrm{Coker}(M \hookrightarrow E^0), \end{aligned}$$

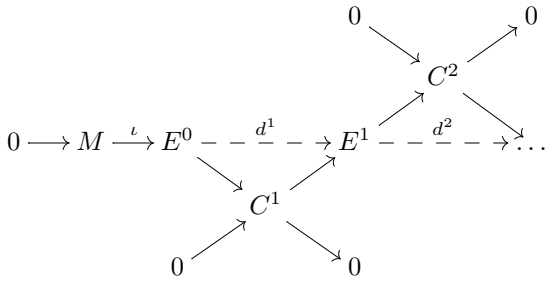
and inductively define

$$\begin{aligned} E^i &= E_A(C^i), \\ C^{i+1} &= \mathrm{Coker}(C^i \hookrightarrow E^i). \end{aligned}$$

Now we may inductively write the exact sequences:

$$\begin{aligned} 0 \to M \to E^0 \to C^1 \to 0, \\ 0 \to C^i \to E^i \to C^{i+1} \to 0. \end{aligned}$$

In this case, C^i is referred to as the ith **cosyzygy** of M. Putting the above exact sequences together we obtain:



The d^i's above are formed by taking the composition of the relevant maps, while ι is the canonical injection. Hence we obtain an **injective resolution** of M, that is a long exact sequence of injective modules starting at M:

$$0 \to M \xrightarrow{\iota} E^0 \xrightarrow{d^0} E^1 \xrightarrow{d^1} E^2 \xrightarrow{d^2} E^3 \to \cdots$$

If this resolution is finite, the index of the final nonzero term is called the **injective dimension** of M and is denoted by $\mathbf{id_A(M)}$, or just $\mathbf{id(M)}$. If $\mathrm{id}(M) = n$, then we have a minimal injective resolution:

$$0 \to M \to E^0 \to E^1 \to \cdots \to E^{n-1} \to E^n \to 0$$

Moreover, if we are given a minimal injective resolution with a nonzero term in degree n, then there does not exist any injective resolution of M of length less than n, because of the uniqueness of injective hulls.

Lemma 7.25 *Let N be an irreducible submodule of M. Then $E_A(M/N)$ is indecomposable and hence*

$$E_A(M/N) \cong E_A(A/\mathfrak{p})$$

for some $\mathfrak{p} \in \mathrm{Spec}(A)$.

Proof First note that N is an irreducible submodule in M iff (0) is an irreducible submodule in M/N. Suppose $E(M/N) = E_1 \oplus E_2$. Let $i : M/N \to E(M/N)$ be the canonical injection and let $\pi_i : E(M/N) \to E_i$ be the projection maps for $i = 1, 2$. Then $(\pi_i \circ i)^{-1}(0)$ is a proper submodule of M/N for $i = 1, 2$. Since $\pi_1^{-1}(0) \cap \pi_2^{-1}(0) = 0$, we have that $(\pi_1 \circ i)^{-1}(0) \cap (\pi_2 \circ i)^{-1}(0) = (0)$. This contradicts the fact that (0) is an irreducible submodule of M/N. So $E(M/N)$ is indecomposable. ■

Proposition 7.26 *Suppose A is Noetherian and M is an A-module, if there exists a decomposition*

$$0 = N_1 \cap \cdots \cap N_r$$

where each N_i is irreducible, then

$$E_A(M) = \bigoplus_{i=1}^{r} E_A(M/N_i).$$

Proof Since $0 = N_1 \cap \cdots \cap N_r$, we have an injection

$$\alpha : M \hookrightarrow \bigoplus_{i=1}^{r} M/N_i.$$

Hence we have an injection

$$E(M) \hookrightarrow \bigoplus_{i=1}^{r} E(M/N_i).$$

To show this is also a surjection, it suffices to show that $\alpha : M \hookrightarrow \bigoplus_{i=1}^{r} M/N_i$ is an essential extension.

For any $i = 1, \ldots, r$, we have an injection

$$\overline{N}_i := N_1 \cap \cdots \cap \widehat{N_i} \cap \cdots \cap N_r \hookrightarrow M/N_i,$$

where the hat $\widehat{\ }$ means that N_i is removed. Let $T \subseteq M/N_i$. Since N_i is irreducible in M, $T \cap \overline{N}_i \neq 0$. Hence $\overline{N}_i \hookrightarrow M/N_i$ is an essential extension. We leave it to the reader to show that this implies that $\alpha : M \hookrightarrow \bigoplus_{i=1}^{r} M/N_i$ is an essential extension. ■

Definition Define

$$\boldsymbol{\mu}_0(\mathfrak{p}, M) := \left\{ \begin{array}{l} \text{the number of copies of } E_A(A/\mathfrak{p}) \\ \text{in a decomposition of } E_A(M) \text{ as a} \\ \text{direct sum of indecomposable in-} \\ \text{jective modules} \end{array} \right\}.$$

Proposition 7.27 *If A is Noetherian and M is an A-module, then*

$$\boldsymbol{\mu}_0(\mathfrak{p}, M) = \dim_{\boldsymbol{\kappa}(\mathfrak{p})} \operatorname{Hom}_{A_\mathfrak{p}}(\boldsymbol{\kappa}(\mathfrak{p}), M_\mathfrak{p}).$$

Hence $\boldsymbol{\mu}_0(\mathfrak{p}, M)$ is well-defined.

Proof This follows from the definition and from part (6) of Theorem 7.9. ■

Definition Given a minimal injective resolution of M,

$$0 \to M \to E^0 \to E^1 \to E^2 \to \cdots$$

we define

$$\boldsymbol{\mu}_i(\mathfrak{p}, M) := \{\text{the number of copies of } E_A(A/\mathfrak{p}) \text{ in } E^i\}.$$

Corollary 7.28 *Given a Noetherian ring A and an A-module M with a minimal injective resolution*

$$0 \to M \to E^0 \to E^1 \to E^2 \to \cdots$$

we have:

$$E^i = \bigoplus_{\mathfrak{p} \in \operatorname{Spec}(A)} E_A(A/\mathfrak{p})^{\boldsymbol{\mu}_i(\mathfrak{p}, M)}$$

Exercise 7.29 *Show that if $\mathfrak{p} \cap S \neq \varnothing$, then $\boldsymbol{\mu}_i(\mathfrak{p}, M) = \boldsymbol{\mu}_i(\mathfrak{p}S^{-1}A, S^{-1}M)$. Hence if $0 \to M \to E_\bullet$ is an injective resolution of M, $0 \to M_\mathfrak{p} \to (E_\bullet)_\mathfrak{p}$ is an injective resolution of $M_\mathfrak{p}$ over $A_\mathfrak{p}$.*

Exercise 7.30 *Show that* $\operatorname{id}_A(M) = \sup_{\mathfrak{p} \in \operatorname{MaxSpec}(A)} \operatorname{id}_{A_\mathfrak{p}}(M)$.

WARNING 7.31 *Contrary to the case with projective dimension, even if $\operatorname{id}_{A_\mathfrak{p}} M_\mathfrak{p} < \infty$ for all $\mathfrak{p} \in \operatorname{Spec}(A)$, it is possible that $\operatorname{id}_A(M) = \infty$.*

Proposition 7.32 *If A is Noetherian and M is an A-module, then*

$$\boldsymbol{\mu}_i(\mathfrak{p}, M) = \dim_{\boldsymbol{\kappa}(\mathfrak{p})} \operatorname{Ext}^i_{A_\mathfrak{p}}(\boldsymbol{\kappa}(\mathfrak{p}), M_\mathfrak{p}).$$

In particular, $\boldsymbol{\mu}_i(\mathfrak{p}, M) < \infty$ for all i and all $\mathfrak{p} \in \operatorname{Spec}(A)$.

Proof By the previous exercise, by replacing A by $A_\mathfrak{p}$ and M by $M_\mathfrak{p}$ we may assume that A is local. Let

$$0 \to M \to E^0 \xrightarrow{d^0} E^1 \xrightarrow{d^1} \cdots$$

be a minimal injective resolution of M. Then $\operatorname{Ext}^i_A(k, M) = H^i(k, E^\bullet)$. We can identify $\operatorname{Hom}_A(k, E^i)$ with the submodule $T^i = (0 : E^i\mathfrak{m})$ of E^i. By construction E^i is an essential extension of the image $d^{i-1}(E^{i-1})$. So for $x \in T^i$, $Ax \cap d^{i-1}(E^{i-1}) \neq$. Since $Ax \cong k$, we have $x \in d^{i-1}(E^{i-1})$. Thus $d^i(T^i) = 0$. So the complex $\operatorname{Hom}_A(k, E^\bullet) \cong T^\bullet$ is exact. Hence

$$\operatorname{Hom}_A(k, E^i) \cong \operatorname{Ext}^i_A(k, M).$$

Thus

$$\boldsymbol{\mu}_i(\mathfrak{p}, M) = \boldsymbol{\mu}_0(E^i) = \dim_k(\operatorname{Hom}_A(k, E^i) = \dim_k \operatorname{Ext}^i_A(k, M).$$

■

Proposition 7.33 *If*

$$E^0 \to E^1 \to E^2 \to \cdots$$

is a minimal injective resolution of an A-module M and $x \in A$ is a nonzerodivisor on A and M, then

$$(0 :_{E^0} x) \to (0 :_{E^1} x) \to (0 :_{E^2} x) \to \cdots$$

is a minimal injective resolution of M/xM over A/xA.

Proof Since x is a nonzerodivisor on A,

$$0 \to A \xrightarrow{x} A \to A/xA \to 0$$

is a minimal free resolution of A/xA over A. Since x is a nonzerodivisor on M, $\operatorname{Hom}_A(A/xA, M) = 0$. Hence $\operatorname{Ext}^i_A(A/xA, M) = M/xM$ if $i = 1$ and 0 otherwise. Break up the minimal injective resolution of M as follows:

$$0 \to M \to E_0(M) \to D \to 0$$

$$0 \to D \to E_1(M) \to E_2(M) \to \cdots .$$

Note that the second exact sequence is an injective resolution $E^\bullet$ of D. Since x is a nonzerodivisor on M, x is a nonzerodivisor on $E_0(M)$. So the following sequence is exact

$$0 \to \operatorname{Hom}_A(A/xA, D) \to \operatorname{Ext}^1_A(A/xA, M) \to 0$$

In other words, $(0 :_D x) = M/xM$. Since $E_0(M)$ is injective, $\operatorname{Ext}^i_A(A/xA, E_0(M)) = 0$ for $i > 0$ and so $\operatorname{Ext}^i_A(A/xA, D) \cong \operatorname{Ext}^{i+1}_A(A/xA, M) = 0$ for $i \geq 1$. Furthermore, since $H^i(\operatorname{Hom}_A(A/xA, E^\bullet)) = \operatorname{Ext}^i_A(A/xA, D) = \operatorname{Ext}^{i+1}_A(A/xA, M) = 0$ for $i > 0$, for $i \geq 0$, applying the functor $\operatorname{Hom}_A(A/xA, -)$ to $0 \to D \to E_1(M) \to E_2(M) \to \cdots$ yields the exact sequence

$$0 \to (0 :_D x) \to (0 :_{E_1(M)} x) \to (0 :_{E_2(M)} x) \to \cdots .$$

It follows that this is a minimal injective resolution of $M/xM = (0 :_D x)$ over A/xA. ■

Corollary 7.34 *If M is an A-module and $x \in \mathfrak{p}$ is a nonzerodivisor on both A and M, then*

$$\boldsymbol{\mu}_i(\mathfrak{p}/xA, M/xM) = \boldsymbol{\mu}_{i+1}(\mathfrak{p}, M).$$

Corollary 7.35 *Given an A-module M with finite injective dimension and $x \in A$ a nonzerodivisor on both A and M, then M/xM has finite injective dimension over A/xA.*

Proposition 7.36 *If A is Noetherian, M is a finitely generated A-module and $\mathfrak{p} \subsetneq \mathfrak{q}$ are two primes with no other prime between, then*

$$\boldsymbol{\mu}_i(\mathfrak{p}, M) \neq 0 \qquad \textit{implies that} \qquad \boldsymbol{\mu}_{i+1}(\mathfrak{q}, M) \neq 0$$

Proof Localizing at $\mathfrak{q}$ we can assume that A is local with maximal ideal $\mathfrak{q}$. Pick $x \in \mathfrak{q} - \mathfrak{p}$. Then we have the exact sequence

$$0 \to A/\mathfrak{p} \xrightarrow{x} A/\mathfrak{p} \to A/(\mathfrak{p} + xA) \to 0.$$

In particular, $\dim(A/(\mathfrak{p} + xA)) = 0$. So $A/(\mathfrak{p} + xA)$ has a filtration with successive quotients equal to $k = A/\mathfrak{q}$. Taking the long exact sequence for Ext associated to the above short exact sequence we get that

$$\cdots \to \operatorname{Ext}^i_A(A/\mathfrak{p}, M) \xrightarrow{x} \operatorname{Ext}^i_A(A/\mathfrak{p}, M) \to \operatorname{Ext}^{i+1}_A(A/(\mathfrak{p} + xA), M) \to \cdots$$

is exact. By Nakayama's Lemma, $x \operatorname{Ext}^i_A(A/\mathfrak{p}, M) \neq \operatorname{Ext}^i_A(A/\mathfrak{p}, M)$ since by assumption $\operatorname{Ext}^i_A(A/\mathfrak{p}, M) \neq 0$. Thus $\operatorname{Ext}^{i+1}_A(A/(\mathfrak{p} + xA)) \neq 0$. By considering the filtration of the finite length module $A/(\mathfrak{p} + xA)$ one sees that $\operatorname{Ext}^{i+1}_A(A/\mathfrak{q}, M) \neq 0$, which is what we wanted to prove. ■

Corollary 7.37 *If A is a Noetherian ring and M is a finitely generated A-module, then* $\operatorname{id}_A(M) \geq \dim(M)$.

Proof Take $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq p_n$ a maximal chain of prime ideals in $\operatorname{Supp}_A(M)$. Then $\mathfrak{p}_0 \in \operatorname{Ass}_A(M)$ so there is an injection $A/\mathfrak{p}_0 \hookrightarrow M$. Hence we have $E_0(A/\mathfrak{p}_0) \hookrightarrow E_0(M)$. By the previous proposition, $E_i(A/\mathfrak{p}_i) \hookrightarrow E_i(M)$ for $i = 0, \ldots, n$. Thus $\operatorname{id}_A(M) \geq \dim(M)$. ■

Proposition 7.38 *Suppose A is local and M is a nonzero finitely generated A-module. If* $\operatorname{id}_A(M) < \infty$, *then* $\operatorname{id}_A(M) = \operatorname{depth}(A)$.

Proof Set $s = \operatorname{depth}(A)$ and $r = \operatorname{id}_A(M)$. Let $x_1, \ldots, x_s$ be a maximal A-sequence. Using Koszul Cohomology, we see that

$$\operatorname{Ext}^s_A(A/\mathbf{x}A, M) = H^s(\mathbf{x} : M) = M/\mathbf{x}M$$

and $H^s(\mathbf{x}, M) = \operatorname{Ext}^i_A(A/\mathbf{x}A, M) = 0$ for $i \neq s$. Thus $s \leq r$.

Since $\operatorname{depth}(A/\mathbf{x}A) = 0$ we have an exact sequence of the form

$$0 \to k \to A/\mathbf{x}A \to L \to 0.$$

Since $\operatorname{id}_A(M) = r$, we have the exact sequence

$$\cdots \to \operatorname{Ext}^r_A(A/\mathbf{x}A, M) \to \operatorname{Ext}^r_A(k, M) \to 0.$$

Further we have $\boldsymbol{\mu}_r(\mathfrak{m}; M) \neq 0$. Thus $\operatorname{Ext}^r_A(k, M) \neq 0$, and hence $\operatorname{Ext}^r_A(A/\mathbf{x}A, M) \neq 0$. Since $A/\mathbf{x}A$ has free resolution $K_\bullet(\mathbf{x}; A)$, the Koszul complex with length s, we must have $r \leq s$. Combining the two parts we have $r = s$. ■

Corollary 7.39 *If A is local with finite injective dimension as a module over itself, then it is Cohen-Macaulay.*

Proof Use the previous two propositions. ■

Up to this point, the work we have done is mostly elementary in nature—we have needed no "weapons of mass destruction" to prove our results. The above corollary clearly motivates the next theorem, whose proof however, is quite nontrivial and will not be presented here.

Theorem 7.40 (Bass' Conjecture) *If A is local and M is a nonzero finitely generated A-module such that $\operatorname{id}_A(M) < \infty$, then A is Cohen-Macaulay.*

In 1971 Peskine and Szpiro proved this theorem in nearly every case when A contains a field. To do this they used Artin Approximation, characteristic p techniques, reduction from characteristic 0 to characteristic p, and worked a bit in the derived category. Later in 1976, Hochster proved the above theorem for every case when A contains a field. To do this, he proved the existence of balanced big Cohen-Macaulay modules. Finally Roberts in 1987 used intersection theory and characteristic p techniques to prove the mixed characteristic cases.

7.4 Gorenstein Rings

Definition A local ring is called a **Gorenstein ring** if it has finite injective dimension as a module over itself.

Lemma 7.41 (Gorenstein Rings in Dimension Zero) *If $(A, \mathfrak{m}, k)$ is local and $\dim(A) = 0$, then the following are equivalent:*

(1) $\operatorname{id}_A(A) < \infty$.

(2) *A is injective as an A-module.*

(3) $A \cong E_A(k)$.

(4) $\mathrm{Hom}_A(k, A) \cong k$.

(5) *(0) is an irreducible ideal in A.*

(6) *There exists a unique nonzero minimal ideal in A.*

Proof (1) $\Rightarrow$ (2) Suppose $\mathrm{id}_A(A) < \infty$. Then by Proposition 7.38 $\mathrm{id}_A(A) = \mathrm{depth}(A) = 0$. Therefore A is injective over itself.

(2) $\Rightarrow$ (3) By assumption A is injective as an A-module. Since A is local, A is indecomposable and so isomorphic to $E_A(A/\mathfrak{p})$ for some prime $\mathfrak{p}$. Since $\mathrm{depth}(A) = \dim(A) = 0$, we have $\mathrm{Ass}_A(A) = \{\mathfrak{m}\}$. Thus $A \cong E_A(k)$.

(3) $\Rightarrow$ (4) By assumption $A \cong E_A(k) = E$. Thus $\mathrm{Hom}_A(k, A) \cong \mathrm{Hom}_A(k, E)$. We can identify $V = \{e \in E : \mathfrak{m}e = 0\}$ with $\mathrm{Hom}_A(k, E)$. Then V is a nonzero vector space over k inside E and $k \hookrightarrow E$ is an essential extension and so we must have $V \cong k$.

(4) $\Rightarrow$ (5) Suppose $\mathrm{Hom}_A(k, A) = k$. Further suppose that I_1, I_2 are proper ideals of A such that $I_1 \cap I_2 = (0)$. Since $\lambda(A) < \infty$ we have $\lambda(I_1), \lambda(I_2) < \infty$. Hence if $I_1, I_2 \neq 0$ we have injections $k \hookrightarrow I_1$ and $k \hookrightarrow I_2$. But this contradicts $\mathrm{Hom}_A(k, A) = k$. Hence $I_1 = 0$ or $I_2 = 0$.

(5) $\Rightarrow$ (4) Suppose the zero ideal (0) is irreducible. Since $\mathrm{Hom}_A(k, A)$ is a vector space over k, we have $\mathrm{Hom}_A(k, A) \cong k^r$. If $r > 1$ then there are distinct copies of k (ideals) in A whose intersection is necessarily the zero ideal. This contradicts our assumption. Hence $r = 1$.

(4) $\Rightarrow$ (6) Suppose $\mathrm{Hom}_A(k, A) = k$. Then every nonzero ideal I, being a submodule of a finite length module, has finite length. Hence there is an injection $k \hookrightarrow I$. Consider the image I_0 of k under one of the nonzero maps to A. Then every ideal I must contain I_0, for otherwise we have disjoint ideals in A isomorphic to k as A-modules, which implies that $\mathrm{Hom}_A(k, A) = \bigoplus_{i=1}^{r} k$ with $r \geq 2$. Thus I_0 is the unique minimal ideal in A.

(6) $\Rightarrow$ (1) Suppose now that A has a unique minimal ideal I_0. Since $\lambda(A) = 0$, $I_0 \cong k$. Since I_0 is minimal, $k = I_0 \to A$ is an essential extension. It follows that $A \hookrightarrow E_A(k)$. Since $\lambda(A) = \lambda(E_A(k))$ (Theorem 7.16), we have $A = E_A(k)$. Thus A is injective and so has finite injective dimension. ■

Proposition 7.42 *If $(A, \mathfrak{m}, k)$ is a local ring with $\mathrm{id}_A(A) = \infty$, then $\boldsymbol{\mu}_i(\mathfrak{m}, A) \neq 0$ for all $i \geq \dim(A)$.*

Proof We proceed by induction on $\dim(A)$. If $\dim(A) = 0$, then every module in an injective resolution of A is of the form $\bigoplus E_A(k)$ and we are done. So now assume $\dim(A) = n$ and the proposition is true for rings of smaller dimension. Take $\mathfrak{p} \neq \mathfrak{m}$ a prime ideal. If $\mathrm{id}_{A_\mathfrak{p}}(A_\mathfrak{p}) = \infty$, then by induction $\mu_i(\mathfrak{p}A_\mathfrak{p}; A_\mathfrak{p}) = \boldsymbol{\mu}_i(\mathfrak{p} : A) \neq 0$ for $i \geq \mathrm{ht}(\mathfrak{p})$. Taking a saturated chain of primes

$$\mathfrak{p} = P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = \mathfrak{m}$$

we see that $n + \mathrm{ht}(\mathfrak{p}) \leq \dim(A)$ and $\boldsymbol{\mu}_i(\mathfrak{m}; A) \neq 0$ for all $i \geq n + \mathrm{ht}(\mathfrak{p})$.

Otherwise, $\mathrm{id}_{A_\mathfrak{p}}(A_\mathfrak{p}) < \infty$ for all nonmaximal primes $\mathfrak{p}$. Since $\mathrm{id}_{A_\mathfrak{p}}(A_\mathfrak{p}) = \dim(A_\mathfrak{p}) = \mathrm{ht}(\mathfrak{p})$, we have that $\boldsymbol{\mu}_i(\mathfrak{p}; A) = 0$ for $i > \mathrm{ht}(\mathfrak{p})$. Thus $\boldsymbol{\mu}_i(\mathfrak{p} : A) = 0$ for all nonmaximal primes $\mathfrak{p}$ and for all $i \geq \dim(A)$. Therefore, since $\mathrm{id}_A(A) = \infty$ we have $\boldsymbol{\mu}_i(\mathfrak{m}; A) \neq 0$ for all $i \geq \dim(A)$. ■

Theorem 7.43 *If $(A, \mathfrak{m}, k)$ is a local ring of dimension n, then the following are equivalent:*

(1) $\mathrm{id}_A(A) < \infty$. *(i.e. A is Gorenstein.)*

(2) $\boldsymbol{\mu}_i(\mathfrak{m}, A) = 0$ *for all* $i > n$.

(3) $\boldsymbol{\mu}_i(\mathfrak{m}, A) = 0$ *for some* $i > n$.

(4) $\boldsymbol{\mu}_i(\mathfrak{m}, A) = 0$ *for some* $i \neq n$, $\boldsymbol{\mu}_n(\mathfrak{m}, A) = 1$.

(5) A *is Cohen-Macaulay and* $\dim_k \mathrm{Ext}^n_A(k, A) = 1$.

(6) $\boldsymbol{\mu}_i(\mathfrak{p}, A) = \delta_{i,\mathrm{ht}(\mathfrak{p})}$ *where*

$$\delta_{i,\mathrm{ht}(\mathfrak{p})} = \begin{cases} 0 & \text{if } i \neq \mathrm{ht}(\mathfrak{p}), \\ 1 & \text{if } i = \mathrm{ht}(\mathfrak{p}). \end{cases}$$

(7) *Every system of parameters of A generates an irreducible ideal of height n in A.*

Proof We prove the following implications, which suffice to prove the equivalence:

$$(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (1) \quad (1) \Rightarrow (4) \Rightarrow (6) \Rightarrow (1) \quad (7) \Leftrightarrow (1) \quad (5) \Leftrightarrow (4).$$

(1) $\Rightarrow$ (2) Obvious.

(2) $\Rightarrow$ (3) Obvious.

(3) $\Rightarrow$ (1) This follows from the previous proposition.

(1) $\Rightarrow$ (4) Since $\mathrm{id}_A(A) < \infty$, A is Cohen-Macaulay by Corollary 7.39. Hence $\mathrm{depth}(A) = n$. Thus $\mathrm{Ext}^i_A(k, A) = 0$ for $i < n$. By the long exact sequence of Ext we have

$$\mathrm{Ext}^n_A(k, A) \cong \mathrm{Hom}_A(k, A/(x_1, \ldots, x_n)),$$

where $x_1, \ldots, x_n$ is a maximal A-sequence. Further we have that

$$\mathrm{id}_{A/(x_1,\ldots,x_n)A}(A/(x_1, \ldots, x_n)A) = 0.$$

So by the zero-dimensional case,

$$\begin{aligned} k &= \mathrm{Hom}_{A/(x_1,\ldots,x_n)A}(k, A/(x_1, \ldots, x_n)A), \\ &= \mathrm{Hom}_A(k, A/(x_1, \ldots, x_n)A), \\ &= \mathrm{Ext}^n_A(k, A). \end{aligned}$$

(4) $\Rightarrow$ (6) Clearly if $\mathrm{id}_A(A) < \infty$ we have $\mathrm{id}_{A_\mathfrak{p}}(A_\mathfrak{p}) < \infty$. Since $\boldsymbol{\mu}_i(\mathfrak{p}; A) = \boldsymbol{\mu}_i(\mathfrak{p}A_\mathfrak{p}; A_\mathfrak{p})$ we get that $\boldsymbol{\mu}_i(\mathfrak{p}; A) = \delta_{i,\mathrm{ht}(\mathfrak{p})}$.

(6) $\Rightarrow$ (1) Use that

$$\mathrm{id}_A(A) = \sup\{i : \mathrm{Ext}^i_A(k, A) \neq 0\} = \sup\{i : \boldsymbol{\mu}_i(\mathfrak{m}; A) \neq 0\}.$$

(1) $\Rightarrow$ (7) Suppose $\mathrm{id}_A(A) < \infty$. Then by the above implications, A is Cohen-Macaulay and $\mathrm{Ext}^n_A(k, A) \cong k$. Let $x_1, \ldots, x_n$ be any system of parameters. Since A is Cohen-Macaulay, any system of parameters is a maximal A-sequence. So by the long exact sequence of Ext we have that $\mathrm{Hom}_{A/\mathbf{x}}(k, A/\mathbf{x}) = \mathrm{Hom}_A(k, A/\mathbf{x}) = k$. Thus $A/\mathbf{x}$ is a zero-dimensional Gorenstein ring. Thus (0) is an irreducible ideal in $A/\mathbf{x}$, or in other words, $(\mathbf{x})$ is an irreducible ideal in A.

(7) $\Rightarrow$ (1) Suppose that every system of parameters of A generates an irreducible ideal. If $\dim(A) = 0$, then A is Gorenstein by the lemma. So by induction we may assume the claim holds for local rings of dimension less then n. Suppose $\dim(A) = n$ and let $x_1, \ldots, x_n$ be a system of parameters. For every $t > 0$, we have

$$(0 :_A \mathfrak{m}) \subseteq ((x_1^{t+1}, \ldots, x_n^{t+1}) :_A \mathfrak{m}).$$

Since $x_1^{t+1}, \ldots, x_n^{t+1}$ is a system of parameters, $(x_1^{t+1}, \ldots, x_n^{t+1})$ is an irreducible ideal. Thus $\mathrm{Hom}_A(k, A/(x_1^{t+1}, \ldots, x_n^{t=1}) = k$. Therefore

$$((x_1^{t+1}, \ldots, x_n^{t+1}) :_A \mathfrak{m}) \subseteq (x_1^t, \ldots, x_n^t)$$

for all t. Therefore $(0 :_A \mathfrak{m}) \subseteq \bigcap_t (x_1^t, \ldots, x_n^t) = 0$. So $\mathrm{Hom}(A/\mathfrak{m}, A) = 0$ and hence $\mathrm{depth}(A) > 0$. So there is a regular element a on A. By induction $\mathrm{id}_{A/a}(A/a) < \infty$. Since A is local and a is a regular element, we have

$$\mathrm{id}_{A/a}(A/a) = \mathrm{id}_A(A) - 1.$$

(See Bruns and Herzog, Corollary 3.1.15.) Therefore $\mathrm{id}_A(A) < \infty$.

(4) $\Rightarrow$ (5) Since $\mathrm{id}_A(A) < \infty$, then A is Cohen-Macaulay by Corollary 7.39. By (4), $\dim_k \mathrm{Ext}^n_A(k, A) = \boldsymbol{\mu}_n(k, A) = 1$.

(5) $\Rightarrow$ (4) This follows from the Ext characterization of depth. ■

So we have the following implications for *local* rings:

Regular $\Rightarrow$ Complete Intersection $\Rightarrow$ Gorenstein $\Rightarrow$ Cohen-Macaulay

Corollary 7.44 *A is Gorenstein if and only if $\widehat{A}$ is Gorenstein.*

Proof We already know that A is Cohen-Macaulay if and only if $\widehat{A}$ is so. Since $\mathrm{Ext}^n_A(k, A) \cong \mathrm{Ext}^n_A(k, A) \otimes_A \widehat{A} = \mathrm{Ext}^n_{\widehat{A}}(k, \widehat{A})$, we see that $\boldsymbol{\mu}_n(\mathfrak{m}; A) = 1$ if and only if $\boldsymbol{\mu}_n(\mathfrak{m}\widehat{A}; \widehat{A}) = 1$. ■

Corollary 7.45 *If A is a local Gorenstein ring with $\dim(A) = d$, and if*

$$0 \to A \to E^0 \to E^1 \to \cdots \to E^d \to 0,$$

is the minimal injective resolution of A then

$$E^i = \bigoplus_{\mathrm{ht}(\mathfrak{p})=i} E_A(A/\mathfrak{p}).$$

Proof This follows from the above theorem. ■

Definition A cochain complex of injective modules

$$E^\bullet : 0 \to E^0 \to E^1 \to \cdots \to E^d \to 0$$

such that $E^i = \bigoplus_{\mathrm{ht}(\mathfrak{p})=i} E_A(A/\mathfrak{p})$, that is each copy of $E_A(A/\mathfrak{p})$ only occurs once in the decomposition of E^i, and such that the homology $H^i(E^\bullet)$ is finitely generated, is called a **dualizing complex** of A. So in particular, if A is Gorenstein, a minimal injective resolution of A is a dualizing complex for A.

Suppose that A is Gorenstein and

$$0 \to A \to E^0 \to E^1 \to \cdots \to E^d \to 0$$

is a minimal injective resolution of A. Now what are the maps in the above resolution? This is a hard question and the answer has to do with the Cousin complex. For more information, ses Hartshorne *Residue and Duality* or Sharp *Cousin Complex Gorenstein Rings*.

Definition If $(A, \mathfrak{m}, k)$ is local and Cohen-Macaulay, with $d = \dim(A)$, then we define the **type** of A to be:

$$\dim_k \mathrm{Ext}^d_A(k, A)$$

So we see that A is Gorenstein if and only if it is Cohen-Macaulay of type 1.

Example 7.46 *Let $A = k[\![t^3, t^4, t^5]\!]$. What is the dimension of A? Well*

$$k[\![t^3, t^4, t^5]\!] \hookrightarrow k[\![t]\!]$$

is an integral extension of A and since $\dim(k[\![t]\!]) = 1$ we have that $\dim(A) = 1$. So A is a Cohen-Macaulay ring of dimension 1. Now the type of A is

$$\dim_k \operatorname{Ext}^1_A(k, A).$$

We claim that

$$\dim_k \operatorname{Ext}^1_A(k, A) = \dim_k \operatorname{Hom}_A(k, A/xA)$$

where x is a parameter of A. To see the above statement, consider the short exact sequence

$$0 \to A \xrightarrow{x} A \to A/xA \to 0$$

and apply $\operatorname{Hom}_A(k, -)$. Now we obtain

$$0 \to \operatorname{Hom}_A(k, A/xA) \to \operatorname{Ext}^1_A(k, A) \xrightarrow{x} \operatorname{Ext}^1_A(k, A)$$

But note that the right most map is in fact the zero map, and hence our claim is true. So if $x = t^3$, then what is

$$\dim_k \operatorname{Hom}_A(k, \frac{k[\![t^3, t^4, t^5]\!]}{(t^3)})?$$

We know that if $\varphi : k[\![x, y, z]\!] \to k[\![t^3, t^4, t^5]\!]$ via

$$x \mapsto t^3, \qquad y \mapsto t^4, \qquad z \mapsto t^5,$$

then $\operatorname{Ker}(\varphi) = (xz - y\cdot x^3 - yz, x^2y - z^2)$, and so

$$k[\![t^3, t^4, t^5]\!] \cong k[\![x, y, z]\!]/\operatorname{Ker}(\varphi).$$

We deduce

$$k[\![t^3, t^4, t^5]\!]/t^3 \cong k[\![x, y, z]\!]/(x, \operatorname{Ker}(\varphi)) \cong k[\![y, z]\!]/(y^2, yz, z^2).$$

Now check that

$$\operatorname{Hom}_A(k, k[\![y, z]\!]/(y^2, yz, z^2)) \cong ky \otimes kz,$$

and hence has dimension 2. Thus A is not Gorenstein. Moreover it can be shown exactly when a ring is a quotient of an ideal generated by minors it is not Gorenstein. To clarify, if

$$A = \frac{k[\![x_{i,j}]\!]}{I_t}, \qquad 1 \le i \le m,\ 1 \le j \le n$$

and I_t is the ideal generated by $t \times t$ minors of

$$\begin{bmatrix} x_{1,1} & \dots & x_{1,n} \\ \vdots & & \vdots \\ x_{m,1} & \dots & x_{m,n} \end{bmatrix},$$

then $\operatorname{ht}(I_t) = (m-t+1)(n-t+1)$ *and* $\dim(A) = mn - \operatorname{ht}(I_t)$. *A theorem of Hochster and Eagon states that A/I_t is normal and Cohen-Macaulay for $t \leq \min\{m,n\}$, and a theorem of Svanes says that A/I_t is Gorenstein if and only if $m = n$ and $0 < t < \min\{m,n\}$. For the maximal minor case, that is when $t = m \leq n$, then A/I_t is Gorenstein if and only if $t = m = n$ or $t = m = 1$. In the case of the example above,* $\operatorname{Ker}(\varphi)$ *was the ideal generated by the* 2×2 *minors of*

$$\begin{bmatrix} x & y & z \\ y & z & x^2 \end{bmatrix}.$$

This is not quite a generic matrix, but if we take the above result for the matrix

$$\begin{bmatrix} x & y & z \\ u & v & w \end{bmatrix}.$$

and the corresponding determinantal ideal in $k[u,v,w,x,y,z]$ and mod out by the regular sequence $u-y, v-z, w-x^2$, we can carry the above result about the Gorenstein property to the previous case.

Let B be a regular local ring and consider $A = B/I$ where I is chosen such that A is Cohen-Macaulay. Then

$$\operatorname{pd}_B(A) + \operatorname{depth}(A) = \operatorname{depth}(B),$$

and so

$$\begin{aligned} \operatorname{pd}_B(A) &= \operatorname{depth}(B) - \operatorname{depth}(A), \\ &= \dim(B) - \dim(A), \\ &= \operatorname{ht}(I). \end{aligned}$$

Hence we can take a minimal free resolution of A over B, where $d = \operatorname{ht}(I)$:

$$F_\bullet : \qquad 0 \to B^{t_d} \to \cdots \to B^{t_1} \to B \to A \to 0$$

Since $\operatorname{depth}_I(B) = \operatorname{ht}(I) = n$, we have

$$\operatorname{Ext}^i_B(A,B) = 0 \qquad i < n. \tag{$\bigstar$}$$

Apply $\operatorname{Hom}_B(-,B)$ to $F_\bullet$ to get

$$0 \to B \xrightarrow{d_1^*} B^{t_1} \to \cdots \xrightarrow{d_n^*} B^{t_n} \to \Omega \to 0$$

where $\Omega = \text{Coker}(d_n^*)$. Since $IA = 0$, and $\Omega = \text{Ext}_B^n(A, B)$, we see that $I\Omega = 0$, and hence $I \subseteq \text{Ann}_A(\Omega)$. Moreover if we apply $\text{Hom}_B(-, B)$ to $F_\bullet^*$, a minimal free resolution of Ω by ($\bigstar$), we get $F_\bullet$ and so

$$\text{Ext}_B^i(\Omega, B) = \begin{cases} 0 & \text{if } i < d, \\ A & \text{if } i = d. \end{cases}$$

Thus $\text{Ann}_A(\Omega)\Omega = 0$ implies that $\text{Ann}_A(\Omega)A = 0$ which show us that $I \supseteq \text{Ann}_A(\Omega)$ and so $I = \text{Ann}_A(\Omega)$.

Remark While our decision to denote $\text{Coker}(d_n^*)$ by Ω may seem a bit arbitrary, we actually did it for a good reason. You will later see that Ω is the *canonical module* for A.

Theorem 7.47 *The type of A is $\mu(\Omega)$ where Ω is as above.*

The proof of the above theorem will be provided later in the next section.

Corollary 7.48 *If A is Cohen-Macaulay and is the quotient of a regular ring B, then the following are equivalent:*

(1) *A is Gorenstein.*

(2) *The type of A is* 1.

(3) $\boldsymbol{\mu}(\Omega) = 1$.

(4) *Ω is cyclic.*

(5) $\Omega \cong A$.

(6) $A \cong \text{Ext}_B^d(A, B)$ *where* $d = \text{pd}_B(A)$.

Proof Exercise. ■

Exercise 7.49 *If*

$$0 \to A^{t_n} \to \cdots \to A^{t_0} \to M \to 0$$

is a minimal free resolution of M, then show $\text{Ext}_A^n(M, A) \neq 0$.

Theorem 7.50 *If $(A, \mathfrak{m}, k)$ is a local Gorenstein ring and $x_1, \ldots, x_d$ is any system of parameters for A, then*

$$E_A(k) = \varinjlim_t (A/(x_1^t, \ldots, x_d^t)A).$$

Proof Let $x_1, \ldots, x_n$ be a system of parameters for A. Since every $e \in E$ is killed by a power of the maximal ideal and since the ideal $\mathbf{x}$ generated by the system of paramters and $\mathfrak{m}$ are cofinal, we have that $E_A(k) = E = \bigcup_t E_t$ where

$$E_t = \{e \in E : \mathbf{x}^t e = 0\} = \text{Hom}_A(A/\mathbf{x}^t A, E).$$

Take a minimal injective resolution $E^\bullet$ of A. Since A is Gorenstein, $E^i = \bigoplus_{\mathrm{ht}(\mathfrak{p})=i} E_A(A/\mathfrak{p})$. Thus $\mathrm{Hom}_A(A/\mathbf{x}^t A, E^i) = 0$ for $i < n$. So for each $t > 0$ we get a commutative diagram

$$\begin{array}{ccc} \mathrm{Ext}^n_A(A/\mathbf{x}^t A, A) & \xrightarrow{\cong} & \mathrm{Hom}_A(A/\mathbf{x}^t A, E) \\ \downarrow & & \vdots \\ \mathrm{Ext}^n_A(A/\mathbf{x}^{t+1} A, A) & \xrightarrow{\cong} & \mathrm{Hom}_A(A/\mathbf{x}^{t+1} A, E). \end{array}$$

So $\varinjlim_t E_t = \varinjlim_t \mathrm{Ext}^n_A(A/\mathbf{x}^t A, A)$. Since A is Gorenstein, it is Cohen-Macaulay. Therefore $x_1^t, \ldots, x_n^t$ is a maximal A-sequence for all $t > 0$. Thus $\mathrm{Ext}^n_A(A/\mathbf{x}^t A, A) = A/\mathbf{x}^t A$ and we are done. ■

Exercise 7.51 *If A is Cohen-Macaulay and $x_1, \ldots, x_d$ is a system of parameters for A, then the map (in the missing above proof) is injective.*

Exercise 7.52 *Letting*

$$A = k[X_1, \ldots, X_d] \text{ or } A = k[\![X_1, \ldots, X_d]\!] \text{ or } A = k[X_1, \ldots, X_d]_{(X_1, \ldots, X_d)}$$

whatever you prefer, show that $E_A(k)$ is a vector space with basis:

$$\left\{ \frac{1}{X_1^{p_1} \cdots X_d^{p_d}} : p_i > 0 \right\} \subseteq k(X_1, \ldots, X_d)$$

Definition If A is a Noetherian ring, A is called **Gorenstein** if for every maximal ideal $\mathfrak{m}$, $A_\mathfrak{m}$ is Gorenstein. Note this is true if and only if for every $\mathfrak{p} \in \mathrm{Spec}(A)$, $A_\mathfrak{p}$ is Gorenstein.

Exercise 7.53 *A Noetherian ring A is Gorenstein if and only if for every finitely generated A-module M*

$$\mathrm{grade}_A \mathrm{Ext}^i_A(M, A) \geq i.$$

Exercise 7.54 *Consider a Noetherian ring A with finite injective dimension. Show that*

$$\mathrm{id}_A(A) = \dim(A).$$

Note that:

$$\text{Regular} \Rightarrow \text{Complete Intersection} \Rightarrow \text{Gorenstein} \Rightarrow \text{Cohen-Macaulay}$$

Example 7.55 *Consider $A = \mathbb{Z}$. Note we have an injective resolution of $\mathbb{Z}$*

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0.$$

Is $\mathbb{Q}/\mathbb{Z}$ indecomposable? No. From Corollary 7.45 we see that

$$\bigoplus_{p\text{prime}} \mathbb{Q}/\mathbb{Z} \cong E_\mathbb{Z}(\mathbb{Z}/p\mathbb{Z})$$

where

$$E_\mathbb{Z}(\mathbb{Z}/p\mathbb{Z}) \cong \varinjlim(\mathbb{Z}/p\mathbb{Z} \xrightarrow{p} \mathbb{Z}/p\mathbb{Z} \xrightarrow{p^2} \cdots).$$

LET'S GET TOGETHER AND DISCUSS THIS :)

7.5 Grothendieck's Functorial Approach

Let A be a Noetherian ring, $\mathfrak{m}$ **any** ideal of A (this follows Grothendieck's notation; often $\mathfrak{m}$ is the maximal ideal in a local ring), and define:

$\mathbf{Ab}$	=	The category of Abelian groups.
$\mathbf{C}$	=	The category of A-modules.
$\mathbf{C}_{\mathfrak{m}}$	=	The category of A-modules with support contained in $V(\mathfrak{m})$.
$\mathbf{C}^{\mathrm{f}}$	=	The category of finitely generated A-modules.
$\mathbf{C}^{\mathrm{f}}_{\mathfrak{m}}$	=	The category of finitely generated A-modules with support contained in $V(\mathfrak{m})$.

Proposition 7.56 *Let $\mathcal{T}$ be a contravarient additive functor from $\mathbf{C}$ to $\mathbf{Ab}$. Then there exits a natural transformation*

$$\eta : \mathcal{T} \to \mathrm{Hom}_A(-, \mathcal{T}(A)).$$

That is, if $f : M \to N$, then the following diagram commutes:

$$\begin{array}{ccc} \mathcal{T}(N) & \xrightarrow{\eta_N} & \mathrm{Hom}_A(N, \mathcal{T}(A)) \\ {\scriptstyle \mathcal{T}(f)}\downarrow & & \downarrow{\scriptstyle \mathrm{Hom}_A(f, \mathcal{T}(A))} \\ \mathcal{T}(M) & \xrightarrow{\eta_M} & \mathrm{Hom}_A(M, \mathcal{T}(A)) \end{array}$$

Proof First note that for $M \in \mathbf{C}$, $\mathcal{T}(M) \in \mathbf{C}$. The A-action that turns $\mathcal{T}(M)$ into an A-module is given by $a \cdot x = \mathcal{T}(\mu_a)(x)$ for $x \in \mathcal{T}(M)$ and where $\mu_a : M \to M$ is the multiplication by a map.

Now for $x \in M$, define a homomorphism $\epsilon_x : A \to M$ by setting $\epsilon_x(1) = x$. Then, since $\mathcal{T}$ is contravariant, we get a homomorphism $\mathcal{T}(\epsilon_x) : \mathcal{T}(M) \to \mathcal{T}(A)$. Now we can define a homomorphism $\eta_M : \mathcal{T}(M) \to \mathrm{Hom}_A(M, \mathcal{T}(A))$ by setting $\eta_M(w)(x) = \mathcal{T}(\epsilon_x)(w)$ for $x \in M$ and $w \in \mathcal{T}(M)$. We leave it to the reader to check that Φ_M is the natural transformation we sought. ■

Proposition 7.57 *Let $\mathcal{T}$ be a contravarient additive functor from $\mathbf{C}^{\mathrm{f}}$ to $\mathbf{Ab}$. The natural tranformation*

$$\eta : \mathcal{T} \to \mathrm{Hom}_A(-, \mathcal{T}(A))$$

is a natural isomorphism if and only if $\mathcal{T}$ is left exact.

Proof If η is a natural isormorphism, then since $\mathrm{Hom}_A(-, \mathcal{T}(A))$ is left exact, so is $\mathcal{T}$.

Now suppose that $\mathcal{T}$ is left exact. First note that since $\mathcal{T}(A) \cong \mathrm{Hom}_A(A, \mathcal{T}(A))$, and since $\mathcal{T}(A)$ is additive, we have that η_F is an isomorphism for any finitely generated free A-module F. Let $M \in \mathbf{C}^{\mathrm{f}}$ and let $A^m \to A^n \to M \to 0$ be a presentation of M. Then we have a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathcal{T}(M) & \longrightarrow & \mathcal{T}(A^n) & \longrightarrow & \mathcal{T}(A^m) \\ & & \downarrow{\scriptstyle \eta_M} & & \downarrow{\scriptstyle \eta_{A^n}} & & \downarrow{\scriptstyle \eta_{A^m}} \\ 0 & \longrightarrow & \mathrm{Hom}_A(M, \mathcal{T}(A)) & \longrightarrow & \mathrm{Hom}_A(A^n, \mathcal{T}(A)) & \longrightarrow & \mathrm{Hom}_A(A^m, \mathcal{T}(A)) \end{array}$$

where the rows are exact. Since A^n, A^m are finitely generated free modules, η_{A^n}, η_{A^m} are isomorphisms. Hence η_M is an isomorphism by the Five Lemma. ■

Corollary 7.58 *Let $\mathcal{T}$ be a contravarient additive functor from $\mathbf{C}^{\mathrm{f}}$ to $\mathbf{Ab}$. $\mathcal{T}$ is exact if and only if $T(A)$ is injective.*

Proof The functor $\mathrm{Hom}_A(-, N)$ is exact if and only if N is injective. By the previous proposition, $\mathcal{T}$ is naturally isormorphic to $\mathrm{Hom}_A(-, \mathcal{T}(A))$ if and only if $\mathcal{T}$ is left exact. ■

We now prove the analogous results in the category $\mathbf{C}^{\mathrm{f}}_{\mathfrak{m}}$.

Proposition 7.59 *Let $\mathcal{T}$ be a contravarient additive functor from $\mathbf{C}^{\mathrm{f}}_{\mathfrak{m}}$ to $\mathbf{Ab}$. Then there exits a natural transformation*

$$\varphi : \mathcal{T} \to \mathrm{Hom}_A(-, I),$$

where $I = \varinjlim_n (\mathcal{T}(A/\mathfrak{m}^n))$.

Proof Let $M \in \mathbf{C}^{\mathrm{f}}_{\mathfrak{m}}$. Since M is finitely generated, there exists $n > 0$ such that $\mathfrak{m}^n M = 0$. Thus M is a finitely generated module over $A/\mathfrak{m}^n$ for some $n > 0$. By Proposition 7.57 we have a natural map

$$\eta_{M,n} : \mathcal{T}(M) \to \mathrm{Hom}_{A/\mathfrak{m}^n}(M, \mathcal{T}(A/\mathfrak{m}^n)) = \mathrm{Hom}_A(M, \mathcal{T}(A/\mathfrak{m}^n)).$$

Moreover, the canonical surjection $A/\mathfrak{m}^{n+i} \to A/\mathfrak{m}^n$ induces maps

$$\mathrm{Hom}_A(M, \mathcal{T}(A/\mathfrak{m}^n)) \to \mathrm{Hom}_A(M, \mathcal{T}(A/\mathfrak{m}^{n+i})).$$

So we have a natural map

$$\varphi_M = \varinjlim_n \eta_{M,n} : \mathcal{T}(M) \to \varinjlim_n \mathrm{Hom}_A(M, \mathcal{T}(A/\mathfrak{m}^n)) = \mathrm{Hom}_A(M, \varinjlim_n \mathcal{T}(A/\mathfrak{m}^n)).$$

■

Proposition 7.60 *Let $\mathcal{T}$ be a contravarient additive functor from $\mathbf{C}^{\mathrm{f}}_{\mathfrak{m}}$ to $\mathbf{Ab}$. The natural transformation*

$$\varphi : \mathcal{T} \to \mathrm{Hom}_A(-, I),$$

with I as above, is a natural isomorphism if and only if $\mathcal{T}$ is left exact.

Proof If φ is a natural isomorphism, then $\mathcal{T}$ is left exact because $\mathrm{Hom}_A(-, I)$ is left exact.

So assume that $\mathcal{T}$ is left exact. Let $M \in \mathbf{C}^{\mathrm{f}}_{\mathfrak{m}}$. As before $\mathfrak{m}^n M = 0$ for all n sufficiently large. Thus we have natural isomorphisms

$$\mathcal{T}(M) \xrightarrow{\cong} \mathrm{Hom}_A(M, \mathcal{T}(A/\mathfrak{m}^n))$$

for n sufficiently large. This then induces a natural isomorphism

$$\mathcal{T}(M) \cong \varinjlim_n \mathrm{Hom}_A(M, \mathcal{T}(A/\mathfrak{m}^n)) = \mathrm{Hom}_A(M, I).$$

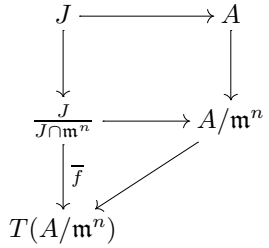
■

Corollary 7.61 *Let $\mathcal{T}$ be a contravarient additive functor from $\mathbf{C}^{\mathrm{f}}_{\mathfrak{m}}$ to $\mathbf{Ab}$. $\mathcal{T}$ is exact if and only if $I = \varinjlim(\mathcal{T}(A/\mathfrak{m}^n))$ is an injective A-module.*

Proof Using Baer's criterion, we must check that if $J \subseteq A$ is an ideal and $J \xrightarrow{f} I$ is an A-module map, then we can lift f to a map $\widetilde{f} : A \to I$ making the resulting triangle commute. Note that $f(J) \subseteq T(A/\mathfrak{m}^n)$ for $n >> 0$. Moreover $f(\mathfrak{m}^n J) = 0$ for $n >> 0$. By the Artin-Rees Lemma, we have

$$\mathfrak{m}^n \cap J = \mathfrak{m}^{n-t}(\mathfrak{m}^t \cap J) \subseteq \mathfrak{m}^{n-t} J$$

for $n >> 0$ and a fixed $t > 0$. So $f(\mathfrak{m}^n \cap J) = 0$ for $n >> 0$ and f induces a map $\overline{f} : J/(J \cap \mathfrak{m}^n) \to T(A/\mathfrak{m}^n)$. Since $T(A/\mathfrak{m}^n)$ is injective over $A/\mathfrak{m}^n$ by Corollary 7.58, we have a commutative diagram



The direct limit of the maps from A to $T(A/\mathfrak{m}^n)$ provides our lift.
The other implication is clear. ■

Definition Let A be Noetherian, $\mathfrak{m}$ an ideal of A, and E be an injective A-module. We define the 0th **local cohomology** module of E with respect to $\mathfrak{m}$, to be

$$\mathrm{H}^0_{\mathfrak{m}}(E) := \{x \in E : \mathfrak{m}^n x = 0 \text{ for some } n > 0\}.$$

Corollary 7.62 *Let A be a Noetherian ring, $\mathfrak{m}$ an ideal of A and E an injective A-module. Then $\mathrm{H}^0_{\mathfrak{m}}(E)$ is injective over A.*

Proof Let $\mathcal{T} : \mathbf{C}^{\mathrm{f}}_{\mathfrak{m}} \to \mathbf{Ab}$ be the functor $\mathrm{Hom}_A(-, E)$. Since E is injective, $\mathcal{T}$ is exact. Hence, by the previous corollary,

$$I = \varinjlim_n \mathcal{T}(A/\mathfrak{m}^n) = \varinjlim_n \mathrm{Hom}_A(A/\mathfrak{m}^n, E) = H^0_{\mathfrak{m}}(E)$$

is injective. ■

Remark Sometimes we denote

$$\Gamma_{\mathfrak{m}}(E) := \{x \in E : \mathfrak{m}^n x = 0 \text{ for some } n > 0\},$$

and in this case we call $\Gamma_{\mathfrak{m}}(E)$ the **$\mathfrak{m}$-torsion functor**.

Theorem 7.63 *Suppose that A is Noetherian, $\mathfrak{m}$ is an ideal such that $\lambda(A/\mathfrak{m}) < \infty$, and $\mathcal{T}$ is a left exact additive contravariant functor from $\mathbf{C}^{\mathrm{f}}_{\mathfrak{m}}$ to $\mathbf{Ab}$. Then the following are equivalent:*

(1) *For all* $M \in \mathbf{C}^{\mathrm{f}}_{\mathfrak{m}}$, $\mathcal{T}(M)$ *is a module of finite length and* $M \to \mathcal{T}\mathcal{T}(M)$ *is an isomorphism.*

(2) $\mathcal{T}$ *is exact and for all maximal ideals* $\mathfrak{m}_i \supseteq \mathfrak{m}$, *if* $k_i = A/\mathfrak{m}_i$, *then* $\mathcal{T}(k_i) \cong k_i$ *via some noncanonical isomorphism.*

Proof (1) $\Rightarrow$ (2) Since $\mathcal{T}(k_i)$ is assumed to be a module of finite length and is killed by $\mathfrak{m}_i$, it is a finite dimensional vector space over k_i. So $\mathcal{T}(k_i) \cong k_i^n$. since $k_i^{n^2} = \mathcal{T}\mathcal{T}(k_i) \cong k_i$ we have that $n = 1$ and so $\mathcal{T}(k_i) \cong k_i$.

It remains to show that if $0 \to M \to N$ is exact, then $\mathcal{T}(N) \to \mathcal{T}(M) \to 0$ is exact. Suppose to the contrary that

$$\mathcal{T}(N) \to \mathcal{T}(M) \to Q \to 0$$

is exact where $Q \neq 0$. Then we have the exact sequence

$$0 \to \mathcal{T}(Q) \to M \to N.$$

Therefore $\mathcal{T}(Q) = 0$. But since $Q \neq 0$ we have a surjection $Q \to k_i \to 0$. Applying $\mathcal{T}$ we have the exact sequence $0 \to \mathcal{T}(k_i) \to \mathcal{Q}$. But $\mathcal{T}(k_i) = k_i$ by above, and $\mathcal{T}(Q) = 0$, a contradition. Therefore $\mathcal{T}$ is exact.

(2) $\Rightarrow$ (1) Since M has a filtration with quotients of the form k_i and since $\mathcal{T}$ is exact with $\mathcal{T}(k_i) = k_i$, $\mathcal{T}(M)$ will have a filtration with quotients of the form k_i. Hence $\mathcal{T}(M)$ is a module of finite length.

Since $\mathcal{T}\mathcal{T}(M)$ is of finite length, we may induct on the length of M to prove the other assertion in (1). We already have $\mathcal{T}\mathcal{T}(k_i) \cong k_i$. For arbitrary M we have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{T}\mathcal{T}(M') & \longrightarrow & \mathcal{T}\mathcal{T}(M) & \longrightarrow & \mathcal{T}\mathcal{T}(M'') & \longrightarrow & 0. \end{array}$$

By induction, since M', M'' have smaller length, the outer maps are isomorphisms. By the Five Lemma, $\mathcal{T}\mathcal{T}(M) \cong M$. ■

Definition Suppose that A is Noetherian, $\mathfrak{m}$ is an ideal such that $\lambda(A/\mathfrak{m}) < \infty$, and $\mathcal{T}$ is a left exact additive contravarient functor from $\mathbf{C}^{\mathrm{f}}_{\mathfrak{m}}$ to $\mathbf{Ab}$. $\mathcal{T}$ is called a **dualizing functor** for A and $\mathfrak{m}$ if $\mathcal{T}$ satisfies one of the equivalent conditions in the above theorem.

Definition Given a dualizing functor, the corresponding module

$$I = \varinjlim(\mathcal{T}(A/\mathfrak{m}^n))$$

is called a **dualizing module** for $\mathcal{T}$.

Corollary 7.64 *If $(A, \mathfrak{m}, k)$ is a local ring and $\mathcal{T}$ is a dualizing functor for A and $\mathfrak{m}$, then*

$$I = \varinjlim(\mathcal{T}(A/\mathfrak{m}^n)) \cong E_A(k).$$

Proof We have already that $k \cong \mathcal{T}(k) \cong \mathrm{Hom}_A(k, I)$, with I as above. Since elements of I are each killed by some power of $\mathfrak{m}$, we have an injection $k \hookrightarrow I$ and this is an essential extension (since $\mathrm{Hom}_A(k, I) \cong k$). Since I is injective, $E_A(k) \cong I$. ■

Definition Let A be a Noetherian finitely generated k_0-algebra and $\mathfrak{m}$ a maximal ideal of A. Then by Noether's Normalization Lemma we have that $k = A/\mathfrak{m}$ is a finite dimensional vector space over k_0. In this case we call

$$\mathrm{Hom}_{k_0}(A/\mathfrak{m}^n, k_0)$$

the **continuous hull** of A with respect to $\mathfrak{m}$.

Corollary 7.65 *Let A be a Noetherian finitely generated k_0-algebra and $\mathfrak{m}$ a maximal ideal of A. Then by Noether's Normalization Lemma we have that $k = A/\mathfrak{m}$ is a finite dimensional vector space over k_0. In this case*

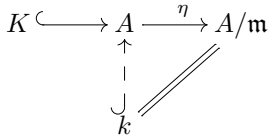
$$E_A(A/\mathfrak{m}) = E_{A_\mathfrak{m}}(k) = \varinjlim \mathrm{Hom}_{k_0}(A/\mathfrak{m}^n, k_0).$$

Proof Let $A = A_\mathfrak{m}$ and let $M \in \mathbf{C}^{\mathrm{f}}_\mathfrak{m}$. Let $\mathcal{T}$ be the functor $\mathrm{Hom}_{k_0}(M, k_0)$. Since $\lambda(M) < \infty$, $\mathrm{Hom}_{k_0}(M, k_0)$ is a finite dimensional k-vector space. Since k is a finite dimensional vector space over k_0, we have by the previous theorem that $\mathcal{T}$ is a dualizing functor. So by the previous corollary,

$$E_A(k) \cong I \cong \varinjlim \mathcal{T}(A/\mathfrak{m}^n) = \varinjlim \mathrm{Hom}_{k_0}(A/\mathfrak{m}^n, k_0).$$

■

Corollary 7.66 *If A is a zero dimensional local ring containing a field K, we have by Cohen's Structure Theorem that A contains a field k which is isomorphic to $A/\mathfrak{m}$, that is we have the following commutative diagram:*



Then $E_A(k) = \mathrm{Hom}_k(A, k)$.

Proof Use the previous corollary. ■

Corollary 7.67 *If $(A, \mathfrak{m})$ is local and Gorenstein of dimension d, then for all $M \in \mathbf{C}^{\mathrm{f}}_\mathfrak{m}$,*

$$\mathrm{Ext}^i_A(M, A) = \begin{cases} 0 & \text{if } i < d, \\ M^\vee & \text{if } i = d. \end{cases}$$

In other words, $\mathrm{Ext}^d_A(-, A)$ is a dualizing functor with $E_A(k)$ its corresponding dualizing module.

Proof Exercise. ■

Corollary 7.68 *If $(A, \mathfrak{m})$ is local and Gorenstein of dimension d, and we have an exact sequence of modules of finite length*

$$0 \to M_1 \to M_2 \to M_3 \to 0,$$

then

$$0 \to \mathrm{Ext}^d_A(M_3, A) \to \mathrm{Ext}^d_A(M_2, A) \to \mathrm{Ext}^d_A(M_1, A) \to 0$$

is exact. We also have that $\mathrm{Ext}^d_A(k, A) \cong k$.

Proof This follows from Theorem 7.63. ■

Thus we see that $\mathcal{T} : \mathbf{C}^{\mathrm{f}}_{\mathfrak{m}} \to \mathbf{Ab}$ where $\mathcal{T}(-) = \mathrm{Ext}^d_A(-, A)$ is an exact functor such that $\mathcal{T}(k) = k$. Hence

$$E_A(k) = \varinjlim_t \mathcal{T}(A/\mathfrak{m}^t) = \varinjlim_t \mathrm{Ext}^d_A(A/\mathfrak{m}^t, A).$$

Chapter 8

Local Cohomology

8.1 Grothendieck's Definition and Basic Properties

Definition Let A be a Noetherian ring, M an A-module and I an ideal of A. We define the ith **local cohomology** of M with respect to I by

$$\mathrm{H}^i_I(M) := \varinjlim_t \mathrm{Ext}^i_A(A/I^t, M).$$

Unfortunately this definition tells us next to nothing about what local cohomology really is, but we do have an immediate corollary to the definition:

Corollary 8.1 *If $(A, \mathfrak{m}, k)$ is a local Gorenstein ring of dimension d, then*

$$\mathrm{H}^d_{\mathfrak{m}}(A) = E_A(k),$$

and $\mathrm{H}^i_{\mathfrak{m}}(A) = 0$ otherwise.

Proof We know that since A is Gorenstein, $\mu_i(\mathfrak{m}; A) = \delta_{i,n}$ where $n = \dim(A)$. So if $0 \to A \to E^\bullet$ is the minimal injective resolution of A, then $\varinjlim_t \mathrm{Hom}_A(A/\mathfrak{m}^t, E^n) = E_A(k)$ (since every element of E^n is killed by some power of $\mathfrak{m}$) and $\mathrm{Hom}_A(A/\mathfrak{m}, E^i) = 0$ for $i < n$ (since no element of $E_A(A/\mathfrak{p})$ is killed by $\mathfrak{m}$ for any prime $p \neq \mathfrak{m}$). Hence $\mathrm{H}^d_{\mathfrak{m}}(A) = E_A(k)$ and $\mathrm{H}^i_{\mathfrak{m}}(A)$ for $i < n$. ■

Now we will discuss the relationship between $\mathrm{H}^0_I(-)$ and $\mathrm{H}^i_I(-)$, starting with an exercise.

Exercise 8.2 *Show that*

$$\mathrm{H}^0_I(M) = \{x \in M : I^n x = 0 \text{ for some } n > 0\}.$$

Now let

$$0 \to M \to E^0 \to E^1 \to \cdots \to E^i \to \cdots$$

be an injective resolution of M. Applying $\mathrm{Hom}_A(A/I^t, -)$ we get:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}_A(A/I^t, M) & \longrightarrow & \mathrm{Hom}_A(A/I^t, E^0) & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Hom}_A(A/I^{t+1}, M) & \longrightarrow & \mathrm{Hom}_A(A/I^{t+1}, E^0) & \longrightarrow & \cdots \end{array}$$

Now we make take the direct limit of the above system to obtain a complex:

$$0 \to \mathrm{H}^0_I(M) \to \mathrm{H}^0_I(E^0) \to \mathrm{H}^0_I(E^1) \to \cdots \to \mathrm{H}^0_I(E^i) \to \cdots$$

Since we know that

$$\begin{aligned} \mathrm{H}^0_I(M) :=& \{x \in M : I^n x = 0 \text{ for some } n > 0\}, \\ =& \varinjlim_t \mathrm{Hom}_A(A/I^t, M), \end{aligned}$$

we see

$$\begin{aligned} H^i(\mathrm{H}^0_I(E^\bullet)) &= H^i(\varinjlim_t \mathrm{Hom}_A(A/I^t, E^\bullet) = \varinjlim_t H^i(\mathrm{Hom}_A(A/I^t, E^\bullet) \\ &= \varinjlim_t \mathrm{Ext}^i_A(A/I^t, M) = \mathrm{H}^i_{\mathfrak{m}}(M) \end{aligned}$$

as cohomology and direct limit commute. Thus if we consider $\mathrm{H}^0_I(-)$ as a functor, then the ith local cohomology is the right derived functor of 0th local cohomology functor, that is

$$\mathrm{H}^i_I(-) = R^i \mathrm{H}^0_I(-).$$

Proposition 8.3 *If E is an injective module, $\mathrm{H}^i_I(E) = 0$ for every $i > 0$.*

Proof If E is injective, then $\mathrm{Ext}^i(A/I^t, E) = 0$ for all $i > 0$. Hence $\mathrm{H}^i_I(E) = 0$ for $i > 0$. By Corollary 7.61, $\mathrm{H}^0_I(E)$ is injective. ■

Proposition 8.4 *Every element of $\mathrm{H}^i_I(M)$ is killed by a power of I.*

Proof Every element of $\mathrm{Ext}^i_I(A/I^t, M)$ is killed by I^t. So every element of $\mathrm{H}^i_I(M)$ is killed by some power of I. ■

Proposition 8.5 *If the filtration*

$$I = J_1 \supseteq J_2 \supseteq \cdots \supseteq J_t \supseteq \cdots$$

*is **cofinal** with respect to $\{I^t\}$, that is for all t, there exists m_t and n_t such that*

$$J_{m_t} \subseteq I^t \qquad \text{and} \qquad I^{n_t} \subseteq J_t,$$

then

$$\mathrm{H}^i_I(M) = \varinjlim_t \mathrm{Ext}^i_A(A/J_t, M).$$

Proof Exercise. ■

Proposition 8.6 *If $\sqrt{I} = \sqrt{J}$, then $\mathrm{H}^i_I(M) = \mathrm{H}^i_J(M)$ for any module M.*

Proof Since A is Noetherian, if $\sqrt{I} = \sqrt{J}$ then $\{I^t\}$ and $\{J^t\}$ are cofinal. Now apply the previous result. ■

Proposition 8.7 $\mathrm{H}^0_I(M) \neq 0$ *if and only if* $\mathrm{Hom}_A(A/I, M) \neq 0$.

Proof ($\Rightarrow$) This implication is clear.
($\Leftarrow$) Suppose that $\mathrm{H}^0_I(M) \neq 0$. Then there exists a nonzero element $x \in M$ such that $I^t x = 0$ and $I^{t-1}x \neq 0$. Take $0 \neq y \in I^{t-1}x$. Then $Iy = 0$ and $\mathrm{Hom}_A(A/I, M) \neq 0$. ■

Proposition 8.8 (LES of $\mathbf{H^i_I(-)}$) *Given an exact sequence*

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

we have long exact sequence of local cohomology modules:

$$\begin{array}{l} 0 \longrightarrow \mathrm{H}^0_I(M_1) \longrightarrow \mathrm{H}^0_I(M_2) \longrightarrow \mathrm{H}^0_I(M_3) \longrightarrow \\ \qquad \mathrm{H}^1_I(M_1) \longrightarrow \mathrm{H}^1_I(M_2) \longrightarrow \mathrm{H}^1_I(M_3) \longrightarrow \cdots \end{array}$$

Proof This follows from the long exact sequence of Ext and the exactness of direct limits. ■

Theorem 8.9 (Relation between $\mathbf{depth_I(M)}$ and $\mathbf{H^i_I(M)}$) *If A is Noetherian, M finitely generated and I is an ideal of A, then $\mathrm{H}^i_I(M) = 0$ for all i if and only if $IM = M$. Otherwise if $IM \neq M$, then*

$$\mathrm{depth}_I(M) = \min\{i : \mathrm{H}^i_I(M) \neq 0\}.$$

Proof First note that

$$\begin{aligned} \mathrm{Supp}(M/I^tM) &= \mathrm{Supp}(M) \cap \mathrm{Supp}(A/I^t), \\ &= \mathrm{Supp}(A/\operatorname{Ann}(M)) \cap \mathrm{Supp}(A/I^t), \\ &= \mathrm{Supp}(A/(\operatorname{Ann}(M) + I^t)). \end{aligned}$$

Hence

$$\begin{aligned} M = IM &\Leftrightarrow M = I^tM \text{ for all } t > 0, \\ &\Leftrightarrow \operatorname{Ann}(M) + I^t = A \text{ for all } t > 0, \\ &\Leftrightarrow \mathrm{Ext}^i_A(A/I^t, M) = 0 \text{ for all } t > 0 \text{ and all } i \geq 0, \\ &\Leftrightarrow \mathrm{H}^i_I(M) = 0 \text{ for all } i \geq 0. \end{aligned}$$

Now suppose that $IM \neq M$. By Theorem 6.9 and by Proposition 8.7 we have that

$$\begin{aligned}\operatorname{depth}_I(M) = 0 &\Leftrightarrow \operatorname{Hom}(A/I, M) \neq 0,\\ &\Leftrightarrow \mathrm{H}^0_I(M) \neq 0.\end{aligned}$$

So assume that the claim is true for $i < n$. If $\operatorname{depth}_I(M) = n$, then $\operatorname{Ext}^i_A(A/I^t, M) = 0$ for all $i < n$ and all $t > 0$. Hence $\mathrm{H}^i_I(M) = 0$ for $i < n$. Now take $x \in I$ a nonzerodivisor on M. Then we have an exact sequence

$$0 \to M \xrightarrow{x} M \to M/xM \to 0.$$

We get the following long exact sequence of local cohomology

$$0 = \mathrm{H}^{n-1}_I(M) \to \mathrm{H}^{n-1}_I(M/xM) \to \mathrm{H}^n_I(M) \to \cdots .$$

Since $\mathrm{H}^i_I(M/xM) = 0$ for $i < n-1$ and $\mathrm{H}^{n-1}_I(M/xM) \neq 0$ by induction. Therefore $\mathrm{H}^n_I(M) \neq 0$. ■

Exercise 8.10 *If $f : A \to B$ is a flat homomorphism of Noetherian rings, where I is an ideal of A and M is an A-module, then*

$$\mathrm{H}^\bullet_{IB}(M \otimes_A B) \cong \mathrm{H}^\bullet_I(M) \otimes_A B.$$

Hint: $\operatorname{Ext}^i_A(A/I^t, M) \otimes_A B \cong \operatorname{Ext}^i_B(B/I^tB, M \otimes_A B)$.

8.2 Local Cohomology and the Koszul Complex

Observe that if A is a ring and $x \in A$, then

$$\varinjlim(A \xrightarrow{x} A \xrightarrow{x} \cdots) = A_x.$$

To see this, define $\varphi_n : A \to A_x$ by sending $1 \mapsto \frac{1}{x^n}$. These maps combine to give a map $\varphi : \varinjlim_t (A \xrightarrow{x} A \xrightarrow{x} \cdots) \to A_x$. Clearly φ is onto. Now suppose that $\frac{a}{x^n} = 0 \in A_x$. Then for some $t > 0$, we have

$$x^t a = 0.$$

But this says that $a = 0$ in the direct limit. Hence φ is an isomorphism. The same proof works for modules. We leave the proof to the reader as an exercise.

Lemma 8.11 *If M is an A-module, then*

$$M_x = \varinjlim(M \xrightarrow{x} M \xrightarrow{x} \cdots).$$

Proof Exercise. ■

In a similar way we will take the direct limit of the Koszul complex. Consider $I = (x_1, \ldots, x_n)$, and set $\mathbf{x}^t = (x_1^t, \ldots, x_n^t)$. While we know that

$$\mathrm{H}^i_I(M) = \varinjlim \mathrm{Ext}^i_A(A/\mathbf{x}^t, M).$$

we would like to try to get our hands on it.

For $\mathbf{x} \in A$, we have that when $s > t$

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & K_1(\mathbf{x}^s; A) & \longrightarrow & K_0(\mathbf{x}^s; A) & \longrightarrow & A/\mathbf{x}^s & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \varphi_1^{st}} & & \downarrow{\scriptstyle \varphi_0^{st}} & & \downarrow & & \\
\cdots & \longrightarrow & K_1(\mathbf{x}^t; A) & \longrightarrow & K_0(\mathbf{x}^t; A) & \longrightarrow & A/\mathbf{x}^t & \longrightarrow & 0
\end{array}$$

where $\varphi_p^{st} : K_p(\mathbf{x}^s; A) \to K_p(\mathbf{x}^t; A)$ via

$$\sum_{1 \le i_1 < \cdots < i_p \le n} a_{i_1,\ldots,i_p} e_{i_1} \wedge \cdots \wedge e_{i_p} \mapsto \sum_{1 \le i_1 < \cdots < i_p \le n} (x_{i_1} \cdots x_{i_p})^{s-t} a_{i_1,\ldots,i_p} e_{i_1} \wedge \cdots \wedge e_{i_p}.$$

Applying $\mathrm{Hom}_A(-, A)$ to $K_\bullet(\mathbf{x}^s; A) \to K_\bullet(\mathbf{x}^t; A)$, we obtain:

$$\begin{array}{ccc}
\mathrm{Hom}_A(K_\bullet(\mathbf{x}^t; A), A) & \longrightarrow & \mathrm{Hom}_A(K_\bullet(\mathbf{x}^s; A), A) \\
\| & & \| \\
K^\bullet(\mathbf{x}^t; A) & \xrightarrow{\varphi_\bullet^{st}} & K^\bullet(\mathbf{x}^s; A)
\end{array}$$

And so we have the commutative diagram:

$$\begin{array}{ccccc}
K^\bullet(\mathbf{x}^t; A) & \longrightarrow & A/\mathbf{x}^t & \to & 0 \\
\downarrow{\scriptstyle \varphi_\bullet^{st}} & & \downarrow{\scriptstyle (x_1 \cdots x_n)^{s-t}} & & \\
K^\bullet(\mathbf{x}^s; A) & \longrightarrow & A/\mathbf{x}^s & \to & 0
\end{array}$$

Definition Define

$$K^\bullet(\mathbf{x}^\infty; A) := \varinjlim_t K^\bullet(\mathbf{x}^t; A).$$

Note that we can similarly define $K^\bullet(\mathbf{x}^\infty; M)$, where we use the maps

$$\varphi_\bullet^{st} \otimes_A \mathrm{id}_M .$$

In this case one should check that we have

$$\begin{aligned}
K^\bullet(\mathbf{x}^\infty; M) &= \varinjlim_t K^\bullet(\mathbf{x}^t; M), \\
&= \varinjlim_t K^\bullet(\mathbf{x}^t; A) \otimes_A M, \\
&= K^\bullet(\mathbf{x}^\infty; A) \otimes_A M.
\end{aligned}$$

So at this point we see that

$$K^\bullet(\mathbf{x}^\infty; A) = K^\bullet(x_1^\infty; A) \otimes \cdots \otimes K^\bullet(x_n^\infty; A)$$

and hence we have $K^\bullet(\mathbf{x}^\infty; A)$:

$$0 \to A \to \bigoplus_{1 \le i_1 \le n} A_{x_{i_1}} \to \cdots \to \bigoplus_{1 \le i_1 < \cdots < i_p \le n} A_{x_{i_1} \cdots x_{i_p}} \to \cdots \to A_{x_1 \cdots x_n} \to 0$$

where each map is just the sum of the localization maps with the appropriate sign.
In a similar fashion we have $K^\bullet(\mathbf{x}^\infty; M)$:

$$0 \to M \to \bigoplus_{1 \le i_1 \le n} M_{x_{i_1}} \to \cdots \to \bigoplus_{1 \le i_1 < \cdots < i_p \le n} M_{x_{i_1} \cdots x_{i_p}} \to \cdots \to M_{x_1 \cdots x_n} \to 0$$

Note that the first nonzero term on the left is in degree zero. This sort of cochain complex is called a **Čech complex**.

Definition Define

$$\begin{aligned} \check{\mathrm{H}}^i_{\mathbf{x}}(M) :=& H^i(K^\bullet(\mathbf{x}^\infty; M)), \\ =& \varinjlim_t H^i(K^\bullet(\mathbf{x}^t; M)). \end{aligned}$$

We call this the **Čech cohomology** of M.

Proposition 8.12 *If A is a ring, M is an A-module, and $I = (x_1, \ldots, x_n)$, then the following are true:*

(1) $\check{\mathrm{H}}^0_{\mathbf{x}}(M) = \mathrm{H}^0_I(M)$.

(2) *Given a short exact sequence*

$$0 \to M_1 \to M_2 \to M_3 \to 0,$$

there exists a long exact sequence:

$$\begin{array}{l} 0 \longrightarrow \check{\mathrm{H}}^0_{\mathbf{x}}(M_1) \longrightarrow \check{\mathrm{H}}^0_{\mathbf{x}}(M_2) \longrightarrow \check{\mathrm{H}}^0_{\mathbf{x}}(M_3) \longrightarrow \\ \qquad \check{\mathrm{H}}^1_{\mathbf{x}}(M_1) \longrightarrow \check{\mathrm{H}}^1_{\mathbf{x}}(M_2) \longrightarrow \check{\mathrm{H}}^1_{\mathbf{x}}(M_3) \longrightarrow \cdots \end{array}$$

(3) *If E is injective, then $\check{\mathrm{H}}^i_{\mathbf{x}}(E) = 0$ for $i > 0$.*

Proof (1)

$$\begin{aligned} \check{\mathrm{H}}^0_{\mathbf{x}}(M) &= \mathrm{Ker}(M \to \bigoplus_{i=1}^n M_{x_i}) \\ &= \{m \in M : x_i^t m = 0 \text{ for some } t > 0 \text{ and all } 1 \le i \le n\} \\ &= \{m \in M : I^t m = 0 \text{ for some } t > 0\} \\ &= \mathrm{H}^0_I(M). \end{aligned}$$

(2) Let

$$0 \to M_1 \to M_2 \to M_3 \to 0,$$

be an exact sequence. Since localization is exact, we get an exact sequence of complexes

$$0 \to K^\bullet(\mathbf{x}^\infty; M_1) \to K^\bullet(\mathbf{x}^\infty; M_2) \to K^\bullet(\mathbf{x}^\infty; M_3) \to 0.$$

Taking the long exact sequence in homology associated to this short exact sequence of complexes we get that

$$0 \to \check{\mathrm{H}}^0_{\mathbf{x}}(M_1) \to \check{\mathrm{H}}^0_{\mathbf{x}}(M_2) \to \check{\mathrm{H}}^0_{\mathbf{x}}(M_3) \to \check{\mathrm{H}}^1_{\mathbf{x}}(M_1) \to \cdots$$

is exact.

(3) Any injective module E is of the form $\bigoplus_i E_A(A/\mathfrak{p}_i)$. Since direct sums commute with homology, it suffices to show that $\check{\mathrm{H}}^i_{\mathbf{x}}(E_A(A/\mathfrak{p})) = 0$ for any prime ideal $\mathfrak{p} \in \mathrm{Spec}(A)$. Since

$$\check{\mathrm{H}}^i_{\mathbf{x}}(E_A(A/\mathfrak{p})) = \check{\mathrm{H}}^i_{\mathbf{x}}(E_{A_\mathfrak{p}}(A/\mathfrak{p})),$$

we may assume that A is local with maximal ideal $\mathfrak{p}$.

Now since $\mathfrak{p}$ is maximal, $E(A/\mathfrak{p}) = \bigcup_i E_n$ where

$$E_n = \{e \in E(A/\mathfrak{p}) \,|\, \mathfrak{p}^n e \;=\; 0\},$$

and since $\check{\mathrm{H}}^i_{\mathbf{x}}(E(A/\mathfrak{p})) = \varinjlim \check{\mathrm{H}}^i_{\mathbf{x}}(E_n)$, it suffices to prove that $\mathrm{H}^i_{\mathbf{x}}(M) = 0$ for $i > 0$ and M finite length. By taking a filtration, it suffices to show that $\mathrm{H}^i_{\mathbf{x}}(k) = 0$ where $k = A/\mathfrak{p}$ is the residue field. Observe that if x_i is a unit, then $k_{x_i} = k$, and if $x_i \in \mathfrak{p}$, then $k_{x_i} = 0$. By considering the Čech complex, one sees that $K^\bullet(\mathbf{x}^\infty; k)$ is exact if at least one x_i is a unit, whereas if all $x_i \in \mathfrak{p}$, the Čech complex reduces to

$$0 \to k \to 0 \to 0 \to \cdots.$$

In either case, $H^i(K^\bullet(\mathbf{x}^\infty; k)) = 0$ for $i > 0$. This completes the proof. ■

Theorem 8.13 *If A is a ring, M is an A-module, and $I = (x_1, \ldots, x_n)$, then*

$$\mathrm{H}^i_I(M) \cong \check{\mathrm{H}}^i_{\mathbf{x}}(M) \text{ for } i \geq 0.$$

Proof We proceed by induction. Note that the previous proposition takes care of the base case $\mathrm{H}^0_I(M) \cong \check{\mathrm{H}}^0_{\mathbf{x}}(M)$. So suppose the theorem is true up to $i > 0$. Take an exact sequence

$$0 \to M \to E \to N \to 0$$

where E is injective. By the long exact sequences of H_I and $\check{\mathrm{H}}_{\mathbf{x}}$ we get that $\check{\mathrm{H}}^i_{\mathbf{x}}(N) \cong \check{\mathrm{H}}^{i+1}_{\mathbf{x}}(M)$ and $\mathrm{H}^i_I(N) \cong \mathrm{H}^{i+1}_I(M)$. By induction, $\check{\mathrm{H}}^i_{\mathbf{x}}(N) \cong \mathrm{H}^i_I(N)$. Hence $\check{\mathrm{H}}^{i+1}_{\mathbf{x}}(M) \cong \mathrm{H}^{i+1}_I(M)$. ■

Corollary 8.14 *If $A \to B$ is a homomorphism of Noetherian rings, I an ideal of A, and M an B-module, then*

$$\mathrm{H}^i_I(M) = \mathrm{H}^i_{IB}(M).$$

Proof The corresponding Čech complexes are isomorphic as complexes of A-modules; that is,

$$K^\bullet(\mathbf{x}^\infty;_A M) \cong K^\bullet(\mathbf{x}^\infty B; M).$$

■

Remark The above result would be difficult to obtain if we only used the Ext-definition of local cohomology.

8.3 Local Duality

The Case of Gorenstein Rings

Proposition 8.15 *If A is Noetherian, $\mathfrak{m}$ a maximal ideal and M is a finitely generated A-module, then*

$$\mathrm{H}^i_{\mathfrak{m}}(M) \cong \mathrm{H}^i_{\mathfrak{m}A_{\mathfrak{m}}}(M_{\mathfrak{m}}) \cong \mathrm{H}^i_{\widehat{\mathfrak{m}A_{\mathfrak{m}}}}(\widehat{M_{\mathfrak{m}}}).$$

Proof (sketch) For a module of finite length T, $T \cong T \otimes_A A_{\mathfrak{m}} \cong T \otimes_A \widehat{A}_{\mathfrak{m}}$. Since tensor products commute with direct limits and since each module $\mathrm{Ext}^i_A(A/\mathfrak{m}^t, M)$ is killed by a power of $\mathfrak{m}$, the result follows. ■

Remark The upshot from the preceding proposition is that when working with local cohomology you can localize and then complete, thus you may reduce to the case of a complete local ring!

WARNING 8.16 *Localization does not commute with completions. Even if A is a complete ring there may be $\mathfrak{p} \in \mathrm{Spec}(A)$ such that $A_{\mathfrak{p}}$ is not complete. This usually does not present much of a difficulty as in most cases one may choose to simply localize first and then complete.*

Theorem 8.17 (Cohen) *If A is a complete local ring, then there exists a complete regular local ring B and an onto map $B \twoheadrightarrow A$. Moreover B will have one of two forms:*

(1) *$B = k[\![X_1, \ldots, X_n]\!]$ where k is a field.*

(2) *$B = V[\![X_1, \ldots, X_n]\!]$ where V is a DVR.*

Lemma 8.18 *If M is an A-module and $F_\bullet$ is a flat resolution of M; that is, each F_i is flat, $F_\bullet$ is exact except in degree 0, and $H_0(F_\bullet) = M$, then*

$$\mathrm{Tor}^A_i(M, N) = H_i(F_\bullet \otimes N).$$

Proof Exercise. (Hint: Think about how to prove the balancing of Tor.) ■

Theorem 8.19 *If A is Noetherian, and $\mathfrak{m}$ is a maximal ideal with M finitely generated, then $\mathrm{H}^i_{\mathfrak{m}}(M)$ satisfies DCC.*

Proof By above, we can assume that A is a complete local ring and that we have a surjective map $\eta : B \to A$ where B is a complete regular local ring. If $\mathfrak{n}$ denotes the maximal ideal of B, then by Corollary 8.14 $\mathrm{H}^i_{\mathfrak{n}}(M) = \mathrm{H}^i_{\mathfrak{m}}(M)$ since $\eta(\mathfrak{n}) = \mathfrak{m}$. By replacing A by B we may assume that A is a complete regular local ring, say of dimension d. Since A is regular, $\mathrm{depth}(A) = d$ and by Theorem 8.9 we have $\mathrm{H}^i_{\mathfrak{m}}(A) = 0$ for $i < d$. Further by Corollary 8.1, $\mathrm{H}^d_{\mathfrak{m}}(A) = E_A(k) = E$. Since A is regular local, we can write $\mathfrak{m} = (x_1, \ldots, x_d)$. The Čech complex $K^\bullet(\mathbf{x}^\infty; A)$ is then a flat resolution of E; that is,

$$0 \to A \to \bigoplus_i A_{x_i} \to \cdots \to A_{x_1 x_2 \cdots x_d} \to \mathrm{H}^d_{\mathfrak{m}}(A) \to 0$$

is exact. By the previous lemma,

$$\mathrm{H}^i_{\mathfrak{m}}(M) = H^i(K^\bullet(\mathbf{x}^\infty; M)) = H^i(K^\bullet(\mathbf{x}^\infty; A) \otimes_A M) = \mathrm{Tor}^A_{d-i}(M, E).$$

Since M is finitely generated, if $F_\bullet \to M \to 0$ is a minimal free resolution of M, then we also have

$$\mathrm{Tor}^A_{d-i}(M, E) = H_{d-i}(F_\bullet \otimes_A E).$$

If we write $F_i = A^{n_i}$ for each i, then $F_i \otimes_A E = E^{n_i}$, which is a module with DCC by Proposition 7.19. Hence $\mathrm{H}^i_{\mathfrak{m}}(M) = H_{d-i}(F_\bullet \otimes_A E)$, being a subquotient of a module with DCC, has DCC. ■

Lemma 8.20 *If $C_\bullet$ is an A-complex and E is an injective A-module, then*

$$H^i(\mathrm{Hom}_A(C_\bullet, E)) \cong \mathrm{Hom}_A(H_i(C_\bullet), E).$$

Proof Exercise. (Or see Cartan-Eilenberg, Theorem 7.2.) ■

Theorem 8.21 (Local Duality) *If A is a complete local Gorenstein ring of dimension n and M is a finitely generated A-module, then for all $i \geq 0$*

$$\mathrm{H}^i_{\mathfrak{m}}(M)^\vee \cong \mathrm{Ext}^{n-i}_A(M, A),$$

where we recall that $\mathrm{H}^i_{\mathfrak{m}}(M)^\vee = \mathrm{Hom}_A(\mathrm{H}^i_{\mathfrak{m}}(M), E_A(A/\mathfrak{m}))$.

Proof Since A is Gorenstein, $\mathrm{H}^i_{\mathfrak{m}}(A) = 0$ for $i < n$ and $\mathrm{H}^n_{\mathfrak{m}}(A) = E_A(k) = E$. As in the previous proposition, we have that

$$\begin{aligned} \mathrm{H}^i_{\mathfrak{m}}(M) &= H^i(K^\bullet(\mathbf{x}^\infty; M)), \\ &= H^i(K^\bullet(\mathbf{x}^\infty; A) \otimes_A M), \\ &= \mathrm{Tor}^A_{n-i}(M, E). \end{aligned}$$

Let $F_\bullet \to M \to 0$ be a free resolution of M. Then

$$\begin{aligned} \mathrm{H}^i_{\mathfrak{m}}(M) &= \mathrm{Tor}^A_{n-i}(M, E), \\ &= H_{n-i}(F_\bullet \otimes_A E). \end{aligned}$$

It follows then that

$$\begin{aligned} \mathrm{H}^i_{\mathfrak{m}}(M)^\vee &= \mathrm{Hom}_A(\mathrm{H}^i_{\mathfrak{m}}(M), E), \\ &= \mathrm{Hom}_A(H_{n-i}(F_\bullet \otimes_A E), E), \\ &= H^{n-i}(\mathrm{Hom}_A(F_\bullet \otimes_A E, E)), \\ &= H^{n-i}(\mathrm{Hom}(F_\bullet, \mathrm{Hom}_A(E, E)), \\ &= H^{n-i}(\mathrm{Hom}_A(F_\bullet, A)), \\ &= \mathrm{Ext}^{n-i}_A(M, A). \end{aligned}$$

The first equation is the definition of $(-)^\vee$, the second holds by the above argument, the third holds because E is injective, the fourth holds by the adjoint isomorphism, the fifth holds since A is complete and local, and the last equation is the definition of Ext. This completes the proof. ■

Corollary 8.22 *If A is a complete local Gorenstein ring of dimension n and M is a finitely generated A-module, then*

$$\mathrm{H}^i_{\mathfrak{m}}(M) \cong \mathrm{Ext}^{n-i}_A(M, A)^\vee$$

Proof This follows from Theorem 7.20 since A is complete and local. ■

Corollary 8.23 *If A is a local Gorenstein ring of dimension n and M is a finitely generated A-module, then*

$$\mathrm{H}^i_{\mathfrak{m}}(M)^\vee \cong \mathrm{Ext}^{n-i}_{\widehat{A}}(\widehat{M}, \widehat{A}) \cong \widehat{\mathrm{Ext}^{n-i}_A(M, A)}.$$

Proof

$$\mathrm{H}^i_{\mathfrak{m}}(M)^\vee \cong \mathrm{H}^i_{\widehat{\mathfrak{m}}}(\widehat{M})^\vee \cong \mathrm{Ext}^{n-i}_{\widehat{A}}(\widehat{M}, \widehat{A}) \cong \widehat{\mathrm{Ext}^{n-i}_A(M, A)}.$$

■

Remark We will show later that there exists a bilinear map

$$\mathrm{H}^i_{\mathfrak{m}}(M) \times \mathrm{Ext}^{n-i}_A(M, A) \to \mathrm{H}^n_{\mathfrak{m}}(A)$$

which leads to this isomorphism as in the above corollary when A is a complete local Gorenstein ring of dimension n.

Theorem 8.24 (Relation between $\dim(M)$ and $\mathrm{H}^i_{\mathfrak{m}}(M)$) *If A is local and M is a finitely generated A-module, then*

$$\dim(M) = \sup\{i : \mathrm{H}^i_{\mathfrak{m}}(M) \neq 0\}.$$

Proof Note that for a system of parameters $x_1, \ldots, x_n$, we have $\mathrm{H}^i_{\mathfrak{m}}(M) = \check{\mathrm{H}}^i_{\mathbf{x}}(M) = 0$ for $i > \dim(M)$. So we need only prove that $\mathrm{H}^d_{\mathfrak{m}}(M) \neq 0$ where $d = \dim(M)$.

Let $I = \mathrm{Ann}_A(M)$. Since $\mathrm{H}^i_{\mathfrak{m}}(M) = \mathrm{H}^i_{\mathfrak{m}A/I}(M) = \mathrm{H}^i_{\widehat{\mathfrak{m}}\widehat{A/I}}(\widehat{M})$, we may assume that $\dim(M) = \dim(A)$ and that A is complete.

By the Cohen Structure Theorem, any complete local ring is a homomorphic image of a complete regular local ring. So $A \cong S/I$ where S is a complete regular local ring. Let $r = \mathrm{ht}(I)$ and let $x_1, \ldots, x_r$ be an S-sequence in I. Then $S/\mathbf{x}$ is complete and $\dim(S/\mathbf{x}) = \dim(A)$. Replacing A by S/I we may assume that A is Gorenstein and complete and that $\dim(M) = \dim(A)$.

Since we have reduced to the case where $\dim(A) = \dim(M)$, we have that $\mathrm{ht}(\mathrm{Ann}_A(M)) = 0$. Therefore $\mathrm{grade}(M) = \mathrm{depth}_{\mathrm{Ann}_A(M)}(M) = 0$ and hence $\mathrm{Hom}_A(M, A) \neq 0$. Now since A is assumed to be Gorenstein, local duality says that $\mathrm{H}^d_{\mathfrak{m}}(M)^\vee \cong \mathrm{Hom}_A(M, A)$, where $d = \dim(M)$. Therefore $\mathrm{H}^d_{\mathfrak{m}}(M) \neq 0$, as required. ■

8.4 Set-Theoretic Complete Intersections

We will see in this section that there are connections between the vanishing of local cohomology modules and the set-theoretic complete intersection property.

Definition If I is an ideal in a regular Noetherian ring R of height n, then I is called a **complete intersection** if there exists $x_1, \ldots, x_n$ such that

$$I = (x_1, \ldots, x_n).$$

The ideal I is called a **local complete intersection** if for every maximal ideal $\mathfrak{m}$, $I_{\mathfrak{m}}$ is a complete intersection in $R_{\mathfrak{m}}$.

The ideal I is called a **set-theoretic complete intersection** if there exists $x_1, \ldots, x_n$ such that

$$\sqrt{I} = \sqrt{(x_1, \ldots, x_n)}.$$

Corollary 8.25 *$\mathrm{H}^i_I(-) = 0$ for all $i > n$ if n is the minimal number of elements in I such that*

$$\sqrt{I} = \sqrt{(x_1, \ldots, x_n)}.$$

Proof The Čech complex $K^\bullet(x^\infty; M)$ has length at most n. ■

Corollary 8.26 *If I is an ideal of height n and if there exists some A-module M such that $\mathrm{H}^i_I(M) \neq 0$ for $i > n$, then I is not a set-theoretic intersection.*

Proof This follows from the previous corollary. ■

Theorem 8.27 (Kunz) *If A is a regular ring of positive characteristic, then the Frobenius map*

$$f^\alpha : A \to A,$$
$$a \mapsto a^{p^n}$$

is flat for all $n > 0$. (Equivalently, the Frobenius functor taking M to $M \otimes^{f^n} A$ is an exact functor.) Conversely if f^n is flat for all $n > 0$, and A is reduced, then A is regular.

Proof See "Characterizations of Regular Local Rings of Characteristic p" by Kunz. ■

Theorem 8.28 (Peskine-Szpiro) *Let A be a regular domain of positive characteristic and I is an ideal such that A/I is Cohen-Macaulay with $\operatorname{ht}(I) = n$. Then*

$$\mathrm{H}^i_I(-) = 0 \qquad \text{for } i > n.$$

Proof Since A is regular, by the previous theorem applying the mth power of the Frobenius functor to the minimal free resolution of A/I, we get a resolution of $A/I^{[p^m]}$, where $I^{[p^m]}$ is the ideal generated by the p^mth powers of the generators of I. Hence $\operatorname{Ext}^i_A(A/I^{[p^m]}, -) = 0$ for all $i > n$. Therefore

$$\mathrm{H}^i_I(-) = \varinjlim_m \operatorname{Ext}^i_A(A/I^{[p^m]}, -) = 0$$

for all $i > n$. ■

Corollary 8.29 *Let A be a regular domain of positive characteristic and I is an ideal such that A/I is Cohen-Macaulay with $\operatorname{ht}(I) = n$. Then*

$$\mathrm{H}^i_I(A) = 0 \qquad \text{for } i \neq n.$$

Proof That $\mathrm{H}^i_I(A)$ vanishes for $i > n$ follows from the previous theorem. Since A is regular, $\operatorname{depth}_I(A) = \operatorname{ht}(I) = n$. Therefore $H^i_I(A)$ vanishes for $i < n$ as well by Theorem 8.9. ■

Example 8.30 *Let $A = k[x_{i,j}]_{\substack{1 \le i \le 2 \\ 1 \le j \le 3}}$ and suppose that k is algebraically closed. If*

$$I = \text{ideal generated by } 2 \times 2 \text{ minors of } \begin{bmatrix} x_{1,1} & x_{1,2} & x_{1,3} \\ x_{2,1} & x_{2,2} & x_{2,3} \end{bmatrix} = (\Delta_1, \Delta_2, \Delta_3)$$

where Δ_i are homogeneous polynomials in A. By a previous discussion, $\operatorname{ht}(I) = 2$ and A/I is Cohen-Macaulay, but not Gorenstein. This can be seen by noticing that we have a free resolution

$$0 \to A^2 \xrightarrow{\mathbf{x}^T} A^3 \to A \to A/I \to 0$$

of A/I. Hence $\operatorname{pd}_A(A/I) = 2$ and $\operatorname{depth}_{\mathfrak{m}}(A/I) = \operatorname{depth}_{\mathfrak{m}}(A) - \operatorname{pd}_A(A/I) = 6 - 2 = 4$, where $\mathfrak{m}$ is the graded maximal ideal.

Is I a set-theoretic complete intersection? If the characteristic of k is p, then by the above theorem we have $\mathrm{H}^i_I(-) = 0$ for $i > 2$. In the late 1990's Paul Newstead showed that I is not a set-theoretic complete intersection by using

the étale version of local cohomology. In characteristic 0*, we can show that* $H^3_I(A) \neq 0$ *and hence* I *is not a set-theoretic complete intersection.*

Let $G = \mathrm{SL}(2,k)$*. Let* G *act on the matrix of variables by left multiplication. Then the three minors* $\Delta_1, \Delta_2, \Delta_3$ *are fixed by the action of* G *and in fact the fixed ring* $A^G = k[\Delta_1, \Delta_2, \Delta_3]$*. Since* $\Delta_1, \Delta_2, \Delta_3$ *are algebraically-independent over* k*,* A^G *is a polynomial ring of dimension* 3 *and so* $H^3_I(A^G) \neq 0$*. We have a split injective map of* A^G *modules* $A^G \hookrightarrow A$*. Therefore the map of local cohomology modules* $H^3_I(A^G) \to H^3_I(A)$ *is injective. Hence* $H^3_I(A) \neq 0$ *and so* I *is not a set-theoretic complete intersection.*

It is an open question in $\mathbb{A}^n$ for $n \geq 3$ in the equicharacteristic 0 case as to whether every curve is a set-theoretic complete intersection. This is equivalent, in the $n = 3$ case, to the question of whether for every height 2 prime $\mathfrak{p} \in k[X,Y,Z]$ there are element $f, g \in k[X,Y,Z]$ such that $\mathfrak{p} = \sqrt{(f,g)}$.

Conjecture 1 *Every curve is a set-theoretic complete intersection—equivalently, every prime ideal of height* $n-1$ *in a ring of dimension* n *is a set-theoretic complete intersection.*

In characteristic p, Cowsik and Nori proved that every curve in $\mathbb{A}^n$ is a set-theoretic complete intersection in 1978. They used results of Mohan Kumar as well as Peskine-Szpiro. Their main theorem was the following:

Theorem 8.31 *If* $A = k[\![x_1, \ldots, x_n]\!]$ *with* $\mathrm{ht}(\mathfrak{p}) = n-1$*, then*

$$\mathfrak{p} = \sqrt{(g_1, \ldots, g_n)}.$$

In the general case, Herzog provides a many examples of set-theoretic complete intersection with his result showing that $k\left[t^{n_1}, t^{n_2}, t^{n_3}\right]$ is a set-theoretic complete intersection if $\gcd(n_1, n_2, n_3) = 1$. For instance, $k\left[t^3, t^4, t^5\right]$ is a set-theoretic complete intersection. We have seen this example many times already

Generalizations to Cohen-Macaulay Rings

Definition Let A be a local Cohen-Macaulay ring of dimension n and let ω be a finitely generated A-module. We call ω a **canonical module** for A if $\widehat{\omega} \cong \mathrm{H}^n_{\mathfrak{m}}(A)^\vee$.

Theorem 8.32 (Local Duality) *If* A *is a complete local Cohen-Macaulay ring of dimension* n *and* M *is a finitely generated* A*-module, we have*

$$\mathrm{H}^i_{\mathfrak{m}}(M)^\vee \cong \mathrm{Ext}^{n-i}_A(M, \omega).$$

(Note that since A *is complete, it has a canonical module.)*

Proof Since A is Cohen-Macaulay, $\mathrm{H}^i_{\mathfrak{m}}(A) = 0$ for $i < n$. So again $K^\bullet(\mathbf{x}^\infty; A)$ is a flat resolution of $\mathrm{H}^n_{\mathfrak{m}}(A)$. Let $F_\bullet \to M \to 0$ be a free resolution of M. Then we get isomorphisms

$$\mathrm{H}^i_{\mathfrak{m}}(M) \cong \mathrm{Tor}^A_{n-i}(M, \mathrm{H}^n_{\mathfrak{m}}(A)) \cong H_{n-i}(F_\bullet \otimes_A \mathrm{H}^n_{\mathfrak{m}}(A)).$$

Hence

$$\begin{aligned}\mathrm{H}^i_{\mathfrak{m}}(M)^\vee &\cong \mathrm{Hom}_A(H_{n-i}(F_\bullet \otimes_A \mathrm{H}^n_{\mathfrak{m}}(A), E)) \\ &\cong H^{n-i}(\mathrm{Hom}_A(F_\bullet \otimes_A \mathrm{H}^n_{\mathfrak{m}}(A), E)) \\ &\cong H^{n-i}(\mathrm{Hom}_A(F_\bullet, \mathrm{Hom}(\mathrm{H}^n_{\mathfrak{m}}(A), E))) \\ &\cong \mathrm{Ext}^{n-i}_A(M, \omega).\end{aligned}$$

■

Proposition 8.33 *If $(A, \mathfrak{m})$ is local with two finitely generated A-modules M and N such that $\widehat{M} \cong \widehat{N}$, then $M \cong N$.*

Proof Since M, N are finitely generated,

$$\mathrm{Hom}_{\widehat{A}}(\widehat{M}, \widehat{N}) \cong \widehat{\mathrm{Hom}_A(M, N)}.$$

Let $\widehat{\varphi} : \widehat{M} \xrightarrow{\cong} \widehat{N}$ be an isomorphism. There exists $\varphi_0 \in \mathrm{Hom}_A(M, N)$ such that

$$\widehat{\varphi} - \widehat{\varphi_0} \in \widehat{\mathfrak{m}}\,\mathrm{Hom}_{\widehat{A}}(\widehat{M}, \widehat{N}).$$

Set $Q = \mathrm{Coker}(\varphi_0)$ and consider the exact sequence

$$M \xrightarrow{\varphi_0} N \to Q \to 0.$$

Tensoring by $A/\mathfrak{m} \cong \widehat{A}/\widehat{m}$ we get the exact sequence

$$M/\mathfrak{m}M \xrightarrow{\overline{\varphi_0}} N/\mathfrak{m}N \to Q/\mathfrak{m}Q \to 0,$$

where $\overline{\varphi_0}$ is the induced map of φ_0 on the quotient. Since $A/\mathfrak{m} \cong \widehat{A}/\widehat{m}$, and since $\overline{\varphi_0} = \overline{\widehat{\varphi_0}} = \overline{\widehat{\varphi}}$, $Q/\mathfrak{m}Q = 0$. Therefore $Q = 0$. Hence φ_0 is onto.

Now pick $\widehat{\psi} : \widehat{N} \xrightarrow{\cong} \widehat{M}$ such that $\widehat{\psi} \circ \widehat{\varphi} = Id_{\widehat{M}}$ and $\widehat{\varphi} \circ \widehat{\psi} = Id_{\widehat{N}}$. Then we get a map $\psi_0 : N \to M$ such that $\psi_0 \circ \varphi_0 : M \to M$ is onto and such that $\varphi_0 \circ \psi_0 : N \to N$ are onto. Since M, N are finitely generated, $\psi_0 \circ \varphi_0$ and $\varphi_0 \circ \psi_0$ are isomorphisms. Hence ψ_0 and φ_0 are isomorphisms, whereby $M \cong N$. ■

Corollary 8.34 *If canonical modules exist for a local Cohen-Macaulay ring A, then they are unique up to A-isomorphism.*

Proof This follows from the definition of the canonical module and the previous proposition. ■

Proposition 8.35 *If A is a local Cohen-Macaulay ring and $A = B/I$ where B is a local Gorenstein ring, then*

$$\omega = \mathrm{Ext}^{\dim(B)-\dim(A)}_B(A, B)$$

is a canonical module for A.

Proof

$$\widehat{\omega} \cong \operatorname{Ext}_{\widehat{B}}^{\dim(B)-\dim(A)}(\widehat{A},\widehat{B}) \cong \operatorname{H}^{\dim(A)}_{\widehat{\mathfrak{m}_B}}(\widehat{A})^\vee \cong \operatorname{H}^{\dim(A)}_{\widehat{\mathfrak{m}_A}}(\widehat{A})^\vee \cong \operatorname{H}^{\dim(A)}_{\mathfrak{m}_A}(A)^\vee,$$

where the second equality uses local duality for the Gorenstein ring B. Therefore ω is a canonical module for A. ■

Proposition 8.36 *Let A be a local Cohen-Macaulay ring, A has a canonical module if and only if A is the image of a Gorenstein ring.*

Proof ($\Leftarrow$) By the previous proposition, if A is the image of a Gorenstein ring, say $A = B/I$ where B is Gorenstein, then $\omega = \operatorname{Ext}_B^{\dim(B)-\dim(A)}(A,B)$ is a canonical module for A.

($\Rightarrow$) Suppose A has canonical module ω and set $B = A * \omega$, that is $B = A \oplus \omega$ as A-modules with multiplication defined by

$$(a,w)\cdot(a',w') = (aa', aw' + a'w).$$

Let $x_1,\dots,x_n$ be a system of parameters for A. By part (3) of the following theorem, $x_1,\dots,x_n$ forms a maximal ω-sequence. Setting $\widetilde{x_i} = (x_i,0) \in B$, we have that $\widetilde{x_1},\dots,\widetilde{x_n}$ is a maximal B-sequence. So $B/(\widetilde{x_1},\dots,\widetilde{x_n}) = A/\mathbf{x} \oplus \omega/\mathbf{x}\omega$ and B has maximal ideal $\mathfrak{p} := \mathfrak{m} \oplus \omega$. We leave it to the reader to check that

$$\begin{aligned}\operatorname{Hom}_B(B/\mathfrak{p}, B/\widetilde{\mathbf{x}}) &\cong \operatorname{Hom}_A(A/\mathfrak{m}, \omega/\mathbf{x}\omega),\\ &\cong \operatorname{Hom}_A(A/\mathfrak{m}, E_{A/\mathbf{x}}(k)),\\ &\cong k,\end{aligned}$$

whence B is Gorenstein and $\dim(B) = \dim(A)$. ■

Theorem 8.37 (Properties of the Canonical Module) *Let $(A,\mathfrak{m},k)$ be a local Cohen-Macaulay ring of dimension n. Suppose that A has a canonical module ω. The following are true:*

(1) *If A is Gorenstein, $\omega \cong A$.*

(2) *If $\dim(A) = 0$, then $\omega \cong E_A(k)$*

(3) *If x is a nonzerodivisor on A, then x is a nonzerodivisor on ω and $\omega/x\omega$ is a canonical module for A/xA.*

(4) *If $x_1,\dots,x_n$ is a system of parameters for A, then*

$$\omega/\mathbf{x}\omega \cong E_{A/\mathbf{x}}(k).$$

(5) $\operatorname{id}_A(\omega) = n$. *Moreover,*

$$\boldsymbol{\mu}_i(\mathfrak{m},\omega) = \begin{cases} 0 & \text{if } i \neq n,\\ 1 & \text{if } i = n.\end{cases}$$

(6) *For every* $\mathfrak{p} \in \operatorname{Spec}(A)$, $\omega_{\mathfrak{p}}$ *is a canonical module for* $A_{\mathfrak{p}}$.

(7) $\mathrm{H}^n_{\mathfrak{m}}(\omega) \cong E_A(k)$.

(8) $\operatorname{Hom}_A(\omega, \omega) \cong A$.

Proof Note that for (1) - (8), we may assume that A is complete.

(1) If A is Gorenstein, then $\mathrm{H}^n_{\mathfrak{m}}(A) \cong E_A(k) = E$. So

$$\omega \cong \operatorname{Hom}_A(\mathrm{H}^n_{\mathfrak{m}}(A), E) \cong \operatorname{Hom}_A(E, E) \cong A.$$

(2) If $\dim(A) = 0$, then $\lambda(A) < \infty$. Hence $\mathrm{H}^0_{\mathfrak{m}}(A) = A$. Therefore

$$\omega \cong \mathrm{H}^0_{\mathfrak{m}}(A)^\vee \cong \operatorname{Hom}_A(A, E) \cong E.$$

(3) Let x be a nonzerodivisor on A. Then we have that

$$0 \to A \xrightarrow{x} A \to A/xA \to 0$$

is exact. Since A is Cohen-Macaulay and x is a nonzerodivisor on A, A/xA is Cohen-Macaulay. So the long exact sequence of cohomology associated to the above short exact sequence reduces to

$$0 \to \mathrm{H}^{n-1}_{\mathfrak{m}}(A/xA) \to \mathrm{H}^n_{\mathfrak{m}}(A) \xrightarrow{x} \mathrm{H}^n_{\mathfrak{m}}(A) \to 0.$$

Applying $(-)^\vee$ we get the exact sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{H}^n_{\mathfrak{m}}(A)^\vee & \xrightarrow{x} & \mathrm{H}^n_{\mathfrak{m}}(A)^\vee & \longrightarrow & \mathrm{H}^{n-1}_{\mathfrak{m}}(A/xA) & \longrightarrow & 0 \\
 & & \downarrow \cong & & \downarrow \cong & & \downarrow \cong & & \\
0 & \longrightarrow & \omega & \xrightarrow{x} & \omega & \longrightarrow & \omega/x\omega & \longrightarrow & 0.
\end{array}$$

Therefore x is a nonzerodivisor on ω and $\omega/x\omega$ is a canonical module for A/xA.

(4) Let $x_1, \ldots, x_n$ be a system of parameters for A. Then $x_1, \ldots, x_n$ is a maximal A-sequence. So for all i, $\omega/(x_1, \ldots, x_i)\omega$ is a canonical module for $A/(x_1, \ldots, x_i)$ and $x_1, \ldots, x_n$ is a maximal ω-sequence by part (3). By (2),

$$\omega/\mathbf{x}\omega \cong E_{A/\mathbf{x}}(k).$$

(Note: In particular $\omega/\mathbf{x}\omega$ is injective over $A/\mathbf{x}$.)

(5) Since $\operatorname{id}_{A/\mathbf{x}}(\omega/\mathbf{x}\omega) = 0$, we have $\operatorname{id}_A(\omega) = n$, see Bruns-Herzog Corollary 3.1.15. Thus $\operatorname{depth}(\omega) = \dim(\omega) = n$. It follows that $\boldsymbol{\mu}_i(\mathfrak{m}, \omega) = 0$ for $i < n$ and $\boldsymbol{\mu}_n(\mathfrak{m}, \omega) = 1$.

(6) By the previous proposition, there is a Gorenstein ring B and a surjective map $\eta : B \to A$ is a homomorphic image of B. Let $\mathfrak{p} \in \operatorname{Spec}(A)$ and let

$\mathfrak{q} = \eta^{-1}(\mathfrak{p})$. Then $B_{\mathfrak{q}} \to A_{\mathfrak{p}}$ is a surjective map. Since $a_{\mathfrak{p}}$ is a homomorphic image of the Gorenstein ring $B_{\mathfrak{q}}$, $A_{\mathfrak{p}}$ has canonical module

$$\begin{aligned}\omega(A_{\mathfrak{p}}) &= \operatorname{Ext}_{B_{\mathfrak{q}}}^{\dim(B_{\mathfrak{q}})-\dim(A_{\mathfrak{p}})}(A_{\mathfrak{p}}, B_{\mathfrak{q}}),\\ &= \operatorname{Ext}_{B}^{\dim(B)-\dim(A)}(A, B) \otimes_B B_{\mathfrak{q}},\\ &= \omega_{\mathfrak{q}},\end{aligned}$$

where ω is a canonical module for A.

(7) Let $0 \to \omega \to I^\bullet$ be the minimal injective resolution of ω. By part (5),

$$\mathrm{H}^n_{\mathfrak{m}}(\omega) = H^n(H^0_m(I^\bullet)) = E_A(k).$$

(8) Using local dulaity and part (7), we have

$$\operatorname{Hom}_A(\omega, \omega) \cong \mathrm{H}^n_{\mathfrak{m}}(\omega)^\vee \cong E_A(k)^\vee = A.$$

■

Theorem 8.38 *Let A be a Cohen-Macaulay ring with a canonical module ω. Then the type of A is equal to the minimal number of generators of ω.*

Proof We may assume that A is complete. Hence $A = B/I$ for a regular local ring B. Recall now that if A is a Cohen-Macaulay ring of dimension n and $A = B/I$, where B is a regular local ring with $\operatorname{ht}(I) = d$, we then have a minimal free resolution of A:

$$0 \to B^{t_d} \to \cdots \to B^{t_1} \to B \to A \to 0$$

By our work above we have that $\operatorname{Ext}^d_B(A, B) = \omega$. We wanted to show that the type of A is equal to the minimal number of generators of ω. We now know know that ω is a canonical module for A. Recall that the the type of A is

$$\dim_k \operatorname{Ext}^n_A(k, A) = \dim_k \operatorname{Hom}_A(k, A/(x_1, \ldots, x_n))$$

where $\mathbf{x}$ is a system of parameters for A. Since $\dim(A/\mathbf{x}) = 0$ and recalling that $\omega/\mathbf{x}\omega$ is the canonical module for $A/\mathbf{x}$, we see that

$$\omega/\mathbf{x}\omega \cong E_{A/\mathbf{x}}(k).$$

Moreover

$$\begin{aligned}A/\mathbf{x} &\cong \operatorname{Hom}_{A/\mathbf{x}}(E_{A/\mathbf{x}}(k), E_{A/\mathbf{x}}(k)),\\ &\cong \operatorname{Hom}_{A/\mathbf{x}}(\omega/\mathbf{x}\omega, \omega/\mathbf{x}\omega).\end{aligned}$$

Now practicing our yoga we have

$$\begin{aligned}\operatorname{Hom}_A(k, A/\mathbf{x}) &\cong \operatorname{Hom}_A(k, \operatorname{Hom}_{A/\mathbf{x}}(\omega/\mathbf{x}\omega, \omega/\mathbf{x}\omega)),\\ &\cong \operatorname{Hom}_{A/\mathbf{x}}(A/\mathfrak{m} \otimes_A \omega/\mathbf{x}\omega, E_{A/\mathbf{x}}(k)),\\ &\cong \operatorname{Hom}_{A/\mathbf{x}}(\omega/\mathfrak{m}\omega, E_{A/\mathbf{x}}(k)),\\ &\cong (\omega/\mathbf{x}\omega)^\vee.\end{aligned}$$

However, putting our steps above together, we see that

$$\begin{aligned}\dim_k \operatorname{Hom}_A(k, A/\mathbf{x}) &= \lambda_k(\operatorname{Hom}_A(k, A/\mathbf{x})),\\ &= \lambda_k((\omega/\mathbf{x}\omega)^\vee),\\ &= \lambda_k(\omega/\mathbf{x}\omega),\\ &= \dim_k(\omega/\mathfrak{m}\omega).\end{aligned}$$

So we see that the type of A is $\dim_k(\omega/\mathfrak{m}\omega)$, which is the minimum number of generators of ω. ■

Definition Let A be Cohen-Macaulay and ω be a finitely generated A-module. ω is called a **canonical module** for A if for A if for every $\mathfrak{m} \in \operatorname{MaxSpec}(A)$, $\omega_\mathfrak{m}$ is a canonical module for $A_\mathfrak{m}$.

Theorem 8.39 *If A is Cohen-Macaulay, ω and ω' are two canonical modules for A, then there exists a projective module P of rank 1 such that*

$$\omega \otimes_A P \cong \omega'.$$

Proof Consider the map $\varphi : \omega \otimes_A \operatorname{Hom}_A(\omega, \omega') \to \omega'$ defined by $\varphi : x \otimes_A f \mapsto f(x)$. Localize this map at a maximal ideal $\mathfrak{m}$. Over $A_\mathfrak{m}$, $\omega_\mathfrak{m} \cong \omega'_\mathfrak{m}$. We conclude that

$$(\operatorname{Hom}_A(\omega, \omega'))_\mathfrak{m} \cong \operatorname{Hom}_{A_\mathfrak{m}}(\omega_\mathfrak{m}, \omega'_\mathfrak{m}) \cong A_\mathfrak{m},$$

and therefore $P = \operatorname{Hom}_A(\omega, \omega')$ is a locally free rank 1 A-module and $\varphi_\mathfrak{m}$ is an isomorphism for every maximal ideal $\mathfrak{m}$. Therefore P is projective and φ is an isomorphism. ■

Example 8.40 *As we have done before, let $A = k[x_{i,j}]_{\substack{1\le i\le 2\\ 1\le j\le 3}}$ and let consider A/I, where I is the ideal $(\Delta_1, \Delta_2, \Delta_3)$ generated by the 2×2 minors of the matrix $\mathbf{X}$ form by putting $x_{i,j}$ is position (i, j). We saw that A/I is a 4-dimensional Cohen-Macaulay ring and that A/I has a free A-resolution:*

$$0 \to A^2 \xrightarrow{\mathbf{X}^T} A^3 \to A \to A/I \to 0.$$

Since A is Gorenstein, A/I has canonical module

$$\omega = \operatorname{Ext}_A^{\dim(A)-\dim(A/I)}(A/I, A) = \operatorname{Ext}_A^2(A/I, A) = \operatorname{Coker}(A^3 \xrightarrow{\mathbf{X}} A^2).$$

Therefore the minimal number of generators for ω is 2. We can conclude that A/I is not Gorenstein for it is of type 2.

Now write $\omega = A\alpha_1 + A\alpha_2$ and define a map $\varphi : \omega \to A/I$ by sending $\varphi : \alpha_1 \mapsto \overline{x_{1,1}}$ and $\varphi : \alpha_2 \mapsto \overline{x_{2,1}}$. We leave it to the reader to check that this map is well-defined and injective. But this now shows that ω is isomorphic to an ideal of A/I!

More generally, let $A = k[x_{i,j}]_{\substack{1\le i\le n\\ 1\le j\le m}}$ and let I_t be the ideal generated by the $t \times t$ minors of A. Then the canonical module ω of A/I is isomorphic to the ideal $J^{m-n} \subseteq A/I$ where J is generated by the $(t-1)\times(t-1)$ minors of any $t-1$ columns. (Note that this agrees with our example above.)

We state the following theorem to give a geometric interpretation.

Theorem 8.41 *If A is a affine domain over $\mathbb{C}$, and A is normal, $\Omega_{A/\mathbb{C}}$ is the module of Kähler differentials of A over $\mathbb{C}$, and*

$$\omega^i := \bigwedge^i \omega_{A/\mathbb{C}},$$

then the canonical module for A is $\Omega^{\dim(A)}$.

8.5 Grothendieck's Functorial Approach

Resolutions and Pairings

In this subsection $\mathbf{C}$ is an Abelian category with enough injectives.

Definition If $A \in \mathbf{C}$ we say that $K^\bullet$, a cochain complex of objects in $\mathbf{C}$ is a **nonexact resolution** of A if $K^i = 0$ for $i < 0$ and there exists $\varepsilon : A \to K^0$, such that

$$0 \to A \xrightarrow{\varepsilon} K^0 \to K^1$$

is exact. We will call such a nonexact resolution an **exact resolution** if $H^i(K^\bullet) = 0$ for all $i > 0$.

WARNING 8.42 *While resolutions are exact, this is a different sort of resolution and hence we use the term* nonexact *resolution. The confusions arises from the usage of the term resolution by Grothendieck to describe what we have renamed a nonexact resolution. So within these notes, the term resolution will always be exact above degree 0.*

Definition Let $K^\bullet$ and $L^\bullet$ be two complexes. $f^\bullet : K^\bullet \to L^\bullet$ is a morphism of **degree** s if

$$f^i : K^i \to L^{i+s},$$

that is if the following diagram commutes:

$$\begin{array}{ccccccc} \cdots & \longrightarrow & K^i & \longrightarrow & K^{i+1} & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle f^i} & & \downarrow{\scriptstyle f^{i+1}} & & \\ \cdots & \longrightarrow & L^{i+s} & \longrightarrow & L^{i+s+1} & \longrightarrow & \cdots \end{array}$$

Definition The group of all morphisms of degree s from $K^\bullet$ to $L^\bullet$ is denoted

$$\mathrm{Hom}^s(K^\bullet, L^\bullet).$$

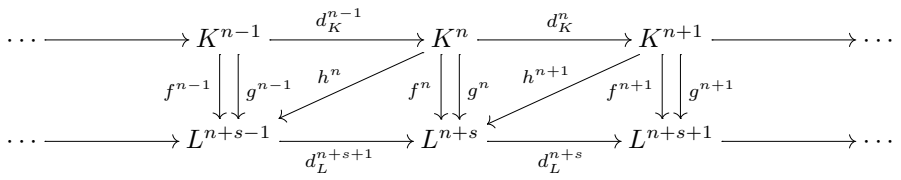
Definition Two maps $f^\bullet$ and $g^\bullet$ of degree s each taking $K^\bullet$ to $L^\bullet$ are called **homotopic** if there exits

$$h^\bullet : K^\bullet \to L^\bullet$$

such that

$$f^n - g^n = d_L^{n+s-1} \circ h^n + h^{n+1} \circ d_K^n.$$

Equivalently, in a more pictorial fashion, if $f^\bullet$ and $g^\bullet$ are homotopic, then we have a diagram



which "commutes" in the sense that the above equation holds.

We denote

$$H^s(K^\bullet, L^\bullet) := \{\text{the group of all homotopic maps from } K^\bullet \to L^\bullet \text{ of degree } s\}$$

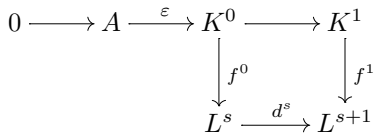
Now consider an object A in $\mathbf{C}$ and let

$$0 \to A \xrightarrow{\varepsilon} K^\bullet$$

be a nonexact resolution of A. Take any complex $L^\bullet$, and consider $f^\bullet \in \mathrm{Hom}^s(K^\bullet, L^\bullet)$. Now we see that $f^0 \circ \varepsilon \in \mathrm{Hom}(A, L^s)$ and we have the following differential

$$\begin{aligned} d_*^s : \mathrm{Hom}(A, L^s) &\to \mathrm{Hom}(A, L^{s+1}), \\ f^0 \circ \varepsilon &\mapsto d^s \circ f^0 \circ \varepsilon, \end{aligned}$$

but we see that $d^s \circ f^0 \circ \varepsilon = 0$ by the following commutative diagram:



Since $f^0 \circ \varepsilon \in \mathrm{Ker}(d^s)$, $f^0 \circ \varepsilon$ is represented up to homotopy by some element in $H^s(\mathrm{Hom}(A, L^\bullet))$. So we have a map:

$$\varphi^s : H^s(K^\bullet, L^\bullet) \to H^s(\mathrm{Hom}(A, L^\bullet)).$$

Theorem 8.43 *Suppose that $K^\bullet$ is an exact resolution of A and $L^\bullet$ consists of injective objects only. Then*

$$\varphi^s : H^s(K^\bullet, L^\bullet) \to H^s(\mathrm{Hom}(A, L^\bullet))$$

as described above is an isomorphism for all s.

Proof This follows from properties of injectives modules and the exactness of $K^\bullet$. We leave it as an exercise for the reader. ■

Corollary 8.44 *Suppose that $K^\bullet$ is an exact resolution of A and $L^\bullet$ is an injective resolution of B, then*

$$\mathrm{Ext}^s(A,B) \cong \mathcal{H}^s(K^\bullet, L^\bullet).$$

Proof Apply the above theorem where $L^\bullet$ is an injective resolution of B. ■

Corollary 8.45 *Let $\mathcal{T} : \mathbf{C} \to \mathbf{C}'$ be an additive covarient functor of Abelian categories with enough injectives. Then for every pair of objects $A, B \in \mathbf{C}$ and for every i, s we have a map*

$$\varphi : R^i\mathcal{T}(A) \times \mathrm{Ext}^s(A,B) \to R^{i+s}\mathcal{T}(B).$$

Proof Let $K^\bullet$ be an injective resolution of A and let $L^\bullet$ be an injective resolution of B. Then we have that $R^i\mathcal{T}(A) = H^i(\mathcal{T}(K^\bullet))$ and $R^{i+s}\mathcal{T}(B) = H^{i+s}(\mathcal{T}(L^\bullet))$. By the above corollary, $\mathrm{Ext}(A,B) = \mathcal{H}^s(K^\bullet, L^\bullet)$. Let h be a map of degree s from $K^\bullet$ to $L^\bullet$. Then $\mathcal{T}(h)$ is a map of degree s from $\mathcal{T}(K^\bullet)$ to $\mathcal{T}(L^\bullet)$.

Now let $\lambda \in R^i\mathcal{T}(K^\bullet)$. Then λ is represented by $\mu \in \mathcal{T}(K^i)$ with $\mathcal{T}(d_K^i)(\mu) = 0$. Hence $\mathcal{T}(d_L^{i+x})(h^i(\mu)) = 0$ since the following diagram commutes

$$\begin{array}{ccccccc}
\cdots & \longrightarrow & \mathcal{T}(K^i) & \xrightarrow[d_K^i]{} & \mathcal{T}(K^{i+1}) & \xrightarrow[d_K^{i+1}]{} & \cdots \\
 & & \downarrow{\scriptstyle h^i} & & \downarrow{\scriptstyle h^{i+1}} & & \\
\cdots & \longrightarrow & \mathcal{T}(L^{i+s}) & \xrightarrow[d_L^{i+s}]{} & \mathcal{T}(L^{i+s+1}) & \xrightarrow[d_L^{i+s+1}]{} & \cdots .
\end{array}$$

So we can define φ by $(\lambda, h) \mapsto h^i(\mu)$. (One should check that this is well-defined.) ■

Serre Duality and Local Duality

Let A be a Noetherian ring, I an ideal of A, and $\mathbf{C}$ be the category of A-modules. Let $\mathcal{T}(-) = \mathrm{H}^0_I(-)$. Thus we have a map

$$\varphi : \mathrm{H}^i_I(M) \times \mathrm{Ext}^s_A(M,N) \to \mathrm{H}^{i+s}_I(N)$$

For another application, if X is a scheme and $\mathcal{O}_X$ is the structure sheaf with $\mathbf{C}$ being the category of $\mathcal{O}_X$-modules and $\mathbf{C}'$ being the category of Abelian groups, then given any $\mathcal{F} \in \mathbf{C}$, there exists an injective resolution of $\mathcal{F}$

$$0 \to \mathcal{F} \to \mathcal{I}^0 \to \mathcal{I}^1 \to \cdots \to \mathcal{I}^n \to \cdots$$

each $\mathcal{I}^i \in \mathbf{C}$ is an injective $\mathcal{O}_X$-module. Define

$$H^i(X,\mathcal{F}) := R^i\Gamma(X,\mathcal{F})$$

and write:

$$0 \to \Gamma(X,\mathcal{F}) \to \Gamma(X,\mathcal{I}^0) \to \Gamma(X,\mathcal{I}^1) \to \cdots \to \Gamma(X,\mathcal{I}^n) \to \cdots$$

Taking homologies we obtain

$$\mathrm{Ext}^i_{\mathcal{O}_X}(\mathcal{G},\mathcal{F}) = H^i(\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{G},\mathcal{I}^\bullet))$$

and so we have a map

$$H^i(X,\mathcal{F}) \times \mathrm{Ext}^s_{\mathcal{O}_X}(\mathcal{F},\mathcal{G}) \to H^{i+s}(X,\mathcal{G}).$$

This leads us to Serre duality:

Theorem 8.46 (Serre Duality) *Let $X = \mathbb{P}^n_k$, then*

$$\varphi_i : H^i(X,\mathcal{F}) \times \mathrm{Ext}^{n-i}_{\mathcal{O}_X}(\mathcal{F},\omega_X) \to H^n(X,\omega_X) = k$$

is a perfect pairing; that is, the canonical maps

$$\mathrm{H}^i(X,\mathcal{F}) \to \mathrm{Ext}^{n-i}_{\mathcal{O}_X}(\mathcal{F},\omega_X)^*,$$
$$\mathrm{Ext}^{n-i}_{\mathcal{O}_X}(\mathcal{F},\omega_X) \to \mathrm{H}^i(X,\mathcal{F})^*$$

are isomorphisms, where $(-)^*$ denotes $\mathrm{Hom}_k(-,k)$.

Proof See Hartshorne or wait til later in the notes. ■

Theorem 8.47 (Local Duality) *Let $(A,\mathfrak{m})$ be a local Gorenstein ring of dimension n. Let M be a finitely generated A-module. Then the pairing*

$$\varphi : \mathrm{H}^i_{\mathfrak{m}}(M) \times \mathrm{Ext}^{n-i}_A(M,A) \to \mathrm{H}^n_{\mathfrak{m}}(A) \cong E_A(k) = E$$

gives rise to maps

$$\mathrm{H}^i_{\mathfrak{m}}(M) \to \mathrm{Ext}^{n-i}_A(M,A)^\vee,$$
$$\mathrm{Ext}^{n-i}_{\widehat{A}}(\widehat{M},\widehat{A}) \to \mathrm{H}^i_{\mathfrak{m}}(M)^\vee$$

which are isomorphisms. In particular, if A is complete, then this is a perfect pairing.

Proof By Matlis duality we need only prove that we have an isomorphism

$$\psi^i_M : \mathrm{H}^i_{\mathfrak{m}}(M) \cong \mathrm{Ext}^{n-i}_A(M,A)^\vee.$$

Case 1: $i = n$ First consider the case where $M = A^t$. Then we have $\mathrm{H}^n_{\mathfrak{m}}(A^t) \cong E^t$ and $\mathrm{Hom}_A(A^t,A) \cong A^t$. So $\varphi : \mathrm{H}^n_{\mathfrak{m}}(A^t) \times \mathrm{Hom}_A(A^t,A) \to \mathrm{H}^n_{\mathfrak{m}}(A) = E$ is just the tensor product map, which induces an isomorphism

$$\psi^n_A : \mathrm{Hom}^i_{\mathfrak{m}}(A) \cong \mathrm{Hom}_A(A,A)^\vee.$$

Clearly we get that $\psi^n_{A^t}$ is an isomorphism for $M = A^t$ and $t > 0$.

Now suppose M is an arbitrary finitely generated A-module. Then M has a presentation

$$A^t \to A^s \to M \to 0.$$

¿From this exact sequence we get the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} \mathrm{H}^n_{\mathfrak{m}}(A^t) & \longrightarrow & \mathrm{H}^n_{\mathfrak{m}}(A^s) & \longrightarrow & \mathrm{H}^n_{\mathfrak{m}}(M) & \longrightarrow & 0 \\ \downarrow{\scriptstyle \psi^n_{A^t}}\cong & & \downarrow{\scriptstyle \psi^n_{A^s}}\cong & & \downarrow{\scriptstyle \psi^n_M} & & \\ \mathrm{Hom}_A(A^t,A)^\vee & \longrightarrow & \mathrm{Hom}_A(A^s,A)^\vee & \longrightarrow & \mathrm{Hom}_A(M,A)^\vee & \longrightarrow & 0. \end{array}$$

The first two vertical maps are isomorphisms as mentioned above. By the five lemma, we have that ψ^n_M is an isomorphism.

Case 2: $i = n-1$ Let M be a finitely generated A-module and choose a short exact sequence of the form:

$$0 \to N \to A^t \to M \to 0.$$

Since A is Gorenstein of dimension n, we have $\mathrm{H}^i_{\mathfrak{m}}(A) = 0$ for $i < n$ and $\mathrm{H}^d_{\mathfrak{m}}(A) \cong E$. By the long exact sequences of Ext and $\mathrm{H}_{\mathfrak{m}}$ and the exactness of the $(-)^\vee$ functor, we have the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{H}^{n-1}_{\mathfrak{m}}(M) & \longrightarrow & \mathrm{H}^n_{\mathfrak{m}}(N) & \longrightarrow & \mathrm{H}^n_{\mathfrak{m}}(A^t) \\ & & \downarrow{\scriptstyle \psi^{n-1}_M} & & \downarrow{\scriptstyle \psi^n_N}\cong & & \downarrow{\scriptstyle \psi^n_{A^t}}\cong \\ 0 & \longrightarrow & \mathrm{Ext}^{n-1}_A(M,A)^\vee & \longrightarrow & \mathrm{Ext}^n_A(N,A)^\vee & \longrightarrow & \mathrm{Ext}^n_A(A^t,A)^\vee. \end{array}$$

The second two vertical maps are isomorphisms by Case 1. Hence ψ^{n-1}_M is an isomorphism.

Case 3: $i < n-1$ By the same arguments as in Case 2, we get the following commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{H}^i_{\mathfrak{m}}(M) & \xrightarrow{\cong} & \mathrm{H}^{i+1}_{\mathfrak{m}}(n) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \psi^i_M} & & \downarrow{\scriptstyle \psi^{i+1}_N}\cong & & \\ 0 & \longrightarrow & \mathrm{Ext}^{n-i}_A(M,A)^\vee & \xrightarrow{\cong} & \mathrm{Ext}^{n-(i+1)}_A(N,A)^\vee & \longrightarrow & 0. \end{array}$$

The top and bottom maps are isomorphisms by the vanishing of the appropriate Ext and local cohomology modules for a free module. The right vertical map is an isomorphism by decreasing induction. Therefore, ψ^i_M is an isomorphism. ■

Chapter 9

Applications and Generalizations

9.1 Hartshorne-Lichtenbaum Vanishing Theorem

Exercise 9.1 *If A is a local ring of dimension d and I is an ideal of A, show that*

$$\sqrt{I} = \sqrt{(x_1, \ldots, x_d)}$$

where $x_1, \ldots, x_d \in I$.

Exercise 9.2 *If A is a Noetherian ring of dimension d and I is any ideal of A, show that*

$$\sqrt{I} = \sqrt{(x_1, \ldots, x_d, x_{d+1})}$$

where $x_1, \ldots, x_{d+1} \in I$.

Note that the first of the two exercises above shows us that if A is a local ring of dimension d, then $\mathrm{H}^i_I(-) = 0$ for $i > d$. This also holds for nonlocal rings by the following proposition:

Proposition 9.3 *If A is a Noetherian ring, I is an ideal of A, M is an A-module, then the following hold:*

(1) $\mathrm{H}^i_I(A) = 0$ *for* $i > n$ *implies that* $\mathrm{H}^i_I(M) = 0$ *for* $i > n$.

(2) *Given a prime ideal* $\mathfrak{p}$ *if* $\mathrm{H}^i_I(A/\mathfrak{p}) = 0$, *if* M *is killed by a power of* $\mathfrak{p}$, *then* $\mathrm{H}^i_I(M) = 0$ *for all* $i > n$.

(3) *If* S *is a finite subset of* $\mathrm{Spec}(A)$ *where for every* $\mathfrak{p} \in S$

$$\mathrm{H}^i_I(A/\mathfrak{p}) = 0 \qquad \text{for } i > n,$$

and every prime ideal in S *is contained in a prime ideal of* $\mathrm{Supp}(M)$, *then* $\mathrm{H}^i_I(M) = 0$ *for all* $i > n$.

(4) $\mathrm{H}^i_I(A) = 0$ *for* $i > \dim(A)$. *Moreover, by (1) above, if* M *is any* A*-module, then* $\mathrm{H}^i_I(M) = 0$ *for all* $i > \dim(A)$.

(5) $\mathrm{H}^i_I(M) = 0$ *for* $i > \dim(M)$.

Proof (1) By the second exercise above we have that $\mathrm{H}^i_I(-) = 0$ for $i > d+1$ where $d = \dim(A)$. First let M be a finitely generated A-module. Take a short exact sequence of the form

$$0 \to N \to A^t \to M \to 0.$$

By the long exact sequence of H_I we have that

$$\mathrm{H}^{n+1}_I(A^t) \to \mathrm{H}^{n+1}_I(M) \to \mathrm{H}^{n+2}_I(N)$$

is exact. $\mathrm{H}^{n+1}_I(A^t) = (\mathrm{H}^{n+1}_I(A))^t = 0$ by assumption. Also $\mathrm{H}^{n+2}_I(N) = 0$ as noted above. Therefore $\mathrm{H}^{n+1}_I(M) = 0$ for all finitely generated A-modules M.

Now let M be any A-module. Then we can write $M = \varinjlim M_\alpha$ as the direct limit of its finitely generated submodules. We then have

$$\mathrm{H}^{n+1}_I(M) = \mathrm{H}^{n+1}_I(\varinjlim M_\alpha) = \varinjlim H^{n+1}_I(M_\alpha) = 0.$$

By induction, we are done.

(2) Since a module is the direct limit of its finitely generated modules, we may assume that M is finitely generated. (See the argument in part (1).) So there exists $t > 0$ such that $\mathfrak{p}^t M = 0$. Since $M_j = \mathfrak{p}^j M/\mathfrak{p}^{j+1}M$ is annihilated by $\mathfrak{p}$, M_j is an $A/\mathfrak{p}$-module for all $0 \le j \le t$. By part (1), $H^i_I(M_j) = H^i_{IA/\mathfrak{p}}(M_j) = 0$ for $i > n$ and all $1 \le j \le t$. It follows from the long exact sequence of H_I that $H^i_I(M) = 0$ for $i > n$.

(3) We may assume M is finitely generated. Let

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_t = (0)$$

be a prime filtration of M with $M_i/M_{i+1} \cong A/\mathfrak{q}_i$ and each $\mathfrak{q}_i \in \mathrm{Ass}_A(M) \subseteq \mathrm{Supp}_A(M)$. by assumption for each i there exists $\mathfrak{p}_{j_i} \in S$ such that $\mathfrak{p}_{j_i} \supseteq \mathfrak{q}_i$. So for each i, M_i/M_{i+1} is annihilated by $\mathfrak{p}_{j_i}$. By part (2), $\mathrm{H}^i_I(M_i/M_{i+1}) = 0$ for $i > n$. Again by the long exact sequence of H_I, we have $\mathrm{H}^i_I(M) = 0$ for $i > n$.

(4) Suppose $\mathrm{H}^i_I(A) \neq 0$ for some $i > n = \dim(A)$. Then there exists $\mathfrak{p} \in \mathrm{Spec}(A)$ such that

$$\mathrm{H}^i_{IA_\mathfrak{p}}(A_\mathfrak{p}) \cong \mathrm{H}^i_I(A_\mathfrak{p}) \cong \mathrm{H}^i_I(A) \otimes_A A_\mathfrak{p} \cong (\mathrm{H}^i_I(A))_\mathfrak{p} \neq 0.$$

However $\dim(A_\mathfrak{m}) \le \dim(A) < i$, so we have a contradiction since $A_\mathfrak{m}$ is local. Hence $\mathrm{H}^i_I(A) = 0$ for $i > \dim(A)$. By part (1), $\mathrm{H}^i_I(M) = 0$ for $i > \dim(A)$.

(5) Let $\overline{A} = A/\operatorname{Ann}_A(M)$. Since M is an $\overline{A}$-module,

$$\mathrm{H}^i_I(M) \cong \mathrm{H}^i_{I\overline{A}}(M).$$

By part (4), $\mathrm{H}^i_{I\overline{A}}(M) = 0$ for $i > \dim(\overline{A}) = \dim(A/\operatorname{Ann}_A(M))$. ■

Definition If A is a Noetherian ring and I is an ideal of A, then we define the **cohomological dimension** of A as follows:

$$\operatorname{cd}(A, I) := \max_M\{d : \mathrm{H}^i_I(M) \neq 0\}$$

where M varies over all A-modules.

Corollary 9.4 *Let $(A, \mathfrak{m})$ be a local ring. Then*

$$\operatorname{cd}(A, \mathfrak{m}) = \dim(A).$$

Proposition 9.5 (Excision for Local Cohomology) *Let $I \subseteq J = I + xA$ be ideals in a local ring A. Let M be an A-module. Then we have a long exact sequence:*

$$\begin{array}{l} 0 \longrightarrow \mathrm{H}^0_J(M) \longrightarrow \mathrm{H}^0_I(M) \longrightarrow \mathrm{H}^0_I(M_x) \longrightarrow \\ \longrightarrow \mathrm{H}^1_J(M) \longrightarrow \mathrm{H}^1_I(M) \longrightarrow \mathrm{H}^1_I(M_x) \longrightarrow \\ \longrightarrow \cdots \qquad\qquad \cdots \longrightarrow \\ \longrightarrow \mathrm{H}^i_J(M) \longrightarrow \mathrm{H}^i_I(M) \longrightarrow \mathrm{H}^i_I(M_x) \longrightarrow \cdots \end{array}$$

Proof First note that for any ideals $I \subseteq J$, we have the exact sequence

$$A/I^t \to A/J^t \to 0$$

for all $t > 0$. Taking the long exact sequence of Ext and taking a direct limit over t, we have a map

$$\mathrm{H}^i_J(M) \to \mathrm{H}^i_I(M).$$

Now for $I \subseteq J = I + xA$, as above, consider the sequence of maps

$$0 \to \mathrm{H}^0_J(M) \to H^0_I(M) \to H^0_I(M_x)$$

where the last map send any element killed by a power of x to 0 and fixes the rest. Clearly if $J^t m = 0$ for $m \in M$, then $I^t m = 0$. So $\mathrm{H}^0_J(M) \to \mathrm{H}^0_I(M)$ is injective. Suppose $x^s m = 0$ with $m \in H^0_I(M)$. Then $I^t m = 0$ for some $t > 0$, hence $J^{t+s} m = 0$ and so $m \in \mathrm{H}^0_J(M)$. Similarly if $m \in \mathrm{H}^0_J(M)$, then $x^s m = 0$ for some $s > 0$. Thus the above sequence is exact for all A-modules M.

Now suppose E is an injective A-module. We want to show that we have a short exact sequence

$$0 \to \mathrm{H}^0_J(E) \to \mathrm{H}^0_I(E) \to \mathrm{H}^0_I(E_x) \to 0. \quad \bigstar$$

Then $E = \bigoplus E(A/\mathfrak{p}_i)$, so we may assume $E = E(A/\mathfrak{p})$ for some prime $\mathfrak{p}$. Recall that $E_A(A/\mathfrak{p})$ is an $A_\mathfrak{p}$-module where every element is killed by a power of $\mathfrak{p}$. If $x \in \mathfrak{p}$, then $E_A(A/\mathfrak{p})_x = 0$. If $\mathbf{x} \notin \mathfrak{p}$, then x acts as a unit on $E_A(A/\mathfrak{p})$ and so $H^0_J(E_A(A/\mathfrak{p})) = 0$ and $E_A(A/\mathfrak{p}) = E_A(A/\mathfrak{p})_x$. Therefore $\bigstar$ is exact.

Now let $0 \to M \to L^\bullet$ be an injective resolution of M. Note that $0 \to M_x \to L^\bullet_x$ is an injective resolution of M_x. Then we have a short exact sequence of complexes

$$0 \to \mathrm{H}^0_J(L^\bullet) \to H^0_I(L^\bullet) \to \mathrm{H}^0_I(L^\bullet_x) \to 0.$$

The associated long exact sequence gives us the desired result. ■

Lemma 9.6 *Let A be a normal domain, let $K = \mathrm{Frac}(A)$, and let L/K be a field extension. Suppose that $x \in L$ is integral over A. Then $A[x] \cong A[X]/(f(X))$ where $f(X)$ is a monic irreducible polynomial in $A[X]$.*

Proof Since x is integral over A, it is algebraic over K. Let $f(X)$ be the minimal polynomial for x in $K[X]$. Since x is integral over A, all conjugates of x are integral over A. Therefore the coefficients of $f(X)$ are integral over A. Since A is normal, the coefficients of $f(X)$ are in A. Let $T = \mathrm{Ker}(A[X] \twoheadrightarrow A[x])$. Clearly $(f(X)) \subseteq T$. If $g(X) \in T$, then $g(x) = 0$. Therefore $f(X) \,|\, g(X)$ in $K[X]$. Since $f(X)$ is monic, $g(X) \in A[X]$. Hence $g(X) \in (f(X))$ and so $A[x] \cong A[X]/T \cong A[X]/(f(x))$. ■

Lemma 9.7 (Chevalley's Lemma) *Let $(A, \mathfrak{m})$ be a complete local ring. Let M be a finitely generated A-module with $\{M_t\}$ a nonincreasing sequence of submodules of M. Then*

$$\bigcap_t M_t = 0 \;\Leftrightarrow\; \textit{for every } n > 0 \textit{ there exists } t > 0 \textit{ with } M_t \subseteq \mathfrak{m}^n M.$$

Proof Note that the implication ($\Leftarrow$) is obvious from Krull's Intersection Theorem.

($\Rightarrow$) Suppose that $\bigcap_t M_t = 0$. Consider the composition

$$\varphi_{t,n} : M_t \hookrightarrow M \twoheadrightarrow M/\mathfrak{m}^n M$$

for each $t, n > 0$. Set $V_{t,n} = \mathrm{Im}(\varphi_{t,n})$. If $V_{t,n} \neq 0$ for all $t > 0$, then since $M/\mathfrak{m}^n M$ has finite length, the modules $V_{t,n}$ stabilize for large t; that is, $V_n = \bigcap_t V_{t,n} = V_{t,n}$ for $t >> 0$. Note that we have a surjection $V_{n+1} \twoheadrightarrow V_n$ for all $n > 0$. Thus we have

$$V = \varprojlim_n V_n \subseteq \varprojlim_n M/\mathfrak{m}^n M = M.$$

However, one checks that

$$V \subseteq \bigcap_{t,n} (M_t + \mathfrak{m}^n M) = \bigcap_t \left(\bigcap_n M_t + \mathfrak{m}^n M \right) = \bigcap_t M_t = 0.$$

Hence $V = 0$ from which it follows that $V_n = 0$ for $n >> 0$; that is, $M_t \subseteq \mathfrak{m}^n M$ for $t >> 0$.

■

Theorem 9.8 (Hartshorne-Lichtenbaum Vanishing Theorem) *Let $(A, \mathfrak{m})$ be a local ring of dimension d and I be an ideal of A. We have the following:*

(1) *If A is a complete local domain, then $\mathrm{H}^d_I(A) = 0$ when I is not $\mathfrak{m}$-primary. Note that this says that $\mathrm{cd}(A, I) \leq d - 1$.*

(2) *$\mathrm{H}^d_I(A) = 0$ if and only if for every minimal prime ideal $\mathfrak{p}$ in $\widehat{A}$ such that $\dim(\widehat{(}A)/\mathfrak{p}) = d$, $\mathfrak{p} + I\widehat{A}$ is not $\widehat{\mathfrak{m}}$-primary.*

Proof First we show that (1) $\Rightarrow$ (2). We may assume that A is complete. Suppose $\mathrm{H}^d_I(A) = 0$. Let $\mathfrak{p}$ be a minimal prime. Then

$$\mathrm{H}^d_I(A) \to \mathrm{H}^d_I(A/\mathfrak{p}) \to 0$$

is exact. Therefore $H^d_I(A/\mathfrak{p}) = 0$. So by (1), $\mathfrak{p} + I$ is not $\mathfrak{m}$-primary.

Conversely, suppose that for all primes $\mathfrak{p}$ with $\dim(A/\mathfrak{p}) = d$, we have $\mathfrak{p} + I$ is not $\mathfrak{m}$-primary. Then $\mathrm{H}^d_I(A/\mathfrak{p}) = \mathrm{H}^d_{(I+\mathfrak{p})/\mathfrak{p}}(A/\mathfrak{p}) = 0$ by part (1). Note that $\mathrm{H}^d_I(A/\mathfrak{p}) = 0$ for the nonminimal associated primes as well since $\dim(A/\mathfrak{p}) < d$. Taking a filtration of A and using the long exact sequence of local cohomology, it follows that $H^d_I(A) = 0$.

We now prove part (1). For this part of the proof, we will need a few steps.

Step 1 Reduction to the case where I is a prime ideal of A such that $\dim(A/I) = 1$.

Suppose this is not the case. Then let I be maximal in the family of non $\mathfrak{m}$-primary ideals such that the $\mathrm{H}^d_I(A) \neq 0$. If I is not prime with $\dim(A/I) = 1$, then there exists $x \notin I$ such that $J = I + xA$ is not $\mathfrak{m}$-primary. Using the excision sequence, we have that

$$\mathrm{H}^d_J(A) \to \mathrm{H}^d_I(A) \to \mathrm{H}^d_I(A_x) \to 0$$

is exact. Since A is a local domain with $\dim(A) = d$, then $\dim(A_x) < d$. Therefore $\mathrm{H}^d_I(A_x) = 0$. But $\mathrm{H}^d_I(A) \neq 0$ by assumption and hence $\mathrm{H}^d_J(A) \neq 0$ by the above exact sequence. This is a contradiction since I was chosen to be maximal.

Step 2 Reduction to the case where A is a complete, local, Gorenstein domain.

Since we can now assume that I is prime, set $P = I$. Let $x_1, \ldots, x_d$ be a system of parameters of A such that $x_1, \ldots, x_{d-1} \in P$ and $x_d \notin P$. To invoke the Cohen Structure Theorem, we need to consider a few separate cases:

Case a: If A is equicharacteristic, then A contains a field k and is module-finite over the ring $S = k[\![x_1, \ldots, x_d]\!]$. Moreover, $P \cap S = (x_1, \ldots, x_d)$.

Case b: If A is mixed characteristic with $\mathrm{char}(A/\mathfrak{m}) = p$ and $p \in P$, we can take $x_1 = p$. Then A is module finite over $S = V[\![x_2, \ldots, x_d]\!]$ where V is a complete DVR and $P \cap S = (p, x_2, \ldots, x_{d-1})$.

Case c: If A is mixed characteristic with $\mathrm{char}(A/\mathfrak{m}) = p$ and $p \notin P$, then A is module-finite over $S = V[\![x_1, \ldots, x_{d-1}]\!]$ where V is a complete DVR and $P \cap S = (x_1, \ldots, x_{d-1})$.

In all three cases, we can find a complete regular local ring S such that $S \to A$ is a module-finite extension and such that $P \cap S$ is an ideal generated by part of a regular system of paramters of S.

Let $P_1, \ldots, P_t$ be the minimal primes of A containing $P \cap S$. Let

$$a \in P - \bigcup_{i \neq 1} P_i.$$

Set $B = S[a]$. Then $B \cong S[X]/(f(X))$ by the previous lemma. Set $Q = P \cap B$. Then P is the only height $d-1$ prime of A containing Q. Therefore $\sqrt{QA} = P$ and hence

$$\mathrm{H}^d_Q(A) = \mathrm{H}^d_{QA}(A) = \mathrm{H}^d_P(A).$$

Note that B is a complete, d-dimensional, complete-intersection and hence Gorenstein. Moreover, A is module-finite over B. So it suffices to show that $\mathrm{H}^d_Q(B) = 0$ by Proposition 9.3.

Step 3 The rest of the proof.

We want to show that $\{P^t\}$ and $\{P^{(t)}\}$ are cofinal families of ideals. Clearly $P^t \subseteq P^{(t)}$ for every $t > 0$. We must also show that for every $n > 0$, there exists $t > 0$ such that $P^{(t)} \subseteq P^n$. Fix $n > 0$. Consider a primary decomposition of P^t. Since P is prime with $\dim(A/P) = 1$, the only possible associated primes of P^t are P and the maximal ideal $\mathfrak{m}$. Recall that the symbolic power $P^{(t)}$ is the smallest P-primary ideal containing P^t. Thus the primary decomposition of P^n is of the form

$$P^n = P^{(n)} \quad \text{or} \quad P^n = P^{(n)} \cap J,$$

where J is $\mathfrak{m}$-primary. If $P^n = P^{(n)}$ then we are done. So assume $P^n = P^{(n)} \cap J$. Since J is $\mathfrak{m}$-primary, there is some $s > 0$ such that $\mathfrak{m}^s \subseteq J \subseteq \mathfrak{m}$. Since A is a

domain,

$$\bigcap_t P^{(t)} = \bigcap_t \left(A \cap P^t A_P\right) \subseteq \bigcap_t P^t A_P = 0,$$

by Krull's Intersection Theorem. By Chevalley's Lemma, there exists $t > 0$ such that $P^{(t)} \subseteq \mathfrak{m}^s$. Hence

$$P^{(\max\{t,n\})} \subseteq P^{(n)} \cap \mathfrak{m}^s \subseteq P^{(n)} \cap J = P^n.$$

Therefore the two sequences of ideal $\{P^t\}$ and $\{P^{(t)}\}$ are cofinal. Hence

$$\mathrm{H}^d_P(A) = \varinjlim_t \mathrm{Ext}^d_A(A/P^t, A) = \varinjlim_t \mathrm{Ext}^d_A(A/P^{(t)}, A).$$

Since $P^{(t)}$ is P-primary, $\mathrm{Hom}_A(A/\mathfrak{m}, A/P^{(t)}) = 0$. Therefore $\mathrm{depth}(A/P^{(t)}) > 0$ for all $t > 0$. Hence by local duality,

$$\mathrm{Ext}^d_A(A/P^{(t)}, A) = H^0_{\mathfrak{m}}(A/P^{(t)})^\vee = 0,$$

for all $t > 0$. Therefore

$$H^d_P(A) = \varinjlim_t \mathrm{Ext}^d_A(A/P^{(t)}, A) = 0.$$

■

9.2 Canonical Modules of Local Rings

Recall the defintion of a canonical module.

Definition If A is a local ring, a finitely generated A-module ω is called a **canonical module** for A if

$$\widehat{\omega} \cong \mathrm{H}^n_{\mathfrak{m}}(A)^\vee. \qquad (\text{i.e.} \quad \omega^\vee \cong \mathrm{H}^d_{\mathfrak{m}}(A))$$

Definition $\mathrm{J}(A)$ is ideal of A defined as follows

$$\mathrm{J}(A) := \{x \in A : \dim(xA) < \dim(A)\},$$

Hence $\mathrm{J}(A)$ is the maximal ideal such that its dimension as a module is less than the dimension of the ring.

Remark Observe that if $x, y \in J(A)$ and $a \in A$ then $x + y \in J(A)$ and $ax \in J(A)$, so $J(A)$ is actually an ideal. Note moreover that $R = A/J(A)$ is unmixed, meaning it has no embedded primes, and equidimensional, meaning $\dim R/\mathfrak{p} = \dim R$ for all $\mathfrak{p} \in \mathrm{Ass}(R)$.

Proposition 9.9 (Properties of Canonical Modules) *If A is a local ring of dimension n, then we have the following:*

(1) *If A is complete, then A has a canonical module.*

(2) *If ω_1 and ω_2 are two canonical modules for A, then there is a nonunique isomorphism $\omega_1 \cong \omega_2$.*

(3) *If $R \longrightarrow fA$ is a local ring homomorphism of local rings such that R is Cohen-Macaulay with canonical module ω_R and A is module-finite over $f(R)$, then $\mathrm{Ext}_R^{\dim(R)-\dim(A)}(A, \omega_R)$ is a canonical module for A. (In particular, if A is the image of a Gorenstein ring or if A is a module finite extension of a Gorenstein ring, then A has a canonical module.).*

(4) *If A has a canonical module ω, then ω is also a canonical module for $R/\mathrm{J}(R)$; that is, ω is killed by $\mathrm{J}(R)$.*

Proof (1) Simply take $\omega = \widehat{\omega} = \mathrm{H}^d_{\mathfrak{m}}(A)^\vee$.

(2) This follows from Proposition 8.33.

(3) Suppose R and A are as above. Set $\omega_A = \mathrm{Ext}^h_R(A, \omega_R)$ where $h = \dim(R) - \dim(A)$. Then

$$\widehat{\omega_A} = \widehat{\mathrm{Ext}^h_R(A, \omega_R)} = \mathrm{Ext}^{\dim(\widehat{R})-\dim(\widehat{A})}_{\widehat{R}}(\widehat{A}, \widehat{\omega_R}) \cong \mathrm{H}^{\dim(R)}_{\mathfrak{m}}(A)^\vee,$$

where the last isomorphism follows from the local duality for Cohen-Macaulay rings.
(4) Consider the short exact sequence

$$0 \to J(A) \to A \to A/J(A) \to 0.$$

Since $\dim(J(A)) < \dim(A) = d$, we have that

$$0 \to \mathrm{H}^d_{\mathfrak{m}}(A) \to \mathrm{H}^d_{\mathfrak{m}}(A/J(A)) \to 0$$

is exact by the long exact sequence of local cohomology. Hence

$$\omega_A \cong \mathrm{H}^d_{\mathfrak{m}}(A)^\vee \cong \mathrm{H}^d_{\mathfrak{m}}(A/J(A))^\vee.$$

Therefore ω_A is killed by $J(A)$. ■

Definition If A is a Noetherian ring and M is a finitely generated A-module, M is said to satisfy **Serre's $\mathbf{S_i}$ condition** if for all $\mathfrak{p} \in \mathrm{Spec}(A)$

$$\mathrm{depth}(M_{\mathfrak{p}}) \geq \min\{\dim(M_{\mathfrak{p}}), i\}.$$

Remark If M is S_i, then for all $\mathfrak{p} \in \mathrm{Spec}(A)$ such that $\dim(M_{\mathfrak{p}}) \leq i$, $M_{\mathfrak{p}}$ is Cohen-Macaulay.

Definition If A is a Noetherian ring and M is a finitely generated A-module, M is said to satisfy **Serre's $\mathbf{R_i}$ condition** if for all $\mathfrak{p} \in \mathrm{Spec}(A)$ such that $\mathrm{ht}(\mathfrak{p}) \leq i$, $A_{\mathfrak{p}}$ is a regular local ring.

Definition A ring A is called **normal** if for all $\mathfrak{p} \in \mathrm{Spec}(A)$, $A_{\mathfrak{p}}$ is a normal domain.

Exercise 9.10 *Show if A is normal, then*

$$A = A_1 \oplus \cdots \oplus A_n$$

where each A_i is a normal domain.

Exercise 9.11 *Show if A is regular, then*

$$A = A_1 \oplus \cdots \oplus A_n$$

where each A_i is a regular domain.

Exercise 9.12 *Show that a ring is normal if and only if A is S_2 and R_1.*

Proposition 9.13 *If A is Noetherian and M is a finitely generated A-module, then the following hold:*

(1) *M satisfies S_i if and only if for all ideals I of A, such that $I \not\subseteq \mathrm{Ann}_A(M)$,*

$$\mathrm{depth}_I(M) \geq \min\left\{\mathrm{ht}\left(\frac{I + \mathrm{Ann}_A(M)}{\mathrm{Ann}_A(M)}\right), i\right\}.$$

(2) *If M is S_1, then M does not have any embedded primes. If A is S_1 then A is unmixed and local. If A is S_2 and catenary, then A is equidimensional.*

(3) *If M is S_i over a ring, and A is a module finite extension of the same ring, then M is S_i as an A-module.*

(4) *Let $f : A \to B$ is a local flat homomorphism of rings, and M is a finitely generated A-module. If $M \otimes_A B$ satisfies S_i over B, then M satisfies S_i over A.*

If M is S_i over A and and the fibers of f,

$$\boldsymbol{\kappa}(\mathfrak{p}) \otimes_A B,$$

are Cohen-Macaulay, then $M \otimes_A B$ satisfies S_i over B.

Proof (1) ($\Rightarrow$) Suppose M satisfies S_i. Set $\overline{I} = \frac{I + \mathrm{Ann}_A(M)}{\mathrm{Ann}_A(M)}$. Then

$$\begin{aligned}
\mathrm{depth}_I(M) &= \inf_{P \supseteq I} \mathrm{depth}(M_P) \\
&\geq \inf_{P \supseteq I} \{\min(i, \dim(M_P))\} \\
&= \inf_{\overline{P} \supseteq \overline{I}} \{\min(i, \dim(M_{\overline{P}}))\} \\
&= \inf_{\overline{P} \supseteq \overline{I}} \{\min(i, \mathrm{ht}(\overline{P}))\} \\
&= \min(i, \inf_{\overline{P} \supseteq \overline{I}} \mathrm{ht}(\overline{P})) \\
&= min(i, \mathrm{ht}(\overline{I})).
\end{aligned}$$

($\Leftarrow$) Now suppose we have the above inequality for all ideal I. Then

$$\operatorname{depth} M_P \geq \operatorname{depth}_P M \geq \min(i, \operatorname{ht}(\overline{P}) = \min(i, \dim(M_P)).$$

(2) ■

Theorem 9.14 *If A is a local ring which is the image of a Gorenstein ring, and ω is the canonical module for A, then we have the following:*

(1) *There exists an A-module homomorphism*

$$A \to \operatorname{Hom}_A(\omega, \omega),$$
$$a \mapsto \text{map defined by multiplication by } a,$$

where $\mathrm{J}(A)$ is the kernel of the map above and so if ω is a faithful A-module, then A is equidimensional and unmixed.

(2) *Suppose that A is equidimensional. Then for all $\mathfrak{p} \in \operatorname{Spec}(A)$, $\omega_{\mathfrak{p}}$ is the canonical module for $A_{\mathfrak{p}}$.*

(3) *If x is a nonzerodivisor on A, then x is a nonzerodivisor on ω and*

$$\omega/x\omega \hookrightarrow \omega_{A/xA}.$$

(4) *Both ω and $\operatorname{Hom}_A(\omega, \omega)$ are S_2. Moreover, $\operatorname{Hom}_A(\omega, \omega)$ can be identified with an A-submodule of $U^{-1}(A/\mathrm{J}(A))$ where U is the set of all nonzerodivisors in $A/\mathrm{J}(A)$. Hence $\operatorname{Hom}_A(\omega, \omega)$ is a semi-local module finite extension of $A/\mathrm{J}(A)$. Moreover*

$$A \to \operatorname{Hom}_A(\omega, \omega)$$

is an isomorphism if and only if A is S_2.

(5) *If A is unmixed, equidimensional, and generically Gorenstein—that is for all $\mathfrak{p} \in \operatorname{Ass}(A)$, $A_{\mathfrak{p}}$ is a Gorenstein local ring, then ω can be identified with an ideal of A containing a nonzerodivisor of A. Moreover if A is S_2, then ω is pure of height 1, that is, for all $\mathfrak{p} \in \operatorname{Ass}(A/\omega)$, $\operatorname{ht}(\mathfrak{p}) = 1$.*

Theorem 9.15 (Murthy's Theorem) *Let A be a Cohen-Macaulay, locally UFD ring that is the image of a Gorenstein ring. Then A is Gorenstein.*

Proof Note that we may assume that A is a local $Cohen - Macualay$ UFD that is the image of a Gorenstein ring of dimension at least 2. Then since A is the image of a Gorenstein ring, we can write $A = S/P$ where S is a Gorenstein ring and $\dim(A) = \dim(S)$. Then A has a canonical module $\omega = \operatorname{Hom}_S(A, S) = \operatorname{Hom}_S(S/P, S)$. By a previous exercise, ω is a torsionfree A-module of rank 1. Hence ω is a reflexive module. One can show then that since ω is a rank 1 reflexive module, then

$$U^{-1}\omega = U^{-1}A = \operatorname{Frac}(A),$$

where $U = A - \{0\}$ is the set of nonzero elements in A.

Hence we have an injection $\omega \hookrightarrow \mathrm{Frac}(A)$. Since ω is finitely generated, write $\omega = \left(\frac{a_1}{t}, \ldots, \frac{a_s}{t}\right)$ where each $\frac{a_i}{t} \in K$ and $0 \neq t \in A$. Hence ω is isomorphic to the ideal $I = (a_1, \ldots, a_s) \subseteq A$.

Now take $\mathfrak{p} \in \mathrm{Ass}(R/I)$. We want to show that $\mathrm{ht}(\mathfrak{p}) = 1$. Suppose $\mathrm{ht}(\mathfrak{p}) \geq 2$. Then consider the short exact sequence

$$0 \to I \to A \to A/I \to 0.$$

Localize at $\mathfrak{p}$ to get the short exact sequence

$$0 \to IA_{\mathfrak{p}} \to A_{\mathfrak{p}} \to A_{\mathfrak{p}}/IA_{\mathfrak{p}} \to 0.$$

Since $\mathrm{ht}(\mathfrak{p}) \geq 2$ and since ω is S_2, $\operatorname{depth} IA_{\mathfrak{p}} \geq 2$. But since $\mathfrak{p} \in \mathrm{Ass}(R/I)$ the depth of $A_{\mathfrak{p}}/IA_{\mathfrak{p}}$ is 0, a contradiction. Hence all associated primes of R/I have height 1.

Now take a primary decomposition of I:

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r,$$

where $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary. Since A is a UFD, A is normal so

$$\mathfrak{q}_i A_{\mathfrak{p}_i} \subseteq A_{\mathfrak{p}_i},$$

where each $A_{\mathfrak{p}_i}$ is a DVR since all the associated primes $\mathfrak{p}_i$ have height one. Thus $\mathfrak{q}_i A_{\mathfrak{p}_i} = (\mathfrak{p}_i A_{\mathfrak{p}_i})^{n_i}$ for some $n_i > 0$. Thus $\mathfrak{q}_i = \mathfrak{p}_i^{(n_i)}$. Since A is a UFD, each height one prime is principal. Therefore

$$I = \mathfrak{p}_1^{(t_1)} \cap \cdots \cap \mathfrak{p}_r^{(t_r)} = \mathfrak{p}_1^{t_1} \cdots \mathfrak{p}_r^{t_r},$$

and so I is principal - that is, $I \cong A$. Thus $\omega \cong I \cong A$. Since A is Cohen-Macaulay with $\omega \cong A$, we have that A is Gorenstein. ■

Recall that if A is a Cohen-Macaulay ring of dimension n with a canonical module ω, then by Local Duality, we have

$$\mathrm{H}^i_{\mathfrak{m}}(M) \cong \mathrm{Ext}^{n-i}_A(M, A)^\vee$$

for all finitely generated A-modules M and all $i \leq n$. Unfortunately this is not the case when A is merely a local ring. However we can say this:

Proposition 9.16 *Let $(A, \mathfrak{m})$ be a local ring of dimension n with a canonical module ω, and let M be a finitely generated A-module. Then only the highest nonzero local cohomology module satisfies a duality, that is:*

$$\mathrm{H}^n_{\mathfrak{m}}(M) \cong \mathrm{Hom}_A(M, \omega)^\vee.$$

Corollary 9.17 *Let $A \to B$ be a homomorphism of local rings and B be a module finite extension of A. If ω is a canonical module for A, then $\mathrm{Hom}_A(B, \omega)$ is a canonical module for B.*

Theorem 9.18 (cf. Theorem 9.14) *If A is a local ring of dimension n with a canonical module ω, then we have the following:*

(1) *There exists an A-module homomorphism*

$$\begin{aligned} &A \to \mathrm{Hom}_A(\omega, \omega), \\ &a \mapsto \textit{map defined by multiplication by } a, \end{aligned}$$

where $\mathrm{J}(A)$ is the kernel of the map above.

(2) *Both ω and $\mathrm{Hom}_A(\omega, \omega)$ are S_2. Moreover, $\mathrm{Hom}_A(\omega, \omega)$ can be identified with an A-submodule of $U^{-1}(A/\mathrm{J}(A))$ where U is the set of all nonzerodivisors in $A/\mathrm{J}(A)$. Hence $\mathrm{Hom}_A(\omega, \omega)$ is a semi-local module finite extension of $A/\mathrm{J}(A)$.*

(3) *If we consider $\mathfrak{p} \in \mathrm{Ass}(A)$ such that $\dim(A/\mathfrak{p}) = \dim(A)$, then we have $\widehat{A}/\mathfrak{p}\widehat{A}$ is equidimensional.*

(4) *The map given above*

$$A \to \mathrm{Hom}_A(\omega, \omega)$$

is an isomorphism if and only if A is S_2.

Proposition 9.19 *Let $(A, \mathfrak{m}) \to (B, \mathfrak{n})$ be a local, flat, homomorphism of rings. Assuming that $B/\mathfrak{m}B$ is a 0-dimensional Gorenstein ring we then have:*

(1) *$E_B(B/\mathfrak{n}) = B \otimes_A E_A(A/\mathfrak{m})$.*

(2) *If ω is a canonical module for A, then $\omega \otimes_A B$ is a canonical module for B.*

Theorem 9.20 *Let $A \to B$ be a flat homomorphism of local rings and M and N be finitely generated A-modules. If*

$$M \otimes_A B \cong N \otimes_A B,$$

then $M \cong N$.

9.3 Mayer-Vietoris Sequence for Local Cohomology

The next theorem is a very useful tool to have when working with local cohomology:

Theorem 9.21 *If A is a Noetherian ring, I and J are two ideals, and M is an A-module, then we have a long exact sequence of local cohomology modules:*

$$\begin{array}{l} 0 \longrightarrow \mathrm{H}^0_{I+J}(M) \longrightarrow \mathrm{H}^0_I(M) \oplus \mathrm{H}^0_J(M) \longrightarrow \mathrm{H}^0_{I\cap J}(M) \longrightarrow \\ \longrightarrow \mathrm{H}^1_{I+J}(M) \longrightarrow \mathrm{H}^1_I(M) \oplus \mathrm{H}^1_J(M) \longrightarrow \mathrm{H}^1_{I\cap J}(M) \longrightarrow \\ \longrightarrow \cdots \qquad\qquad \cdots \longrightarrow \\ \longrightarrow \mathrm{H}^i_{I+J}(M) \longrightarrow \mathrm{H}^i_I(M) \oplus \mathrm{H}^i_J(M) \longrightarrow \mathrm{H}^i_{I\cap J}(M) \longrightarrow \cdots \end{array}$$

Proof First let M be any A-module. It is easy to check that we that the following sequence is exact:

$$\begin{array}{ccccc} 0 & \longrightarrow & H^0_{I+J}(M) & \longrightarrow & H^0_I(M) \oplus H^0_J(M) \longrightarrow H^0_{I\cap J}(M) \\ & & x & \longmapsto & (x,-x) \\ & & & & (x,y) \longmapsto x+y. \end{array}$$

Now let E be an injective A-module. We wish to show this left exact sequence is also right exact; that is that

$$0 \to H^0_{I+J}(E) \to H^0_I(E) \oplus H^0_J(E) \to H^0_{I\cap J}(E) \to 0$$

is exact. By previous work, $E = \bigoplus_i E_A(A/\mathfrak{p}_i)$. Since direct sums commute with homology, we may assume that $E = E_A(A/\mathfrak{p})$ for some prime ideal $\mathfrak{p}$. Since $E_A(A/\mathfrak{p}) = E_{A_\mathfrak{p}}(A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p})$ and since $H^0_I(E) = H^0_{IA_\mathfrak{p}}(E)$, we may assume that A is local with maximal ideal $\mathfrak{p}$. By a previous proposition, $E = E_A(k)$ is Artinian, and so $E = \varinjlim M_i$ where $\lambda(M_i) < \infty$. Since direct limits commute with homology, we may assume that $E = M$ and $\lambda(M) < \infty$. By replacing A by $A/\operatorname{Ann}_A(M)$, we may assume that $\dim(A) = 0$. Note then that the only radical ideals in A are (0) and A. Since we may replace I and J by $\sqrt{I}$ and $\sqrt{J}$, there are four cases to consider: $I = 0$ or A and $J = 0$ or A. But each of these cases is easily checked by hand.

Now let M be an arbitrary A-module and let $0 \to M \to L^\bullet$ be an injective resolution of M. Then we have a short exact sequence of complexes

$$0 \to H^0_{I+J}(L^\bullet) \to H^0_I(L^\bullet) \oplus H^0_J(L^\bullet) \to H^0_{I\cap J}(L^\bullet) \to 0.$$

The associated long exact sequence in homology, gives us the Mayer-Vietoris sequence. ■

At this point let us revisit an exercise that we stated earlier:

Exercise 9.22 *If*

$$A = \frac{\mathbb{C}[X,Y,U,V]}{(X,Y)\cap(U,V)}$$

show that A is not Cohen-Macaulay.

When this exercise was given earlier, Hartshorne's Connectedness Theorem was the intended tool to be used to solve this problem. However, now we may give another proof using the theorems above.

Exercise 9.23 *Prove Hartshorne's Connectedness Theorem, Theorem 6.64, using the Mayer-Vietoris Sequence for local cohomology.*

Thus from the exercise above we see that in a sense, Hartshorne's Connectedness Theorem, Theorem 6.64, is merely a special case of the Mayer-Vietoris seqence for local cohomology.

9.4 Faltings' Connectedness Theorem

Theorem 9.24 (Faltings Connectedness Theorem) *If $(A,\mathfrak{m})$ is a complete local domain of dimension d and $\mathfrak{a}$ is an ideal of A be generated by at most $d-2$ elements, then the punctured spectrum,*

$$\operatorname{Spec}(A/\mathfrak{a}) - \{\mathfrak{m}/\mathfrak{a}\},$$

is connected.

Proof Suppose for some ideals I, J of A containing $\mathfrak{a}$ we have $\operatorname{Spec}(A/\mathfrak{a}) - \{\mathfrak{m}/\mathfrak{a}\} = V(I/\mathfrak{a}) \cup V(J/\mathfrak{a})$ and $V(I/\mathfrak{a}) \cap V(J/\mathfrak{a}) = \{\mathfrak{m}/\mathfrak{a}\}$. In other words, $\sqrt{I\cap J} = \sqrt{\mathfrak{a}}$ and $\sqrt{I+J} = \mathfrak{m}$; that is, $I+J$ is $\mathfrak{m}$-primary. We wish to show that $V(I/\mathfrak{a}) = \{\mathfrak{m}/\mathfrak{a}\}$ or $V(J/\mathfrak{a}) = \{\mathfrak{m}/\mathfrak{a}\}$. Algebraically, we must show that $\sqrt{I} = \mathfrak{m}$ or $\sqrt{J} = \mathfrak{m}$. By the Mayer-Vietoris sequence for I, J we get that

$$H^{d-1}_{I\cap J}(A) \to H^d_{I+J}(A) \to H^d_I(A) \oplus H^d_J(A) \to H^d_{I\cap J}(A) \to 0$$

is exact. Since $\mathfrak{a}$ is generated by at most $d-2$ elements, $H^{d-1}_{\mathfrak{a}}(A) = H^d_{\mathfrak{a}}(A) = 0$. Since $\sqrt{I\cap J} = \sqrt{\mathfrak{a}}$, $H^{d-1}_{I\cap J}(A) = H^d_{I\cap J}(A) = 0$. Hence

$$H^d_{I+J}(A) \cong H^d_I(A) \oplus H^d_J(A).$$

Since $I+J$ is $\mathfrak{m}$-primary, $H^d_{I+J}(A) \neq 0$. Therefore $H^d_I(A) \neq 0$ or $H^d_J(A) \neq 0$. Hence, by the Hartshorne Lichtenbaum Vanishing Theorem, one of I or J is $\mathfrak{m}$-primary. Therefore either $\sqrt{I} = \mathfrak{m}$ or $\sqrt{J} = \mathfrak{m}$. ■

Definition A finite dimensional ring A is called **equidimensional** if

$$\dim(A) = \dim(A/\mathfrak{p})$$

whenever $\mathfrak{p}$ is a minimal element of $\operatorname{Spec}(A)$.

The following result is due to Hochster and Huneke:

Theorem 9.25 (Generalized Faltings Connectedness Theorem) *If A is an equidimensional local ring of dimension n, $\mathrm{H}^n_{\mathfrak{m}}(A)$ is indecomposable, and $\mathfrak{a}$ is an ideal of A be generated by less than $n-2$ elements, then the punctured spectrum,*

$$\mathrm{Spec}(A/\mathfrak{a}) - \{\mathfrak{m}/\mathfrak{a}\},$$

is connected.

The following connectedness result is due to Fulton and Hansen and is derived from Falting's result.

Theorem 9.26 *Let K be an algebraically closed field, and let X and Y be irreducible sets in $\mathbb{P}^n_K$. If $\dim X + \dim Y \geq n+1$, then $X \cap Y$ is connected.*

9.5 The Krull Schmidt Theorem

We will state the Krull Schmidt Theorem for modules of finite length and then progressively generalize it.

The Krull Schmidt Theorem for Modules of Finite Length

Theorem 9.27 (Krull-Schmidt) *Let M be a module of finite length over a ring A. Then we can write*

$$M = M_1 \oplus \cdots \oplus M_r$$

where each M_i is indecomposable. Moreover if

$$M = M'_1 \oplus \cdots \oplus M'_s$$

is another such decomposition, then $r = s$ and there exists $\sigma \in S_r$ such that $M_i \cong M'_{\sigma(i)}$ for every i.

The Krull Schmidt Theorem over Complete Local Rings

Proposition 9.28 *Let A be a complete local ring and M be a finitely generated A-module. If $f : M \to M$ is a A-module homomorphism, we have the following:*

(1) *$M = V \oplus W$ such that $f|_V$ is an isomorphism and given any t, there exists n such that $f^n(W) \subseteq \mathfrak{m}^t W$.*

(2) *If M is indecomposable, then every endomorphism f is either an isomorphism or for some t, there exists n sufficiently large such that $f^n(W) \subseteq \mathfrak{m}^t W$.*

(3) *If M is indecomposable, then the nonunits of $\mathrm{End}_A(M)$ form a 2-sided ideal.*

Theorem 9.29 (Krull-Schmidt) *Let M be a finitely generated module over a complete local ring A. Then we can write*

$$M = M_1 \oplus \cdots \oplus M_r$$

where each M_i is indecomposable. Moreover if

$$M = M_1' \oplus \cdots \oplus M_s'$$

is another such decomposition, then $r = s$ and there exists $\sigma \in S_r$ such that $M_i \cong M'_{\sigma(i)}$ for every i.

Exercise 9.30 *If A is a complete local ring, M, N, and T are finitely generated A-modules, if $M \oplus T \cong N \oplus T$, then show that $M \cong N$. Moreover show that if*

$$\bigoplus_{i=1}^{n} M \cong \bigoplus_{i=1}^{n} N$$

then $M \cong N$.

Theorem 9.31 *Let $A \to B$ be a local, flat, homomorphism, with M and N finitely generated A-modules, if $M \otimes_A B \cong N \otimes_A B$, then $M \cong N$.*

9.6 S_2-ification

Theorem 9.32 *Let A be local, equidimensional, and S_2, with a canonical module ω. The the following are true:*

(1) *For all $\mathfrak{p} \in \operatorname{Spec}(A)$, $\widehat{A}/\mathfrak{p}\widehat{A}$ is generically Gorenstein. In particular if $\mathfrak{p} \in \operatorname{Ass}_A(A)$, then $\widehat{A}/\mathfrak{p}\widehat{A}$ is unmixed and generically Gorenstein.*

(2) *For all $\mathfrak{p} \in \operatorname{Spec}(A)$, $\omega_{\mathfrak{p}}$ is a canonical module for $A_{\mathfrak{p}}$.*

Proposition 9.33 *If A is a local ring with $\mathrm{J}(A) = 0$, and ω is a canonical module for A, consider*

$$A \hookrightarrow \operatorname{Hom}_A(\omega, \omega) = B.$$

In this case it can be shown that B is module finite over A and it is contained in the total quotient ring of A as an A-algebra. The following hold:

Every maximal ideal of B has the same height.

If A is complete, then so is B. Moreover, if

$$B = \widehat{B}_{\mathfrak{m}_1} \oplus \cdots \oplus \widehat{B}_{\mathfrak{m}_r}$$

then

$$\omega = \omega_1 \oplus \cdots \oplus \omega_r,$$

where each ω_i is a canonical module for $\widehat{B}_{\mathfrak{m}_i}$

ω is a canonical module fo B in the sence that for all $\mathfrak{p} \in \mathrm{Spec}(B)$, $\omega_{\mathfrak{p}}$ is a canonical module for $B_{\mathfrak{p}}$.

Definition If $A \hookrightarrow B$ and B is a semi-local, module finite extension of A, then B is called the **$\mathbf{S_2}$-ification** of A if

(1) B is contained in the total quotient ring of A. as an A-subalgebra.

(2) For any $b \in B$,

$$D(b) := (A :_A b) = \{a \in A : ab \in A\}$$

is an ideal of height 2 or larger.

(3) B is S_2.

Remark The letter D used in the aboved definition is hopefully reminsient of the word *denomators*.

Proposition 9.34 *If A is local and $\mathrm{J}(A) = 0$, let*

$$R = \{b \in Q(A) : \mathrm{ht}(D(b)) \geq 2\}.$$

Then

(1) *R is a subring of $Q(A)$ containg A.*

(2) *If B is a A-algebra of $Q(A)$ such that B is S_2, then $R \subseteq B$.*

(3) *R is the S_2-ification of A if and only if R is a finitely generated A-module.*

Proposition 9.35 *If A is a local ring, and $\mathrm{J}(A) = 0$ with ω being a canonical module for A, then*

$$B = \mathrm{Hom}_A(\omega, \omega)$$

is the S_2-ification of A.

Proposition 9.36 *If A is local, $\mathrm{J}(A) = 0$, assume that A is catenary. If B is the S_2-ification of A, then for all $\mathfrak{p} \in \mathrm{Spec}(A)$, $B_{\mathfrak{p}}$ is the S_2-ification of $A_{\mathfrak{p}}$.*

Proof ■

Theorem 9.37 *If A is a local equidimenisonal catenary, ring with canonical module ω, then for all $\mathfrak{p} \in \mathrm{Spec}(A)$, $\omega_{\mathfrak{p}}$ is a canonical module for $A_{\mathfrak{p}}$.*

Proof COME BACK TO THIS!

■

Definition If A is a normal catenary domain, then ω, a finitely generated A-module, is called a **canonical module** for A if $\omega_{\mathfrak{p}}$ is a canonical module for $A_{\mathfrak{p}}$, for all $\mathfrak{p} \in \mathrm{Spec}(A)$.

Theorem 9.38 *If ω and ω' are two canonical modules for a normal catenary domain A, then there exists a projective module P of rank 1 over A such that*

$$\omega \otimes_A P \cong \omega'.$$

Proof Let $P = \mathrm{Hom}_A(\omega, \omega')$ and let $\psi : \omega \otimes P$ be given by $\psi(x \otimes f) = f(x)$. Localizing at $\mathfrak{p} \in \mathrm{Spec}(A)$, we have that $\mathrm{Hom}_A(\omega, \omega') \cong A_{\mathfrak{p}}$ and so $\psi_{\mathfrak{p}}$ is an isomorphism. Therefore ψ is an isomorphism. Since $P \cong A_{\mathfrak{p}}$ locally, P is a projective module. ■

Bibliography

[1] M.F. Atiyah and I.G. Macdonald. *Introduction to Commutative Algebra.* Addison-Wesley, 1969.

[2] N. Bourbaki. *Elements of Mathematics: Commutative Algebra Chapters 1-7.* Springer, 1972.

[3] W. Bruns, and J. Herzog, *Cohen-Macaulay Rings*, Cambridge Studies In Advances Mathematics, **39**, Cambridge University Press, Cambridge, 1993.

[4] H. Cartan and S. Eilenberg. *Homological Algebra.* Princeton Mathematics Series **19**, Princeton, 1956.

[5] D. Dummit, and R. Foote. *Abstract algebra, third edition.* John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[6] D. Eisenbud. *Commutative Algebra with a view toward Algebraic Geometry.* Graduate Texts in Mathematics **150**, Springer, 1995.

[7] T. Hungerford. *Algebra.* Graduate Texts in Mathematics **73**, Springer, 1984.

[8] H.C. Hutchins. *Examples of Commutative Rings.* Polygonal Publishing House, 1981.

[9] E. Kunz. *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, 1985.

[10] S. Lang. *Algebra.* Graduate Texts in Mathematics **211**, Springer, 2002.

[11] H. Matsumura. *Commutative Algebra.* Benjamin, 1980.

[12] ———. *Commutative Ring Theory.* Cambridge University Press, 2000.

[13] D. Mumford. *The Red Book of Varieties and Schemes.* Lecture Notes in Mathematics **1358**, Springer, 1999.

[14] M. Nagata. *Local Rings.* Interscience Tracts in Pure and Applied Mathematics **13**, J. Wiley, 1962.

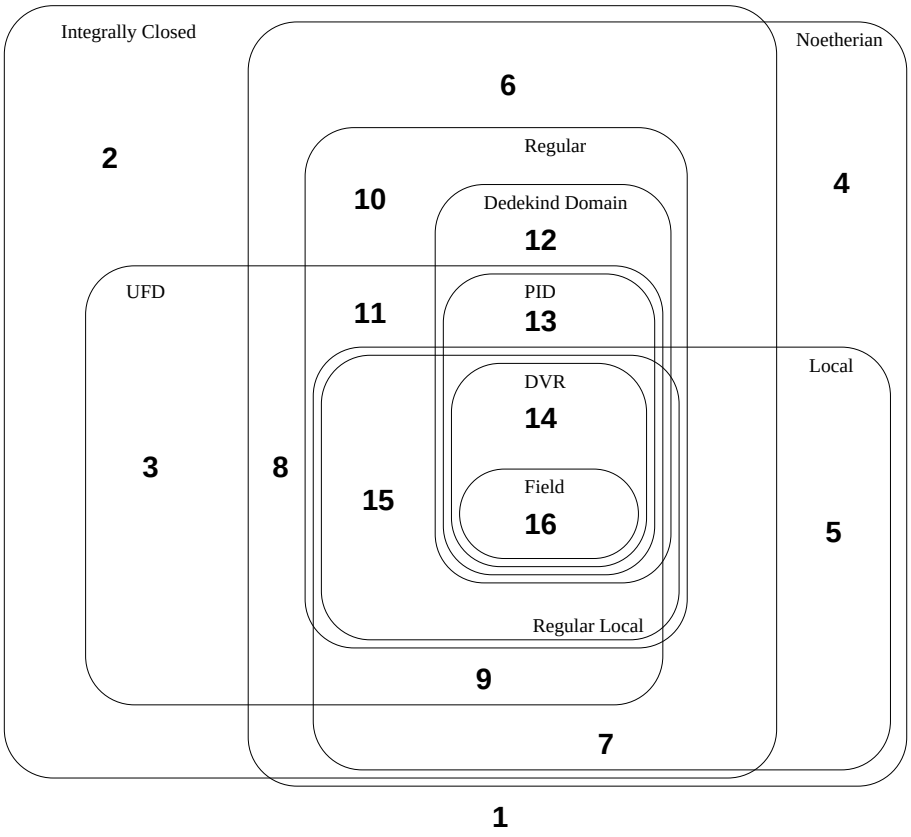
[15] J.-P. Serre. *Local Algebra.* Springer Monographs in Mathematics, Springer, 2000.

[16] O. Zariski and P. Samuel. *Commutative Algebra, Volumes I and II.* Van Nostrand (new edition Springer 1975), 1958–1960.

Appendix A

Diagram and Examples of Domains

All rings are assumed to be domains in the diagram below:



Examples:

(1) Not Noetherian, not integrally closed:

- $k[X^2, X^3, Y_1, Y_2, Y_3, \ldots]$

(2) Integrally closed, not a UFD, not Noetherian:

- $\mathbb{Z}[2X, 2X^2, 2X^3, \ldots]$
- $k[U, V, Y, Z, X_1, X_2, X_3, \ldots]/(UV - YZ)$

(3) A UFD but not Noetherian:

- $k[X_1, X_2, X_3, \ldots]$

(4) Noetherian, not local, not integrally closed:

- $k[X^2, X^3]$
- $\mathbb{Z}[\sqrt{5}]$

(5) Local, not integrally closed:

- $k[X^2, X^3]_{(X^2, X^3)}$
- $k[\![X^2, X^3]\!]$

(6) Noetherian, integrally closed, not regular, not a UFD, not local:

- $k[W, X, Y, Z]/(WX - YZ)$
- $\mathbb{R}[W, X, Y, Z]/(X^2 + Y^2 + Z^2 - W^2)$

(7) Local, integrally closed, not regular, not a UFD:

- $(k[W, X, Y, Z]/(WX - YZ))_{(W,X,Y,Z)}$
- $k[\![W, X, Y, Z]\!]/(WX - YZ)$

(8) Noetherian, a UFD, not regular, not local:

- $k[V, W, X, Y, Z]/(V^2 + W^2 + X^2 + Y^2 + Z^2)$
- $\mathbb{R}[W, X, Y, Z]/(W^2 + X^2 + Y^2 + Z^2)$

(9) Noetherian, a UFD, local, not regular:

- $(k[V, W, X, Y, Z]/(V^2 + W^2 + X^2 + Y^2 + Z^2))_{(V,W,X,Y,Z)}$

(10) Regular, not a Dedekind domain, not a UFD:

- $k[X, Y, Z]/(X^2 + Y^2 - 1)$

(11) A UFD, regular, not a Dedekind domain, not local:

- $k[X, Y]$, $\mathbb{Z}[X]$

(12) A Dedekind domain, not a UFD and hence not local:

- $\mathbb{Z}[\sqrt{-5}]$

(13) A PID but not local:

- $\mathbb{Z}$
- $k[X]$
- $\mathbb{Z}[i]$

(14) A DVR, not a field:

- $\mathbb{Z}_{(p)}$
- $k[X]_{(X)}$

(15) A Regular local ring, not a Dedekind domain:

- $k[\![X, Y]\!]$
- $k[X, Y]_{(X,Y)}$

(16) A field:

- $\mathbb{Q}$
- $\mathbb{R}$
- $\mathbb{C}$
- $\mathbb{Z}/p\mathbb{Z}$

Above k represents any field and $\mathfrak{m}$ represents any maximal ideal in the given ring. For further information on examples 2,6,8,9, see [8]. These four examples are all nontrivial.

Appendix B

Table of Invariances

The table below summarizes those basic properties of commutative rings that are and are not preserved under the basic operations on rings. For example, the symbol ✓ that appears in the upper left box means that if A is Noetherian, then $A[X]$ is Noetherian as well. An ✖ in the table merely means "not in general."

A	$A[X]$	$A[\![X]\!]$	$A/\mathfrak{a}$	$A/\mathfrak{p}$	$U^{-1}A$	$A_{\mathfrak{p}}$	$\widehat{A}$	$\widetilde{A}$
Noetherian	✓	✓	✓	✓	✓	✓	✓	✖
local	✖	✓	✓	✓	✖	✓	✓	✖
local and complete	✖	✓	✓	✓	✖	✖	✓	✓
normal domain	✓	✓	✖	✖	✓	✓	✖	✓
Dedekind domain	✖	✖	✖	✓	✓	✓	✖	✓
UFD	✓	✖	✖	✖	✓	✓	✖	✓
PID	✖	✖	✖	✓	✓	✓	✖	✓
regular local	✖	✓	✖	✖	✖	✓	✓	✓
DVR or a field	✖	✖	✖	✓	✓	✓	✓	✓

In the above table, $\widehat{A}$ denotes the completion of A with respect to some ideal I which is taken to be the unique maximal ideal if A is local. Local, as throughout these notes, is taken to mean Noetherian and local. For the third and fourth columns $\mathfrak{a}$ denotes an arbitrary ideal of A while $\mathfrak{p}$ denotes a prime ideal. Lastly, $\widetilde{A}$ denotes the integral closure of A, which is assumed to be a domain in this column.