Introduction to Commutative Algebra

April 8, 2008

About This Document

This document was typeset by Jason McCullough and Bart Snapp. It is a synthesis of class notes taken during a course taught by Professor S.P. Dutta at the University of Illinois Urbana-Champaign. Special thanks to: Michael Dewar, Dan Lior, and Patrick Szuta, for making many comments and corrections concerning these notes.

Please report corrections, suggestions, gripes, complaints, and criticisms to: `snapp@coastal.edu` (Bart Snapp) or `jmccullo@math.uiuc.edu` (Jason McCullough)

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 and B.

(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

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

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

Proposition 0.9 *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. ■

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

Example 0.11 *Consider $k[X, Y]$ where k is a field. Now $(X) \cup (Y)$ is not an ideal as it contains X, Y, but not $X + Y$.*

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

Lemma 0.12 (Prime Avoidance) *Let A be a ring and I be an ideal of A. If $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are prime ideals such that*

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

then

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

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 $\mathfrak{p}_i$.

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 0.13 (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 0.14 *$\mathbb{Z}$ is a Noetherian ring which is not an Artinian ring.*

Example 0.15 *If k is a field $k[x_1, \ldots, x_n, \ldots]$, is neither Artinian nor Noetherian.*

Example 0.16 *Any field is an Artinian ring.*

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

Example 0.17 *A finite Abelian group is a $\mathbb{Z}$-module which is both Noetherian and Artinian.*

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

Example 0.19 $A = k[x_1, \ldots, x_n, \ldots]$ *is a finitely generated* $k[x_1, \ldots, x_n, \ldots]$*-module which is not Noetherian.*

Example 0.20 $\mathbb{Z}_{p^\infty}$ *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, $M_i/M_{i+1} \simeq A/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ in A.

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

Definition The **length** of an A-module, denoted by $\ell_A(M)$, 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 $\ell_A(M) = n$.

Proposition 0.22 *M has finite length if and only if M is both Artinian and Noetherian.*

Proposition 0.23 *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.*

Proposition 0.24 *Given a short exact sequence of A-modules*

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

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

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

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

Theorem 0.25 (Hilbert's Basis Theorem) *If A is a Noetherian ring, then $A[x]$ is a Noetherian ring.*

Corollary 0.26

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

Lemma 0.28 *If A is a ring with an ideal I which is not prime, then there exist I_1 and I_2 each containing I such that $I \supseteq I_1 I_2$.*

Lemma 0.29 *If A is a Noetherian ring with an ideal I, I must contain a finite product of prime ideals.*

Lemma 0.30 *Every Artinian domain is a field.*

Theorem 0.31 *A ring A is Artinian if and only if A is Noetherian and every prime ideal is maximal.*

Proof See [17]. ■

Corollary 0.32 *If A is an Artinian ring, then A is Noetherian.*

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

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

Proposition 0.34 *If A and B are rings, with B an A-module, 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 linear combination of solutions in A.

Proposition 0.35 *Every free module is flat.*

Example 0.36 *$\mathbb{Q}$ is flat over $\mathbb{Z}$ but $\mathbb{Q}$ is not free over $\mathbb{Z}$.*

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 $U^{-1}M$.

WARNING 0.37 *The homomorphism $A \to U^{-1}A$ defined via $x \mapsto x/1$ is* ***not*** *generally injective, consider $A = \mathbb{Z}/6\mathbb{Z}$ and $U = \{1, 3\}$.*

Proposition 0.38 (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.*

$$\begin{tikzcd} A \arrow[r, "\eta"] \arrow[d, "\varphi"'] & U^{-1}A \arrow[dl, dashed, "\widetilde{\varphi}"] \\ B & \end{tikzcd}$$

Proposition 0.39 *If M is an A-module and U is a multiplicatively closed subset of A, then there is a canonical isomorphism $M \otimes_A U^{-1}A \simeq U^{-1}M$. Moreover, this isomorphism is functorial. That is, if $f : M \to N$, the following diagram commutes*

$$\begin{tikzcd} M \otimes_A U^{-1}A \arrow[r, "\eta_M"] \arrow[d, "f \otimes \mathbb{1}_{U^{-1}A}"'] & U^{-1}M \arrow[d, "U^{-1}f"] \\ N \otimes_A U^{-1}A \arrow[r, "\eta_N"'] & U^{-1}N \end{tikzcd}$$

where η_M and η_N represent the canonical isomorphisms.

Proposition 0.40 *$U^{-1}A$ is a flat A-module.*

As an immediate corollary we have:

Corollary 0.41 *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 0.42 *$A_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}$.*

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

(1) $M \neq 0$.

(2) $M_{\mathfrak{m}} \neq 0$ *for some maximal ideal* $\mathfrak{m}$ *of* A.

(3) $M_{\mathfrak{p}} \neq 0$ *for some prime ideal* $\mathfrak{p}$ *of* A.

Corollary 0.44 *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.

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 A-module M and M is $\mathfrak{p}$-coprimary, then N is also $\mathfrak{p}$-coprimary.*

Proof Exercise. ■

Proposition 1.3 *If an A-module M is $\mathfrak{p}$-coprimary, 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 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

$$A/I \hookrightarrow M.$$

Since $\mathfrak{p}x \subseteq \mathfrak{p}^l \subseteq I$, $\mathrm{Ann}_A(\overline{x}) = \mathfrak{p}$. Hence x has a nonzero image in $A/\mathfrak{p}$. 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 $ax \in \mathfrak{p}$ and thus $a \in \mathfrak{p}$. So

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

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 Exercise. ■

Definition Let A be a Noetherian ring. Given finitely generated A-modules $N \hookrightarrow M$, N is called **primary** (resp. **$\mathfrak{p}$-primary**) 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. Considering $xy \in I$ 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 $x^n \in I$.

($\Leftarrow$) Assuming whenever $xy \in I$ and $y \notin I$, we have $x^n \in I$ for some $n \in \mathbb{N}$ clearly forces the map

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

to be injective or nilpotent. ■

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

Proof This follows from Proposition 1.1 and the proof of the forward direction of Proposition 1.6. ∎

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 $A/\mathfrak{p} \simeq k[x,y,z]/(x,z) \simeq k[y]$, 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 $x \notin \mathfrak{p}^2$ and $y \notin \mathfrak{p}$, but $xy = z^2 \in \mathfrak{p}^2$. Thus the map $A/\mathfrak{p}^2 \xrightarrow{\overline{y}} A/\mathfrak{p}^2$ is nilpotent. 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. 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 $\varphi(\overline{m}) = a\overline{m}$.

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

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

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

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

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

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

Lemma 1.14 *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 $\operatorname{Ker}(\varphi) = N_1 \cap N_2$ 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 1.15 (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 1.14, 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

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

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:

$$\begin{tikzcd} M/N \arrow[r, hook, "\overline{\varphi}"] & \bigoplus_{i=1}^{n} M/N_i \arrow[d, "\pi_i"] \\ A/\mathfrak{p} \arrow[u, hook, "\iota"] \arrow[r, dashed, "\iota_i"] & M/N_i \end{tikzcd}$$

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 1.16 *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 whenever $\frac{a}{u} \in U^{-1}\mathfrak{p}$. 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 1.17 *If N is $\mathfrak{p}$-primary and $\mathfrak{p} \cap U = \varnothing$, then $U^{-1}N$ is $\mathfrak{p}$-primary.*

Theorem 1.18 *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* $m \leqslant n$ *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 1.16, 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 1.19 *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 1.18 and the above exercise, we know how to find a primary decomposition of any submodule of $U^{-1}M$.

Lemma 1.20 *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 1.16. ■

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

Proposition 1.21 *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 $\eta : M \to U^{-1}M$ be the canonical map. Take $U = A - \mathfrak{p}_i$. 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 1.16, $U^{-1}N_i = U^{-1}N_i'$. Therefore by Lemma 1.20,

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

■

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

Proposition 1.22 *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 1.22, $\eta^{-1}(\mathfrak{p}^n A_{\mathfrak{p}})$ 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 1.23 *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 Primary Decomposition and Polynomial Extensions

Definition For any module M we will write denote by $M[x]$ the $A[x]$-module $M \otimes_A A[x]$.

Proposition 1.24 *Let N be a proper submodule of M. Suppose N is $\mathfrak{p}$-coprimary. Then $N[x]$ is $\mathfrak{p}$-coprimary.*

Proof Let $f(x) = a_0 + a_1 x + \cdots + a_t x^t$. We wish to show that $N[x] \xrightarrow{f(x)} N[x]$ is nilpotent if $f(x) \in \mathfrak{p}[x]$ and injective otherwise. First suppose $f(x) \in \mathfrak{p}[x]$. Since N is $\mathfrak{p}$-coprimary, we can pick $n > 0$ such that the map $N \xrightarrow{a_i^n} N$ is the zero map for $i = 0, \dots, t$. Then for $m > tn$, $f(x)^m N[x] = 0$.

Now suppose $f(x) \notin \mathfrak{p}[x]$. We proceed with two cases.

Case 1. Suppose $a_0 \notin \mathfrak{p}$. Then $N \xrightarrow{a_0} N$ is injective. So for any nonzero element of $N[x]$

$$n(x) = n_0 + n_1 x + \cdots + n_s x^s$$

we may write

$$n(x) = n_i x^i + \cdots + n_s x^s$$

where $n_i \neq 0$ and $n_j = 0$ for $j < i$. Then

$$f(x)n(x) = f_0 n_i x^i + (\text{higher degree terms}) \neq 0.$$

So $N[x] \xrightarrow{f(x)} N[x]$ is injective.

Case 2. Suppose $a_0 \in \mathfrak{p}$. By assumption there is some $a_i \notin \mathfrak{p}$. So we may write

$$f(x) = g(x) + h(x)$$

where $g(x)$ and $h(x)$ are nonzero and such that all the coefficients of $g(x)$ are in $\mathfrak{p}$ and no coefficient of $h(x)$ is in $\mathfrak{p}$. Suppose there is some $n(x) \in N[x]$ such that $f(x)n(x) = 0$. Then $(g(x) + h(x))n(x) = 0$. Therefore $g(x)n(x) = -h(x)n(x)$. Similarly:

$$\begin{aligned} g(x)^2 n(x) &= g(x)(g(x)n(x)) \\ &= g(x)(-h(x)n(x)) \\ &= -h(x)(g(x)n(x)) \\ &= h(x)^2 n(x) \end{aligned}$$

Inductively, we get that $g(x)^m n(x) = (-1)^m h(x)^m n(x)$. Since $g(x) \in \mathfrak{p}[x]$, there is some $m > 0$ such that $g(x)^m n(x) = 0$. Since all coefficients of $h(x)$ lie outside

$\mathfrak{p}$, $(-1)^m h(x)^m n(x) \neq 0$ by Case 1. This is a contradiction. Thus $f(x)n(x) \neq 0$ and again $N[x] \xrightarrow{f(x)} N[x]$ is injective. ■

Corollary 1.25 *If N is $\mathfrak{p}$-primary, then $N[x]$ is $\mathfrak{p}[x]$-primary.*

Theorem 1.26 *Let A be a Noetherian ring, N be a proper submodule of a finitely generated A-module M, and*

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

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

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

is a primary decomposition of $N[x]$ where $N_i[x]$ is $\mathfrak{p}_i[x]$-primary.

Proof Note that if N_i is $\mathfrak{p}_i$-primary, then $N_i[x]$ is $\mathfrak{p}_i[x]$-primary by Corollary 1.25. Since $A[x]$ is a free A-module, $A[x]$ is a flat A module. Therefore $N[x] = N_1[x] \cap \cdots \cap N_n[x]$. ■

1.2.3 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 1.27 *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*

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

where x is a nonzero element of M which is killed by $\mathfrak{p}$. Note that any nonzero $x \in M$ 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,

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

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.

Exercise 1.30 *If $(A, \mathfrak{m}, k)$ is a local ring and x is a nonzerodivisor on $\mathfrak{m}$, then show there exists a short exact sequence:*

$$0 \to k \to \overline{\mathfrak{m}} \to \mathfrak{m}_{\overline{A}} \to 0$$

where $\overline{\mathfrak{m}} = \mathfrak{m}/x\mathfrak{m}$ and $\mathfrak{m}_{\overline{A}}$ is the maximal ideal of $\overline{A} = A/xA$.

Corollary 1.31 *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 $\mathfrak{p}_i$-primary 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

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

where x is a nonzero element of M that is killed by $\mathfrak{p}$. Since $0 + \mathfrak{p} = a + \mathfrak{p}$, and these elements map to 0 and ax respectively, we see that a is a zerodivisor on M and hence is an element of D. ■

Corollary 1.32 *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 1.33 *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 1.34 (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 $i = 1, \ldots, n$, $M_{i-1}/M_i \simeq A/\mathfrak{p}_i$ 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 $Q/M_0 \simeq T \simeq A/\mathfrak{p}'$, 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 1.32. ■

Proposition 1.35 *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 $M = (\alpha_1, \dots, \alpha_n)A$. Set $\varphi : A \to \bigoplus_{i=1}^n M$ defined by

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

It's easy to see that $I = \operatorname{Ker}(\varphi)$, and thus $A/\operatorname{Ker}(\varphi) \hookrightarrow \bigoplus_{i=1}^n M$. By Corollary 1.32, it follows that

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

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

Proposition 1.36 *Let A be a Noetherian ring and M be a finitely generated A-module. Define $N = \{a \in A : a^n M = 0$ for some $n > 0\}$. Then*

$$N = \bigcap_{\mathfrak{p} \in \operatorname{Ass}_A(M)} \mathfrak{p}.$$

Proof Exercise. ■

Proposition 1.37 *Let $\mathcal{P}$ be the collection of prime ideals of A that are minimal in $\operatorname{Ass}_A(A)$. Then*

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

Proof Exercise. ■

Proposition 1.38 *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) $\mathfrak{p} \supseteq \operatorname{Ann}_A(M)$.

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

Proof Exercise. ■

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

Corollary 1.39 *Let A be a Noetherian ring and M be a finitely generated A-module. The minimal elements of $\operatorname{Ass}_A(M)$ are the minimal elements of $\operatorname{Supp}_A(M)$.*

Exercise 1.40 *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

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

Proposition 1.41 *Let A be a Noetherian ring and M be a finitely generated A-module. M has finite length if and only if $\operatorname{Ass}_A(M)$ consists of maximal ideals only.*

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

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

Then for $i = 1, \ldots, n$, $M_i/M_{i+1} \simeq A/\mathfrak{m}_i$ 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 1.34, $\operatorname{Ass}_A(M) \subseteq \{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$.

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

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

Then for $i = 1, \ldots, n$, $M_i/M_{i+1} \simeq A/\mathfrak{p}_i$ 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

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

Since $(M_i)_{\mathfrak{p}}/(M_{i+1})_{\mathfrak{p}} \simeq (M_i/M_{i+1})_{\mathfrak{p}} \neq (0)$, 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 1.38, $\mathfrak{p} \supseteq \mathfrak{q}$ for some prime ideal $\mathfrak{q} \in \operatorname{Ass}_A(M)$. ∎

Corollary 1.42 (Finite Length Criteria) *Let $(A, \mathfrak{m})$ be a local ring and M a finitely generated A-module. Then the following are equivalent:*

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

(2) *M is Artinian and Noetherian.*

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

(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 assume 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 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 **$\mathfrak{p}$-primary** 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 1.43 *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

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

By Corollary 1.32

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

But by assumption, $\mathfrak{p} \notin \mathrm{Ass}(N(\mathfrak{p}))$ and as $M'/N(\mathfrak{p}) \simeq A/\mathfrak{q}$ 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

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

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

Exercise 1.44 *Let A be a Noetherian ring and*

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

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

Exercise 1.45 *Let $f : A \to B$ be a homomorphism of Noetherian rings. Let M be a finitely generated B-module. Show that*

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

Hence $\operatorname{Ass}_A(M)$ 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 $(\mathcal{I}, \leqslant)$ is a partially ordered set such that for every $\alpha, \beta \in \mathcal{I}$ there exists $\gamma \in \mathcal{I}$ with $\alpha \leqslant \gamma$ and $\beta \leqslant \gamma$.

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 $\alpha \leqslant \beta$ 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 $\alpha \leqslant \beta \leqslant \gamma$, the following diagram commutes:

$$\begin{tikzcd} X_\alpha \arrow[rr, "\varphi_{\alpha\beta}"] \arrow[dr, "\varphi_{\alpha\gamma}"'] & & X_\beta \arrow[dl, "\varphi_{\beta\gamma}"] \\ & X_\gamma & \end{tikzcd}$$

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 $\alpha \leqslant \beta$ 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 $\alpha \leqslant \beta$:

$$\begin{tikzcd}
Y & & \varinjlim(X_\alpha) \arrow[ll, dashed, "\varphi"'] \\
& X_\beta \arrow[ul, "\psi_\beta"] \arrow[ur, "\varphi_\beta"'] & \\
& X_\alpha \arrow[u, "\varphi_{\alpha\beta}"'] \arrow[uul, bend left, "\psi_\alpha"] \arrow[uur, bend right, "\varphi_\alpha"'] &
\end{tikzcd}$$

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* $(\psi_\alpha) : (B_\alpha) \to (C_\alpha)$ *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* $(M_u)_{u\in U}$ *for a direct system since for any* $u, u' \in U$, *we have inclusions* $M_u \hookrightarrow M_{uu'}$ *and* $M_{u'} \hookrightarrow M_{uu'}$. *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 $\alpha\leqslant\beta$ 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 $\alpha\leqslant\beta\leqslant\gamma$, the following diagram commutes:

$$\begin{tikzcd}
X_\beta \arrow[rr, "\varphi_{\alpha\beta}"] & & X_\alpha \\
& X_\gamma \arrow[ul, "\varphi_{\beta\gamma}"] \arrow[ur, "\varphi_{\alpha\gamma}"'] &
\end{tikzcd}$$

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 $\alpha\leqslant\beta$ 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 $\alpha\leqslant\beta$:

$$\begin{tikzcd}
Y \arrow[rr, dashed, "\varphi"] \arrow[dr, "\psi_\beta"] \arrow[ddr, bend right, "\psi_\alpha"'] & & \varprojlim(X_\alpha) \arrow[dl, "\varphi_\beta"'] \arrow[ddl, bend left, "\varphi_\alpha"] \\
& X_\beta \arrow[d, "\varphi_{\alpha\beta}"] & \\
& X_\alpha &
\end{tikzcd}$$

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*

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

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 $X_1, \dots, X_n$ over A by considering all infinite sums of the form

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

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 $A[\![X_1, \dots, X_n]\!]$.

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

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

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 $(\psi_\alpha) : (B_\alpha) \to (C_\alpha)$ 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.

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:

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

are both continuous maps.

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

$$\begin{aligned} A \times A &\to A \\ (a, b) &\mapsto a + b \end{aligned} \qquad\qquad \begin{aligned} A \times A &\to A \\ (a, b) &\mapsto ab \end{aligned} \qquad\qquad \begin{aligned} A &\to A \\ a &\mapsto a^{-1} \end{aligned}$$

are all 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 2.10 *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 2.11 *Show that the topology defined above makes M a topological module.*

Thus by Exercise 2.10, M is Hausdorff if and only if

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

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

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

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

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 a complete space is complete, $\prod_{n=0}^{\infty} M/M_n$ is complete under the product topology. Define

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

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

Exercise 2.12 *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 2.13 *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 2.14 *Let M be an 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 2.15 *If M is a filtered module with filtration (M_n), show that*

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

Proposition 2.16 *If M is a filtered A-module with filtration (M_n), and $\widehat{M}$ is its completion, then*

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

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:

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

The second statement then follows easily. ■

Exercise 2.17 *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 2.18 *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:

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

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 2.19 *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 $\widehat{A} \simeq \widehat{A_{\mathfrak{m}}}$.*

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 2.20 *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 $\widehat{M}/\widehat{M}_n \simeq M/M_n$,

$$\operatorname{Gr}(\widehat{A}) \simeq \operatorname{Gr}(A),$$
$$\operatorname{Gr}(\widehat{M}) \simeq \operatorname{Gr}(M).$$

Exercise 2.21 *Let A be a filtered ring that is Hausdorff under the given filtration. Show that if $\operatorname{Gr}(A)$ is an integral domain, then so is A.*

Proposition 2.22 *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

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

is exact.

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

So let $\overline{x} \in \operatorname{Ker}(\operatorname{Gr} g)$. 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 2.23 *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 $f_n : \underline{M_n/M_{n+1}} \to N_n/N_{n+1}$ 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 $y_{n+1} = y - f(\underline{x_n})$. 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 $(x_i)_{i \geqslant 0}$ 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 2.24 *Suppose A is complete, and M is a Hausdorff filtered A-module. Suppose further that* $\mathrm{Gr}(M)$ *is a finitely generated* $\mathrm{Gr}(A)$*-module. Let $x_1, \ldots, x_d$ be elements of M such that their images generate* $\mathrm{Gr}(M)$*. 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 $\mathrm{Gr}(M)$ over $\mathrm{Gr}(A)$. 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

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

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 2.25 *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 2.22. Since $\mathrm{Gr}(M)$ is Noetherian, $\mathrm{Gr}(N)$ is finitely generated. By the previous corollary, N is finitely generated. ■

Corollary 2.26 *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 2.24. ■

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

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

Exercise 2.28 *If p is a prime in $\mathbb{Z}$, show that the p-adic integers are:*

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

Exercise 2.29 *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 2.23 we have:

Corollary 2.30 *If A is a ring with a finitely generated ideal I such that:*

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

(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 2.24. ■

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

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

for all $n \geqslant 0$.

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 $n \geqslant 0$. Then we may write

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

where $\deg(a_i) = m + n - d_i \geqslant n$. 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 $N \cap I^{m+n}M \subseteq I^n(N \cap I^m M)$. ■

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 $i \geqslant 0$:

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

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

Definition If A is a ring we define the **Jacobson radical** to be

$$\mathfrak{J}(A) := \bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m}.$$

Exercise 2.32 *Show that $x \in \mathfrak{J}(A)$ if and only if $1 - ax$ is a unit for all $a \in A$.*

Exercise 2.33 *Show that if A is I-adically complete, then $I \subseteq \mathfrak{J}(A)$.*

Theorem 2.34 (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 $i = 1, \ldots, d$. Therefore

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

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 $i = 1, \ldots, d$. Observe that $\det(B) \in 1 - I$. Thus setting $a = 1 - \det(B)$ completes the proof. ■

Corollary 2.35 (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 2.34, 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 $M = 0$. ■

Corollary 2.36 *Let $(A, \mathfrak{m})$ be a quasilocal ring and M be a finitely generated A-module. If $M = \mathfrak{m}M$, then $M = 0$.*

Exercise 2.37 *Prove Krull's Intersection Theorem, Theorem 2.34, 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 2.38 *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.*

Corollary 2.39 *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 $\{\bar{b}_1, \ldots, \bar{b}_n\}$ of $M \otimes_A k$. We claim that $\{b_1, \ldots, b_n\}$ is a minimal set of generators for M. Write

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

Setting $\overline{M} = M / \sum_{i=1}^{n} b_i A$ we then have $\overline{M} = \mathfrak{m}\overline{M}$, and so by Corollary 2.35, Nakayama's Lemma, we see that $M = \sum_{i=1}^{n} b_i A$. To see that this is minimal, suppose that it is not, then we have $\sum_{i=1}^{n-1} c_i A = M$. But now $\{\bar{c}_1, \ldots, \bar{c}_{n-1}\}$ form a basis for $M \otimes_A k$, a contradiction as $M \otimes_A k$ is a free module of rank n. ■

Compare Corollary 2.39 with the following exercise:

Exercise 2.40 *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 2.24.*

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

Corollary 2.41 *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 2.31, 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 2.42 *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 2.34, 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 2.43 *Let A be a Noetherian ring and let $I \subsetneq J$ be two ideals of A. Suppose that A is J-adically complete. Show that A is also I-adically complete.*

Lemma 2.44 *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 2.31, $(I^n N)$ 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 2.22:

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

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 $(y_i)_{1 \leqslant i \leqslant n}$ 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

$$\begin{tikzcd}
0 \arrow[r] & N/N \cap I^{n+1} M \arrow[r, "f_{n+1}"] \arrow[d] & M/I^{n+1} M \arrow[r, "g_{n+1}"] \arrow[d, "\varphi"] & T/I^{n+1} T \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & N/N \cap I^n M \arrow[r, "f_n"] & M/I^n M \arrow[r, "g_n"] & T/I^n T \arrow[r] & 0.
\end{tikzcd}$$

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 $(y_n) \in \varprojlim M/I^nM$ that maps to (x_n) via g. ■

WARNING 2.45 *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 2.46 *If A is Noetherian with A-modules M and N, and I is an ideal of A, then*

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

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

Proof This follows from Lemma 2.44. ■

Proposition 2.47 *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*

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

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 tensor product and inverse limits we get that $\bigoplus_{i=1}^n \widehat{A} \simeq (\widehat{\bigoplus_{i=1}^n A})$. 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

$$\begin{tikzcd} A^s \otimes_A \widehat{A} \arrow[r] \arrow[d, "\varphi"] & A^r \otimes_A \widehat{A} \arrow[r] \arrow[d, "\psi"] & M \otimes_A \widehat{A} \arrow[r] \arrow[d, "\theta"] & 0 \\ \widehat{A^s} \arrow[r] & \widehat{A^r} \arrow[r] & \widehat{M} \arrow[r] & 0. \end{tikzcd}$$

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 2.44. Since φ and ψ are isomorphisms, θ is also an isomorphism by the Five Lemma. ■

Theorem 2.48 *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.

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

Corollary 2.49 *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 2.50 *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, $\widehat{J} \simeq J\widehat{A}$.*

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

(3) *The maximal ideals of A are in bijective correspondence with the maximal ideals of A that contain I. Further, if $\mathfrak{m}$ is a maximal ideal with $I \nsubseteq \mathfrak{m}$. 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 2.51 *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 $M/\mathfrak{m} \simeq M \otimes_A A/\mathfrak{m} \neq 0$. 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 $I = \operatorname{Ker}(\varphi)$. 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:

$$\begin{tikzcd} N' \arrow[rr, "g \circ f"] \arrow[dr, two heads, "\pi"'] & & N'' \\ & N/\operatorname{Ker}(g \circ f) \arrow[ur, hook, "\overline{g \circ f}"'] & \end{tikzcd}$$

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

$$\begin{tikzcd}
M \otimes_A N' \arrow[rr, "0"] \arrow[dr, two heads, "M\otimes_A \pi"'] & & M \otimes_A N'' \\
& M \otimes_A (N/\operatorname{Ker}(g \circ f)) \arrow[ur, hook, "\overline{M\otimes_A (g\circ f)}"'] &
\end{tikzcd}$$

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

$$\begin{tikzcd}
M \otimes_A \operatorname{Im}(f) \arrow[rr, hook, "\gamma"] \arrow[dr, hook, "\alpha"'] & & M \otimes_A \operatorname{Ker}(g) \arrow[dl, hook', "\beta"] \\
& M \otimes_A N &
\end{tikzcd}$$

In $M \otimes_A N$ we have then

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

Thus

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

is an exact sequence. Therefore so is

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

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

Example 2.52 *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 $N = 0$.

WARNING 2.53 *Recall that a module M is called* ***faithful*** *if*

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

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 $\operatorname{Ann}_{\mathbb{Z}}(\mathbb{Q}) = 0$ so $\mathbb{Q}$ is faithful, however*

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

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

Lemma 2.54 *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

$$\begin{tikzcd}
 & & & 0 \arrow[d] & \\
 & K \otimes_A M \arrow[r] \arrow[d] & K \otimes_A N \arrow[r] \arrow[d] & K \otimes_A P \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & F \otimes_A M \arrow[r] \arrow[d] & F \otimes_A N \arrow[r] \arrow[d] & F \otimes_A P \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & T \otimes_A M \arrow[r] \arrow[d] & T \otimes_A N \arrow[r] \arrow[d] & T \otimes_A P \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

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 2.55 *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*

$$M \to M \otimes_A B,$$
$$x \mapsto x \otimes 1,$$

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 2.51 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

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

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

$$\begin{tikzcd} A/I \simeq mA \arrow[r, hook, "\varphi"] \arrow[d, "\mathbb{1}_{A/I}\otimes_A B"'] \arrow[dr, "0"] & M \arrow[d, "\widetilde{f}"] \\ A/I \otimes_A B \arrow[r, hook, "\varphi\otimes_A \mathbb{1}_B"] & M \otimes_A B \end{tikzcd}$$

Since $f^{-1}(IB) = I$, we get that the map $\mathbb{1}_{A/I} \otimes_A B$ 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

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & M' \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & M'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M' \otimes_A B \arrow[r] \arrow[d] & M \otimes_A B \arrow[r] \arrow[d] & M'' \otimes_A B \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M' \otimes_A B/A \arrow[r] \arrow[d] & M \otimes_A B/A \arrow[r] \arrow[d] & M'' \otimes_A B/A \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

where all columns are exact (check it!) 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 assumption, 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 2.51 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. Thus if $M \otimes_A B = 0$ then $M = 0$. ∎

Theorem 2.56 *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 $\bigcap I^n M = 0$. So the I-adic topology on M is Hausdorff. Therefore $M \to \widehat{M}$ is injective. Since M is finitely generated, $\widehat{M} \simeq M \otimes_A \widehat{A}$. 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 2.57 *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 2.58 *If $f : A \to B$ is a local homomorphism of local rings, f is flat if and only if f is faithfully flat.*

Example 2.59 *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.

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.

Remark 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

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

Definition We denote by $B_k(x) : \mathbb{Z} \to \mathbb{Z}$ for $k \geqslant 0$ the 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 $B_k(x)$ is essentially polynomial for all $k \geqslant 0$. Also 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 $k > 1$.

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

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

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

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

(4) *$\Delta f(n)$ 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) 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 exercise,

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

where $a_0, \ldots, a_t \in \mathbb{Z}$. Let $Q(x) = \sum_{i=0}^{t} a_i B_{k+1}(n)$. 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) $\ell_{A_0}(M_n) < \infty$ *for all* $n \geqslant 0$.

(2) *Define the **Hilbert function** $\chi(M, n) := \ell_{A_0}(M_n)$. Then $\chi(M, n)$ is essentially polynomial of degree at most $r - 1$.*

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

$$\Delta^{r-1}\chi(M, n) \leqslant \ell_{A_0}(M_0)$$

with equality holding if and only if

$$\begin{aligned} \psi : M_0 \otimes_{A_0} A_0[X_1, \ldots, X_r] &\to M \\ m_0 \otimes aX_1^{i_1} \cdots X_r^{i_r} &\mapsto a \cdot x_1^{i_1} \cdots x_r^{i_r} \cdot m_0 \end{aligned}$$

is an isomorphism where the X_i's are indeterminates.

Proof We will show this in several parts:

(1) To show $\ell_{A_0}(M_n) < \infty$, 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 $\alpha_1, \ldots, \alpha_s$ generate M over A with each α_i homogeneous of degree d_i. Each element in M_n is then a sum of elements of the form

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

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) Proceeding 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 $\chi(M, n) = 0$ for n sufficiently large and we have that the degree of $\chi(M, n) = -1$.

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 $L = M/x_rM$. So both N and L are killed by x_r and hence are both graded modules over

$$\overline{A} = A_0[\mathbf{x}]/_r A_0[\mathbf{x}] = A/x_rA,$$

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

$$\ell_{A_0}(L_{n+1}) - \ell_{A_0}(M_{n+1}) + \ell_{A_0}(M_n) - \ell_{A_0}(N_n) = 0.$$

And so we see that

$$\ell_{A_0}(M_{n+1}) - \ell_{A_0}(M_n) = \ell_{A_0}(L_{n+1}) - \ell_{A_0}(N_n),$$

which shows us

$$\Delta\chi(M,n) = \chi(L,n+1) - \chi(N,n).$$

By the inductive hypothesis, the right-hand side is essentially polynomial of degree at most $r-2$. Thus $\Delta\chi(M,n)$ is essentially polynomial of degree at most $r-2$. By Lemma 3.2, we have the degree of $\chi(M,n)$ 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

$$\begin{aligned}\psi : M_0 \otimes_{A_0} A_0[X_1, \ldots, X_r] &\to M\\ m \otimes aX_1^{i_1} \cdots X_r^{i_r} &\mapsto m \cdot a \cdot x_1^{i_1} \cdots x_r^{i_r}.\end{aligned}$$

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

$$\begin{aligned}\ell_{A_0}(M_n) &\leqslant \ell_{A_0}(M_0 \otimes_{A_0} F_n)\\ &\leqslant \ell_{A_0}(M_0) \cdot N,\end{aligned}$$

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 $\chi(M,n)$ is essentially polynomial of degree at most $r-1$. So by $\chi(M,n)$ we shall instead now mean the polynomial equal to $\chi(M,n)$ for large n. Thus for n sufficiently large,

$$\chi(M,n) = \ell_{A_0}(M_n) \leqslant \ell_{A_0}(M_0)\cdot N = \ell_{A_0}(M_0)\cdot \frac{(n+r-1)!}{(r-1)!n!}$$

So we see that

$$\chi(M,n) \leqslant \ell_{A_0}(M_0)\cdot \frac{(n+r-1)!}{(r-1)!n!}$$

and so

$$(r-1)!\chi(M,n) \leqslant \ell_{A_0}(M_0)\cdot \frac{(n+r-1)!}{n!}.$$

Taking the limit as n goes to infinity of both sides, we get

$$\Delta^{r-1}\chi(M,n) \leqslant \ell_{A_0}(M_0).$$

Now if ψ as described above is an isomorphism it is clear that

$$\Delta^{r-1}\chi(M,n) = \ell_{A_0}(M_0).$$

($\Leftarrow$) Conversely, suppose that $\Delta^{r-1}\chi(M,n) = \ell_{A_0}(M_0)$. We will show that ψ as described above is an isomorphism. Proceed by induction on $\ell_{A_0}(M_0)$. Suppose that $\ell_{A_0}(M_0) = 1$ 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

$$\ell_{A_0}(k[\mathbf{X}]_n) = \ell_{A_0}(L_n) + \ell_{A_0}(M_n)$$

and so

$$\chi(k[\mathbf{X}],n) = \chi(L,n) + \chi(M,n).$$

¿From here we see

$$\Delta^{r-1}\chi(k[\mathbf{X}],n) = \Delta^{r-1}\chi(L,n) + \Delta^{r-1}\chi(M,n).$$

However, by (2) we see that $\Delta^{r-1}\chi(k[\mathbf{X}],n)$ and $\Delta^{r-1}\chi(M,n)$ are both of degree zero, and since $\ell_{A_0}(M_0) = 1$, we have that they are both 1. Thus

$$\Delta^{r-1}\chi(L,n) = 0$$

We claim that if $L \neq (0)$, then $\Delta^{r-1}\chi(L,n) > 0$. 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

$$\ell_{A_0}(L_n) \geqslant \ell_{A_0}((k[\mathbf{X}]f)_n).$$

Since $k[\mathbf{X}]$ is a domain, multiplication by f is injective. Therefore, $f \cdot k[\mathbf{X}] \simeq k[\mathbf{X}]$ as k-modules. Thus

$$\ell_{A_0}((k[\mathbf{X}]f)_n) = \ell_{A_0}(k[\mathbf{X}]_{n-d}) = \binom{n-d+r-1}{r-1}.$$

and so $\Delta^{r-1}\chi(L,n) > 0$.

Now suppose that $\ell_{A_0}(M_0) > 1$ and look at

$$0 \longrightarrow L \longrightarrow M_0[\mathbf{X}] \xrightarrow{\psi} M \longrightarrow 0$$

where $L = \operatorname{Ker}(M)$. So we need to show that $L = (0)$. Supposing $L \neq (0)$, we then have

$$\chi(M_0[\mathbf{X}],n) = \chi(L,n) + \chi(M,n),$$

and so

$$\Delta^{r-1}\chi(M_0[\mathbf{X}],n) = \Delta^{r-1}\chi(L,n) + \Delta^{r-1}\chi(M,n).$$

But $\Delta^{r-1}\chi(M_0[\mathbf{X}],n) = \ell_{A_0}(M_0) = \Delta^{r-1}\chi(M,n)$. Hence $\Delta^{r-1}\chi(L,n) = 0$. 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 $M_0^i/M_0^{i+1} \simeq A_0/\mathfrak{m}_i \simeq k_i$ 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 $- \otimes_{A_0} A_0[X_1,\dots,X_r]$ we obtain the exact sequence

$$0 \to M_0^{i+1}[\mathbf{X}] \to M_0^i[\mathbf{X}] \to k_i[\mathbf{X}] \to 0 \tag{$\bigstar$}$$

as $A_0[X_1,\dots,X_r]$ 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 $L \nsubseteq M_0^{i+1}[\mathbf{X}]$. 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

$$\chi(L_i,n) \leqslant \chi(L,n)$$
$$\Delta^{r-1}\chi(L_i,n) \leqslant \Delta^{r-1}\chi(L,n),$$

but by an argument similar to the one above we see that $\Delta^{r-1}\chi(L_i, n) > 0$ and hence that $\Delta^{r-1}\chi(L, n) > 0$. So we see that $L = 0$ and hence our map ψ is an isomorphism. ■

Definition The polynomial representative of the Hilbert function $\chi(M, n) = \ell_{A_0}(M_n)$ is called the **Hilbert polynomial** of M. We will abuse notation and simply denote this polynomial by $\chi(M, n)$.

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 $\ell_k(M_n) = \dim_k(M_n) < \infty$.

(2) The dimensions of the vector spaces M_i exhibit polynomial growth.

Definition If $\chi(M, n)$ is of degree d, then the **Hilbert multiplicity** of M is

$$e_n(M) := \Delta^d\chi(M, n) = d!\, a_d,$$

where $\chi(M, n) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$.

3.1.2 The Hilbert-Samuel Polynomial

As we have seen, if A is a graded ring and M is a finitely generated graded A-module, then we can define the Hilbert function $\chi(M, n)$ of M. In this section, we will investigate the Hilbert polynomial of a canonical grading that can be put on any Noetherian ring. We will call this polynomial the Hilbert-Samuel polynomial. However, before this can be done, we need more tools.

Lemma 3.4 *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 2.35, $M = 0$. 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 3.5 *If A is Noetherian and M, N are finitely generated A-modules, then*

$$\mathrm{Supp}(M \otimes_A N) = \mathrm{Supp}(M) \cap \mathrm{Supp}(N)$$

Proof ($\subseteq$) Suppose that $\mathfrak{p} \in \mathrm{Supp}(M \otimes_A N)$. Write

$$\begin{aligned} 0 \neq (M \otimes_A N)_{\mathfrak{p}} &\simeq M \otimes_A N \otimes_A A_{\mathfrak{p}} \\ &\simeq M \otimes_A N_p \\ &\simeq M \otimes_A A_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_p \\ &\simeq M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}}. \end{aligned}$$

This shows us that $M_{\mathfrak{p}} \neq (0)$ and that $N_{\mathfrak{p}} \neq (0)$.

($\supseteq$) If $\mathfrak{p} \in \mathrm{Supp}(M) \cap \mathrm{Supp}(N)$, $M_{\mathfrak{p}} \neq 0$ and $N_{\mathfrak{p}} \neq 0$ we see by Lemma 3.4 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 $\mathfrak{p} \in \mathrm{Supp}(M \otimes_A N)$. ■

Lemma 3.6 *Let A be a Noetherian ring and M a finitely generated A-module such that for some ideal $\mathfrak{a}$ of A, $\ell(M/\mathfrak{a}M) < \infty$. 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) $\ell(M/M_n) < \infty$.

(2) *If $N \hookrightarrow M$, then $\ell(N/\mathfrak{a}N) < \infty$.*

Proof (1) First note that $\ell(M/\mathfrak{a}M) < \infty$ if and only if $\mathrm{Supp}(M/\mathfrak{a}M)$ consists entirely of maximal ideals. Write

$$\mathrm{Supp}(M/\mathfrak{a}M) = \mathrm{Supp}(M \otimes_A A/\mathfrak{a}) = \mathrm{Supp}(M) \cap \mathrm{Supp}(A/\mathfrak{a}),$$

and

$$\mathrm{Supp}(M/\mathfrak{a}^n M) = \mathrm{Supp}(M \otimes_A A/\mathfrak{a}^n) = \mathrm{Supp}(M) \cap \mathrm{Supp}(A/\mathfrak{a}^n).$$

But $\mathrm{Supp}(A/\mathfrak{a}) = \mathrm{Supp}(A/\mathfrak{a}^n)$. Thus, $\ell(M/\mathfrak{a}^n M) < \infty$ for each n if and only if $\ell(M/\mathfrak{a}M) < \infty$. By construction we have the following exact sequence

$$M/\mathfrak{a}^n M \to M/M_n \to 0.$$

Hence $\ell(M/M_n) < \infty$ for all $n > 0$.

(2) Now if $N \hookrightarrow M$,

$$\mathrm{Supp}(N/\mathfrak{a}N) = \mathrm{Supp}(N) \cap \mathrm{Supp}(A/\mathfrak{a}) \subseteq \mathrm{Supp}(M) \cap \mathrm{Supp}(A/\mathfrak{a}).$$

But $\mathrm{Supp}(M) \cap \mathrm{Supp}(A/\mathfrak{a}) = \mathrm{Supp}(M/\mathfrak{a}M)$, hence $\mathrm{Supp}(N/\mathfrak{a}N)$ consists only of maximal ideals and we see that $\ell(N/\mathfrak{a}N) < \infty$. ■

Proposition 3.7 *Let A be Noetherian, M finitely generated with $\mathfrak{a}$ an ideal of A such that $\ell(M/\mathfrak{a}M) < \infty$. Let (M_i) be an $\mathfrak{a}$-good filtration of M. Then*

$$P((M_i), n) := \ell(M/M_n)$$

is essentially polynomial.

Proof Write

$$\Delta P((M_i), n) = P((M_i), n+1) - P((M_i), n) = \ell(M/M_{n+1}) - \ell(M/M_n).$$

Since length is additive, we see that the right-hand side is $\ell(M_n/M_{n+1})$ by looking a the exact sequence

$$0 \to M_n/M_{n+1} \to M/M_{n+1} \to M/M_n \to 0.$$

Now

$$\begin{aligned} \mathrm{Gr}(M) &= M/M_1 \oplus M_1/M_2 \oplus \cdots \oplus M_n/M_{n+1} \oplus \cdots, \\ \mathrm{Gr}_{\mathfrak{a}}(A) &= A/\mathfrak{a} \oplus \mathfrak{a}/\mathfrak{a}^2 \oplus \cdots \oplus \mathfrak{a}^n/\mathfrak{a}^{n+1} \oplus \cdots. \end{aligned}$$

Note that while $\mathrm{Gr}_{\mathfrak{a}}(A)$ 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 $\ell(M/\mathfrak{a}M) < \infty$. Hence

$$\begin{aligned} \mathrm{Supp}(M/\mathfrak{a}M) &= \mathrm{Supp}(M) \cap \mathrm{Supp}(A/\mathfrak{a}) \\ &= \mathrm{Supp}(A/\operatorname{Ann}(M)) \cap \mathrm{Supp}(A/\mathfrak{a}) \\ &= \mathrm{Supp}(A/\operatorname{Ann}(M) \otimes_A A/\mathfrak{a}) \\ &= \mathrm{Supp}(A/(\operatorname{Ann}(M) + \mathfrak{a})), \end{aligned}$$

and so we see $\ell(A/(\operatorname{Ann}(M)+\mathfrak{a})) < \infty$. 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

$$\mathrm{Gr}_{\mathfrak{b}}(B) = B/\mathfrak{b} \oplus \mathfrak{b}/\mathfrak{b}^2 \oplus \cdots \oplus \mathfrak{b}^n/\mathfrak{b}^{n+1} \oplus \cdots$$

is a graded ring over $B/\mathfrak{b}$ which is finitely generated 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 $\ell_A(M_n) = \ell_B(M_n)$. Hence by the Hilbert-Serre Theorem, Theorem 3.3, $\chi(E_0(M), n) = \ell(M_n/M_{n+1})$ 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 3.8 (Samuel) *If A is Noetherian, M is a finitely generated A-module, $\mathfrak{a}$ is an ideal of A such that $\ell(M/\mathfrak{a}M) < \infty$, and (M_i) is a filtration of M such that $\mathfrak{a}^n M \subseteq M_n$, then define*

$$P_{\mathfrak{a}}(M, n) := \ell(M/\mathfrak{a}^n M).$$

The following are true:

(1) $P_{\mathfrak{a}}(M, n) \geqslant P((M_i), n)$.

(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

$$\ell(M/\mathfrak{a}^n M) \geqslant \ell(M/M_n) \qquad (\bigstar)$$

and so by definition $P_{\mathfrak{a}}(M, n) \geqslant P_{\mathfrak{a}}((M_i), n)$.

Now for (2) we will start by defining

$$R(n) = \ell(M/\mathfrak{a}^n M) - \ell(M/M_n) = \ell(M_n/\mathfrak{a}^n M).$$

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 $\ell(M/\mathfrak{a}^{n+m} M) \geqslant \ell(M/M_{n+m})$. By $(\bigstar)$ we see that

$$P_{\mathfrak{a}}(M, n+m) \geqslant P_{\mathfrak{a}}((M_i), n+m) \geqslant P_{\mathfrak{a}}(M, n) \geqslant P_{\mathfrak{a}}((M_i), n)$$

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 $R(n) \geqslant 0$ 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 $\ell(M/\mathfrak{a}M) < \infty$, then $P_{\mathfrak{a}}(M, n)$ as defined above by

$$P_{\mathfrak{a}}(M, n) := \ell(M/\mathfrak{a}^n M).$$

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

$$d(M) := \deg(P_{\mathfrak{m}}(M, n)).$$

Corollary 3.9 *Properties of the Hilbert-Samuel polynomial $P_{\mathfrak{a}}(M, n)$:*

(1) $\deg(P_{\mathfrak{a}}(M, n)) \leqslant m$ *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*

$$\Delta^r P_{\mathfrak{a}}(M, n) \leqslant \ell(M/\mathfrak{a}M).$$

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 3.10 *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 $\ell(M/\mathfrak{a}M) < \infty$. 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 $\ell(M/\mathfrak{a}M) < \infty$, 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 2.31, (L_i) is $\mathfrak{a}$-good. Thus $\ell(M \mathfrak{a}^n M) = \ell(N/\mathfrak{a}^n N) + \ell(L/L \cap a^n M)$ and so

$$\begin{aligned} P_{\mathfrak{a}}(M, n) &= P_{\mathfrak{a}}(N, n) + P_{\mathfrak{a}}((L_i), n) \\ &= P_{\mathfrak{a}}(N, n) + P_{\mathfrak{a}}(L, n) - R(n), \end{aligned}$$

by the previous theorem. ■

Corollary 3.11 *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 $\ell(M/\mathfrak{m}M) < \infty$. Then

$$d(M) = \max\{d(L), d(N)\}.$$

Proposition 3.12 *Let A be Noetherian, M finitely generated, $\mathfrak{a}$ an ideal of A, and $\ell(M/\mathfrak{a}M) < \infty$. 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 $\operatorname{Ann}(M) + \mathfrak{a}$ and $\operatorname{Ann}(M) + \mathfrak{a}'$ are both finitely generated ideals show us that there exists m and m' greater than zero such that:

$$(\operatorname{Ann}(M) + \mathfrak{a}')^m \subseteq \operatorname{Ann}(M) + \mathfrak{a}$$
$$(\operatorname{Ann}(M) + \mathfrak{a})^{m'} \subseteq \operatorname{Ann}(M) + \mathfrak{a}'.$$

We leave it as an exercise to now check that:

$$\begin{aligned}\deg(P_{\mathfrak{a}}(M,n)) &= \deg(P_{(\operatorname{Ann}(M)+\mathfrak{a})}(A,n))\\ \deg(P_{(\operatorname{Ann}(M)+\mathfrak{a})}(A,n)) &= \deg(P_{(\operatorname{Ann}(M)+\mathfrak{a}')}(A,n))\\ \deg(P_{(\operatorname{Ann}(M)+\mathfrak{a}')}(A,n)) &= \deg(P_{\mathfrak{a}'}(M,n))\end{aligned}$$

With the three above equalities proved, the proposition is proved. ■

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 3.13 *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 $\ell(M/\mathfrak{a}M) < \infty$. Then

$$e_{\mathfrak{a}}(M,n) = e_{\mathfrak{a}}(L,n) + e_{\mathfrak{a}}(N,n).$$

Proof This follows from Proposition 3.10. ■

Proposition 3.14 *If A is Noetherian, M is a finitely generated with $\ell(M/\mathfrak{a}M) < \infty$ where $\mathfrak{a}$ is an ideal of A, and $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ 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 $\ell(A/\mathfrak{a}) < \infty$. Hence

$$\operatorname{Ass}_A(A/\mathfrak{q}) = \{\mathfrak{m}_1, \dots, \mathfrak{m}_r\}$$

is a set containing only maximal ideals. Now use the Primary Decomposition Theorem, Theorem 1.15, 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,

$$A/\mathfrak{a}^n \simeq A/\mathfrak{q}_1^n \oplus \cdots \oplus A/\mathfrak{q}_r^n.$$

Now apply $- \otimes_A M$ to obtain

$$M/\mathfrak{a}^n M \simeq M/\mathfrak{q}_1^n \oplus \cdots \oplus M/\mathfrak{q}_r^n \tag{$\bigstar$}$$

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

$$A/\mathfrak{q}_i \simeq A_{\mathfrak{m}_i}/\mathfrak{q}_i A_{\mathfrak{m}_i} = A_{\mathfrak{m}_i}/\mathfrak{a}_i.$$

Similarly we see that $A/\mathfrak{q}_i^n \simeq A_{\mathfrak{m}_i}/\mathfrak{a}_i^n$. Applying $- \otimes_A M$ we see that

$$M/\mathfrak{q}_i^n M \simeq M_{\mathfrak{m}_i}/\mathfrak{a}_i^n M_{\mathfrak{m}_i}$$

and so by ($\bigstar$) we obtain

$$M/\mathfrak{a}^n M \simeq \bigoplus_{i=1}^r M_{\mathfrak{m}_i}/\mathfrak{a}_i^n M_{\mathfrak{m}_i}.$$

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 $\ell(M/\mathfrak{a}M) < \infty$, so is the Hilbert-Samuel multiplicity of M with respect to $\mathfrak{a}$.

3.2 The Topological Approach

3.2.1 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 3.15 *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 3.16 *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 3.17 *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 3.16 every subset of X is Noetherian. Hence let

$$\mathcal{S} = \left\{ Y \subseteq X : \begin{array}{l} Y \text{ is closed in } X \text{ and for } Y \text{ the above} \\ \text{proposition does not hold} \end{array} \right\}.$$

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

$$\begin{aligned} Z_1 &= V_{1,1} \cup V_{1,2} \cup \cdots \cup V_{1,r}, \\ Z_2 &= V_{2,1} \cup V_{2,2} \cup \cdots \cup V_{2,s}, \end{aligned}$$

where each $V_{1,i}$ is a component of Z_1 and each $V_{2,i}$ is a component of Z_2. Hence

$$Y = V_{1,1} \cup \cdots \cup V_{1,r} \cup \cdots \cup V_{2,1} \cup \cdots \cup V_{2,s}.$$

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

$$\dim(X) := \sup \left\{ d : \begin{matrix} \text{there exists a chain } X_0 \supsetneq \cdots \supsetneq X_d \text{ of} \\ \text{length } d \text{ of irreducible closed subsets of } X, \end{matrix} \right\}.$$

Proposition 3.18 *If X is a Noetherian topological space,*

$$\dim(X) = \sup \dim(X_i)$$

where X_i is a component of X.

3.2.2 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 3.19

(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

$$V(\mathfrak{a}) := \{\mathfrak{p} \in \mathrm{Spec}(A) : \mathfrak{p} \supseteq \mathfrak{a}\}.$$

We define the Zariski topology on Spec(A) as follows: Define $V(\mathfrak{a})$ to be the closed sets of 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 Spec(A) are sets of the form

$$\operatorname{Spec}(A) - V(\mathfrak{a}) = \left\{ \mathfrak{p} \in \operatorname{Spec}(A) : \begin{array}{l} \mathfrak{p} \text{ does not contain the generators} \\ \text{of the ideal } \mathfrak{a} \end{array} \right\}$$

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, 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 Spec(A). This sort of point is everywhere dense and is called a **generic point**.

Definition Let f be any element of A. Define

$$D(f) := \operatorname{Spec}(A) - V(f) = \{\mathfrak{p} \in \operatorname{Spec}(A) : f \notin \mathfrak{p}\}.$$

Proposition 3.20 *$\{D(f) : f \in A\}$ form a basis of* Spec(A).

Proof First we need to check

$$\operatorname{Spec}(A) = \bigcup_{f \in A} D(f)$$

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 3.21 *Show that* $\operatorname{Spec}(\mathbb{C}[X]) = \overline{\{(0)\}}$.

Definition Let Z be any subset of Spec(A). Define

$$I(Z) := \bigcap_{\mathfrak{p} \in Z} \mathfrak{p}.$$

Proposition 3.22 *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 3.23 *If $Z_1 \subseteq Z_2$ are two closed subsets of* Spec(A)*, then*

$$I(Z_2) \subseteq I(Z_1).$$

Proof Exercise. ■

Proposition 3.24 *For any subset Z of* 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 Spec(A) and the radical ideals of A.

Proposition 3.25 *If Z is a closed subset of* 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, $I_1 \cdot I_2 \subseteq I(Z)$. Hence $Z \subseteq V(I_1 \cdot I_2) = V(I_1) \cup V(I_2)$. Thus $Z = V(I_1) \cup V(I_2)$ is not irreducible.

($\Leftarrow$) Now suppose that $I(Z)$ is prime. Since this is a point in the topological space Spec(A), it is irreducible. ■

Proposition 3.26 *If A is a Noetherian ring, then* Spec(A) *is a Noetherian topological space.*

Proof Suppose A is Noetherian, then by the Primary Decomposition Theorem, Theorem 1.15, we have

$$(0) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$$

where each $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary and so $V(\mathfrak{q}_i) = V(\mathfrak{p}_i)$. Eliminate those $V(\mathfrak{p}_i)$ for which p_i is not minimal in Ass(A). Then reindexing we have

$$\mathrm{Spec}(A) = V(0) = V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_s).$$

Since the $V(\mathfrak{p}_i)$ are the irreducible components of Spec(A) this proves the proposition. ■

WARNING 3.27 *The converse of the above proposition is* ***not*** *true. We leave it as an exercise to show that if k is a field, then*

$$A = \frac{k[X_1, \dots, X_n, \dots]}{(X_1^2, \dots, X_n^2, \dots)}$$

is not a Noetherian ring but $\operatorname{Spec}(A)$ *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 $\operatorname{Spec}(A)$. To be explicit:

$$\dim(A) = \sup\{d : \text{there exists } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d \text{ such that } \mathfrak{p}_i \in \operatorname{Spec}(A)\}.$$

This notion of dimension is often simply referred to as the **dimension** of a ring. If M is an A-module, then

$$\dim(M) := \dim(A/\operatorname{Ann}(M)).$$

Exercise 3.28 *Given a ring A and an A-module M, show that the dimension of M is the dimension of the topological space* $\operatorname{Supp}_A(M) \subseteq \operatorname{Spec}(A)$.

Example 3.29 *While*

$$\dim(A) = \sup\{d : \textit{there exists } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d \textit{ such that } \mathfrak{p}_i \in \operatorname{Spec}(A)\}.$$

Nagata gives an example of a ring A such that A is Noetherian but with infinite dimension in [14].

Example 3.30 *In the ring* $\mathbb{C}[X_1, \dots, X_n]$ *we have the chain of prime ideals*

$$(0) \subsetneq (X_1) \subsetneq \cdots \subsetneq (X_1, \dots, X_n).$$

Thus the dimension of $\mathbb{C}[X_1, \dots, X_n]$ *is at least n.*

Suppose that a ring A has finite dimension. If $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ are maximal prime ideals in $\operatorname{Spec}(A)$, 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 $\mathfrak{m} \in \operatorname{MaxSpec}(A)$.

(2) $\dim(A) = \sup \dim(A/\mathfrak{p})$ where $\mathfrak{p}$ is a minimal prime ideal of A.

3.3 Systems of Parameters and the Dimension Theorem

Recall that a local ring is a ring that is Noetherian with a unique maximal ideal.

Definition (Third Notion of Dimension) Let A be a local ring and M a finitely generated A-module. Define

$$s(M) := \inf \left\{ d : \begin{array}{l} \text{there exists } x_1, \ldots, x_d \in \mathfrak{m} \text{ such} \\ \text{that } \ell(M/(x_1, \ldots, x_d)M) < \infty \end{array} \right\}.$$

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 $s(M) = n$, then any sequence $x_1, \ldots, x_n$ such that

$$\ell(M/(x_1, \ldots, x_n)M) < \infty$$

is called a **system of parameters** of M.

Theorem 3.31 (The Dimension Theorem) *Let A be a local ring and M a finitely generated A-module. Then*

$$\dim(M) = d(M) = s(M).$$

Proof We will show $\dim(M) \leqslant d(M) \leqslant s(M) \leqslant \dim(M)$.

$\dim(M) \leqslant d(M)$ Proceeding by induction on $d(M)$. Suppose that $d(M) = 0$. Then

$$d(M) = P_{\mathfrak{m}}(M, n) = \ell(M/\mathfrak{m}^n M)$$

is constant for n sufficiently large. Thus for large enough n,

$$\ell(M/\mathfrak{m}^n M) = \ell(M/\mathfrak{m}^{n+1} M)$$

which shows us that $\ell(\mathfrak{m}^n M/\mathfrak{m}^{n+1} M) = 0$. 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 2.35, $\mathfrak{m}^n M = 0$ 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 $d(M) = n > 0$. Take any maximal chain

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m$$

in $\operatorname{Supp}(M)$. We need to show $m \leqslant n$. We know that $\mathfrak{p}_0$ is a minimal element of $\operatorname{Supp}(M)$ and hence is a minimal element in $\operatorname{Ass}_A(M)$. So we have an injection

$$A/\mathfrak{p}_0 \hookrightarrow M.$$

Set $N = A/\mathfrak{p}_0$. By Corollary 3.11, $d(N) \leqslant d(M)$. So it suffices to show that $m \leqslant d(N)$. 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 3.10, we have that

$$P_{\mathfrak{m}}(N,n) = P_{\mathfrak{m}}(N,n) + P_{\mathfrak{m}}(N/xN,n) - R(n),$$

where $\deg(R(n)) < \deg(P\mathfrak{m}(N,n)) = d(N)$. But then

$$P_{\mathfrak{m}}(N/xN,n) = R(n).$$

Thus $d(N/xN) = \deg(P_{\mathfrak{m}}(M,n)) = \deg(R(n)) < n$. By the inductive hypothesis, $\dim(N/xN) \leqslant d(N/xN)$. Since

$$\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m$$

is a strict chain of prime ideals in $\operatorname{Supp}(N/xN)$, we have that

$$m - 1 \leqslant \dim(N/xN) \leqslant d(N/xN) \leqslant n - 1.$$

Hence $\dim(M) = m \leqslant n = d(M)$.

$\boldsymbol{d(M) \leqslant s(M)}$ If $n = s(M)$, consider $x_1, \ldots, x_n$ a system of parameters for M. In this case we have by definition that

$$\ell_A(M/(x_1,\ldots,x_n)M) < \infty.$$

Consider $\mathfrak{a} = (x_1, \ldots, x_n)$. Now if we consider the image of $\mathfrak{a}$ in $M/\operatorname{Ann}_A(M)$, we have that

$$\overline{\mathfrak{a}} = (\overline{x}_1, \ldots, \overline{x}_n)$$

where $\overline{x}_i$ is the image of $x_i \in M/\operatorname{Ann}_A(M)$. By Proposition 3.12, $d(M)$ depends only on M and

$$\operatorname{Supp}(M/\mathfrak{m}M) = \operatorname{Supp}(M/\mathfrak{a}M),$$

and thus we see that

$$d(M) = \deg(P_{\mathfrak{m}}(M,n)) = \deg(P_{\mathfrak{a}}(M,n)) \leqslant n,$$

using that $\mathfrak{a}$ is generated by n elements and applying Corollary 3.9.

$\boldsymbol{s(M) \leqslant \dim(M)}$ Proceed by induction on $\dim(M)$. Write

$$\begin{aligned}\dim(M) = 0 &\Leftrightarrow \operatorname{Ass}_A(M) = \{\mathfrak{m}\},\\ &\Leftrightarrow \ell_A(M) < \infty,\end{aligned}$$

and so we see $s(M) = 0$.

Now assume that $\dim(M) = n$. Let $\mathfrak{p}_i$ be the minimal prime ideals in $\operatorname{Supp}(M)$. By Corollary 1.39, these primes are also minimal in $\operatorname{Ass}(M)$ so there are only finitely many such primes. By the Prime Avoidance Lemma, Lemma 0.12, 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, $s(M/xM) \leqslant \dim(M/xM)$. But $s(M) - 1 \leqslant s(M/xM)$ and so

$$s(m) \leqslant s(M/xM) + 1 \leqslant \dim(M/xM) + 1 \leqslant \dim(M).$$

Putting the above steps together we have shown

$$\dim(M) \leqslant d(M) \leqslant s(M) \leqslant \dim(M),$$

and hence $\dim(M) = d(M) = s(M)$. ■

Corollary 3.32 *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 $s(A) = \dim(A)$ is less than or equal to the number of generators of $\mathfrak{m}$. ■

Corollary 3.33 *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 2.16

$$M/\mathfrak{m}^n M \simeq \widehat{M}/\widehat{\mathfrak{m}^n}\widehat{M} \simeq \widehat{M}/\widehat{\mathfrak{m}}^n\widehat{M},$$

and so $P_{\mathfrak{m}}(M, n) = P_{\widehat{\mathfrak{m}}}(\widehat{M}, n)$. ■

Corollary 3.34 *If $(A, \mathfrak{m})$ is a local ring, then*

$$\dim(A) = \min\{i : (a_1, \ldots, a_i) = \mathfrak{a} \textit{ where } \mathfrak{a} \textit{ is } \mathfrak{m}\textit{-primary}\}.$$

Proof Let $\dim(A) = n$, then there exists $x_1, \ldots, x_n$ a system of parameters of A such that $\ell(A/\mathbf{x}) < \infty$. Thus $(x_1, \ldots, x_n)$ is $\mathfrak{m}$-primary. Since $s(A) = n$, we see that we cannot obtain $y_1, \ldots, y_t$ with $t < n$ such that $\ell(A/\mathbf{y}) < \infty$. So for any $y_1, \ldots, y_t$ with $t < n$, $(y_1, \ldots, y_t)$ is not $\mathfrak{m}$-primary. ■

Corollary 3.35 *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

$$\operatorname{ht}(\mathfrak{p}) = \sup \left\{ n : \begin{matrix} \text{there exists a chain of prime ideals} \\ \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{n-1} \subsetneq \mathfrak{p}_n = \mathfrak{p} \end{matrix} \right\}.$$

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

$$\begin{aligned} \operatorname{ht}(I) &= \inf\{\operatorname{ht}(\mathfrak{p}) : I \subseteq \mathfrak{p}\} \\ &= \inf\{\operatorname{ht}(\mathfrak{p}) : \mathfrak{p} \text{ is minimal in } \operatorname{Ass}_A(A/I)\}. \end{aligned}$$

Definition If A is a Noetherian ring and I is any ideal, then the **coheight**, denoted $\operatorname{coht}(I)$ is defined as

$$\operatorname{coht}(I) = \dim(A/I).$$

Exercise 3.36 *Check that for any ideal I, $\operatorname{ht}(I) + \dim(A/I) \leqslant \dim(A)$.*

WARNING 3.37 *Even if I is a prime ideal, the above inequality may be strict.*

Corollary 3.38 (Krull's Ideal Theorem) *Let A be a Noetherian ring and $\mathfrak{p}$ is a prime ideal. Then $\operatorname{ht}(\mathfrak{p}) \leqslant n$ 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 Since $\operatorname{ht}(\mathfrak{p}) = \dim(A_{\mathfrak{p}})$, $\dim(A_{\mathfrak{p}}) \leqslant n$ 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. 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 3.39 (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 3.38 the minimal prime containing (x) has height at most one. The prime $\mathfrak{p}$ containing (x) cannot have height zero, as then $\mathfrak{p} \in \operatorname{Ass}(A)$ by Corollary 1.39 and hence then every element of $\mathfrak{p}$ is a zero divisor, which is not the case. ■

Remark The above corollary to the Dimension Theorem is sometimes called **Krull's Hauptidealsatz**.

Corollary 3.40 *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 3.41 *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*

$$\dim(M/(x_1, \ldots, x_i)M) \geqslant \dim(M) - i.$$

Equality holds if and only if $x_1, \ldots, x_i$ form part of a system of parameters for M.

Exercise 3.42 *Let A be a Noetherian ring of dimension at least 2. Then A has infinitely many prime ideals of height 1.*

Example 3.43 *A ring A is Artinian if and only if $\dim(A) = 0$.*

Example 3.44 *A PID has dimension one.*

Example 3.45 $\dim(\mathbb{Z}) = 1$.

Example 3.46 *If k is a field, then $\dim(k[X]) = 1$.*

Example 3.47 *If k is a field, then $\dim(k[\![x]\!]) = 1$.*

Lemma 3.48 *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 $P_1 = \mathfrak{p}[X]$.

Proof Suppose not. Then

$$\mathfrak{p}[X] \subsetneq P_1 \subsetneq P_2$$

and so

$$(0) \subsetneq (P_1/\mathfrak{p})[X] \subsetneq (P_2/\mathfrak{p})[X]$$

in $(A/\mathfrak{p})[X]$. Set $U = A - \mathfrak{p}$. Since $P_1 \cap U = P_2 \cap U = \varnothing$, and since localizations are exact, we have

$$(0) \subsetneq U^{-1}(P_1/\mathfrak{p})[X] \subsetneq U^{-1}(P_2/\mathfrak{p})[X]$$

is a strict chain of prime ideals in $(A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p})[X] = U^{-1}(A/\mathfrak{p})[X]$. 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 3.49 *If A is Noetherian and I is an ideal of A, then*

$$\mathrm{ht}(I) = \mathrm{ht}(I \cdot A[X]).$$

Proof By the Primary Decomposition Theorem, Theorem 1.15,

$$\mathrm{Ass}\left(\frac{A[X]}{IA[X]}\right) = \{\mathfrak{p}_i[X] : \mathfrak{p}_i \in \mathrm{Ass}(A/I)\},$$

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

$$\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{p}[X]).$$

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 1.15, we see that $\mathfrak{p}[X] \supseteq (a_1, \ldots, a_n)[X]$ minimally. Thus $\mathrm{ht}(\mathfrak{p}[X]) \leqslant n$.

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

$$\mathfrak{p}_0[X] \subsetneq \mathfrak{p}_1[X] \subsetneq \cdots \subsetneq \mathfrak{p}_n[X] = \mathfrak{p}[X]$$

is a chain of prime ideals in $A[X]$. Thus $\mathrm{ht}(\mathfrak{p}[X]) \geqslant \mathrm{ht}(\mathfrak{p})$ and so we see that $\mathrm{ht}(\mathfrak{p}[X]) = \mathrm{ht}(\mathfrak{p})$. ■

Theorem 3.50 *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 $\mathfrak{p}_0 A[X] \subsetneq \cdots \subsetneq \mathfrak{p}_n A[X] \subsetneq \mathfrak{p}_n A[X] + xA[X]$ in $A[X]$. It is then clear that $\dim(A[X]) \geqslant \dim(A) + 1$, so it is enough to show $\dim(A[X]) \leqslant \dim(A) + 1$. 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 3.48, we have

$$\mathfrak{p}_0[x] = P_0 = P_1 = \cdots = P_{n-1} \subsetneq P_n.$$

Thus $n \leqslant 1$ and so we see that $\dim(A[X]) = 1$.

Now suppose that $\dim(A) = n > 0$ and let $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ be a strict chain of prime ideals in A. 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 $\dim(A_{\mathfrak{p}_{n-1}}[X]) = \dim(A_{\mathfrak{p}_{n-1}}) + 1 \leqslant \dim(A)$. In $A_{\mathfrak{p}_{n-1}}[X]$ we have a strict chain

$$P_0 A_{p_{n-1}} \subsetneq P_1 A_{p_{n-1}} \subsetneq \cdots \subsetneq P_{n-1} A_{p_{n-1}}$$

and thus

$$n - 1 \leqslant \dim(A_{\mathfrak{p}_{n-1}})[X] \leqslant \dim(A).$$

Thus $n \leqslant \dim(A) + 1$ and so $\dim(A[X]) = \dim(A) + 1$.

Case 2: Suppose that $\mathfrak{p}_{n-1} = \mathfrak{p}_n$. By Lemma 3.48, we have $P_{n-1} = \mathfrak{p}_{n-1}[X]$. By Lemma 3.49, we have $\mathrm{ht}(\mathfrak{p}_{n-1}[X]) = \mathrm{ht}(\mathfrak{p}_{n-1})$. Thus

$$\dim(A) \geqslant \mathrm{ht}(\mathfrak{p}_{n-1}) = \mathrm{ht}(P_{n-1}) \geqslant n - 1.$$

Thus $n \leqslant \dim(A) + 1$ and so we see that $\dim(A[X]) = \dim(A) + 1$. ■

Exercise 3.51 *If A is Noetherian, show that*

$$\dim(A[\![X]\!]) = \dim(A) + 1$$

Hint: Does every maximal ideal in $A[\![X]\!]$ contain X?

Corollary 3.52 *We have that if k is a field, then*

$$\begin{aligned}
\dim(k[X_1, \ldots, X_n]) &= \dim(k[\![X_1, \ldots, X_n]\!]) = n, \\
\dim(\mathbb{Z}[X_1, \ldots, X_n]) &= \dim(\mathbb{Z}[\![X_1, \ldots, X_n]\!]) = n + 1, \\
\dim(\mathbb{Z}_{(p)}[X_1, \ldots, X_n]) &= \dim(\mathbb{Z}_{(p)}[\![X_1, \ldots, X_n]\!]) = n + 1.
\end{aligned}$$

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, then C is faithful as an $A[b]$-module and C is finitely generated over A.

(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 $A[x]$-module, $\det(X) \in \operatorname{Ann}_{A[b]}(C) = 0$. 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, $\mathbb{Z}[X]/(X^2+1) \simeq \mathbb{Z}[i]$ 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 Clear from the proposition above. ■

Definition Let $A \subseteq B$ be commutative rings. Let

$$B' = \{b \in B : b \text{ is integral over } A\}.$$

Then B' is a subring of B called the **integral closure** of A in B. If $B' = A$ we say A is **integrally closed** in B. By the above proposition, B' 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 $\operatorname{Frac}(A)$. We denote the integral closure of A by $\widetilde{A}$ and when $A = \widetilde{A}$, we say that A is **integrally closed**.

Exercise 4.4 *If A is a UFD, then A is integrally closed.*

Exercise 4.5 *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 4.6 *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 4.7 *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 $\mathfrak{m} \in \operatorname{MaxSpec}(A)$. Note that for every maximal ideal $\mathfrak{m}$, $A \subseteq A_\mathfrak{m} \subseteq K$ where $K = \operatorname{Frac}(A)$. 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 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 4.8 *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 4.9 *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 4.8. ■

Proposition 4.10 *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

$$x(x^{n-1} + \cdots + a_1) = -a_0.$$

We must have $a_0 \neq 0$, for otherwise, using that x is a nonzerodivisor we have that $x^{n-1} + \cdots + a_1 = 0$, which is an integral dependence of smaller degree. Therefore $0 \neq a_0 \in xB \cap A$. ■

Proposition 4.11 *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 4.12 *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 such that $\mathfrak{p}B \subseteq Q \subseteq P$. Then

$$\begin{aligned} \mathfrak{p}B \cap A &= P \cap A \\ &= Q \cap A \\ &= \mathfrak{p}. \end{aligned}$$

By the previous proposition $Q = P$. ■

Proposition 4.13 *Suppose $A \subseteq B$ is an integral extension and suppose*

$$P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_n$$

is a strict chain of prime ideals in B. Then

$$P_1 \cap A \subsetneq P_2 \cap A \subsetneq \cdots \subsetneq P_n \cap A$$

is a strict chain of prime ideals in A. In particular $\dim(B) \leqslant \dim(A)$.

Proof Follows from the previous proposition. ■

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 4.14 (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 4.9. 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 4.15 (Integral Extensions Preserve Dimension) *Suppose $A \hookrightarrow B$ 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 4.14 there is a prime ideal P_0 lying over $\mathfrak{p}_0$. By Theorem 4.14 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 $\dim(B) \geqslant \dim(A)$. But by Proposition 4.13, $\dim(B) \leqslant \dim(A)$. Therefore $\dim(B) = \dim(A)$. ■

Corollary 4.16 *Suppose $A \subseteq B$ is an integral extension. Let I be any ideal in B lying over an ideal $\mathfrak{a}$ in A. Then* $\mathrm{ht}(I) \leqslant \mathrm{ht}(\mathfrak{a})$.

Proof Take any minimal prime $\mathfrak{p} \supseteq \mathfrak{a}$ so that $\mathrm{ht}(\mathfrak{a}) = \mathrm{ht}(\mathfrak{p})$. By Theorem 4.14 there is a prime ideal P of B lying over $\mathfrak{p}$ such that $P \supseteq I$. By Proposition 4.13 it follows that $\mathrm{ht}(P) \leqslant \mathrm{ht}(\mathfrak{p})$. Thus

$$\mathrm{ht}(I) = \inf_{Q \supseteq I} \mathrm{ht}(Q) \leqslant \mathrm{ht}(P) \leqslant \mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{a}).$$

■

Exercise 4.17 *Suppose $f : A \to B$ is a ring map that makes B a faithfully flat A-module. Then f has the Going-Up Property.*

Exercise 4.18 *Suppose $f : A \to B$ is a ring homomorphism. Then the following hold:*

(1) *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.*

(2) $\operatorname{Spec}(A)$ *is compact.*

(3) *Suppose* f *has the Going-Up Property. Then* f^* *is a closed map.*

Proposition 4.19 *Suppose* A *is an integral domain,* $K = \operatorname{Frac}(A)$*,* 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* $\sigma \in \operatorname{Gal}_K(L)$ *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:

$$\begin{tikzcd} B \arrow[r, hook] & L \\ A \arrow[u, hook] \arrow[r, hook] & K \arrow[u, hook] \end{tikzcd}$$

Let $x \in L$. Since L is an algebraic extension of K, there is a relation of the form

$$x^n + \lambda_{n-1}x^{n-1} + \cdots + \lambda_n = 0,$$

where $\lambda_0, \ldots, \lambda_{n-1} \in K$. Since $K = \operatorname{Frac}(A)$, 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 $\sigma \in \operatorname{Gal}_K(L)$. 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, $\sigma(B) \subseteq B$. Applying σ^{-1} we see that $\sigma(B) = B$. 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 4.20 *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 4.21 *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 4.11, $P = \sigma_i(Q)$. Suppose $P \not\subseteq \sigma_i(Q)$ for any i. Then by prime avoidance, Lemma 0.12, $P \not\subseteq \bigcup_{i=1}^n \sigma_i(Q)$. 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 $(L_i, \sigma_i) \leqslant (L_j, \sigma_j)$ 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
$$(L_{i_1}, \sigma_{i_1}) \leqslant (L_{i_2}, \sigma_{i_2}) \leqslant \cdots$$
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 4.22 (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 4.21, 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 $P \cap A = (0)$. Let $U_1 = A - \{0\}$ 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 4.23 *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 4.24 *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 4.12.
($\Leftarrow$) 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 $Q \subsetneq P$ 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 4.25 *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 4.26 *Let A be Noetherian, B be a finitely generated A-algebra, and $f : A \hookrightarrow B$ be a ring homomorphism. If we suppose the Going-Down Property holds, then $f^* : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is an open map.*

Exercise 4.27 *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 4.28 *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 $A \simeq k[t^3, t^4, t^5]$ and that $k[t^3, t^4, t^5] \hookrightarrow k[t]$ is an integral extension. Since $\dim k[t] = 1$, $\dim A = 1$.

4.2 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 4.29 *$k[X_1, X_2, \ldots, X_n]$ and $k[[X_1, \ldots, X_n]]$ are normal domains.*

Definition A local PID is called a **discrete valuation ring**, often denoted **DVR**.

Example 4.30 *$\mathbb{Z}_{(p)}, k[[X]]$, and $k[X]_{(X)}$, where k is a field, are DVRs.*

Proposition 4.31 (Characterization of DVRs) *Let $(A, \mathfrak{m})$ be a local integral 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, $\mathfrak{m} \in \operatorname{Ass}_A(A/Ax)$.*

(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 local, 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. Since $\dim(A) = 1$, $\ell(A/xA) < \infty$. 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 $\mathfrak{m}yx^{-1} \subseteq A$ where $\mathfrak{m}yx^{-1}$ 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 $\mathfrak{m} = (x_1, \dots, x_n)$. 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 $i = 1, \dots, n$. 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 2.35, $\det(A) = 0$. 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) Exercise. ■

Theorem 4.32 (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 $\dim(A_Q) = \mathrm{ht}(Q) = 1$.

($\Leftarrow$) As a scholium to Proposition 4.7 we know that if $A = \bigcap_{\mathfrak{m} \in \mathrm{MaxSpec}(A)} A_\mathfrak{m}$ then A is integrally closed. 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 $z \in \bigcap_{\mathrm{ht}(P)=1} A_P$. 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 $x \in \mathfrak{q}_i A_{\mathfrak{p}_i}$ for all i. Thus $x \in yA$. So $\frac{x}{y} \in A$. Hence A is normal. ■

Example 4.33 *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 $\frac{\overline{y}}{\overline{x}}$ is integral over A but is not in A. To see this, note $\frac{\overline{y}}{\overline{x}} = (1+x)^{\frac{1}{2}}$ is an infinite series. It follows then that A is not normal.

Example 4.34 *Consider $A = k[x,y,z]/(xz - y^2, x^3 - yz, x^2y - z^2)$. Note $A \simeq k[t^3, t^4, t^5]$, and we have the nonsurjective 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 4.35 *$k[x_1, x_2, \ldots, x_n]$ is a UFD, and so it is normal.*

Example 4.36 *The ring $k[x,y,u,v]/(xy - uv)$ is not normal. This is hard to show. We will discuss this later.*

4.3 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.

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 $K = \mathrm{Frac}(A)$. An A-submodule M of K is called a **fractional ideal** of A if all elements of M have a common denominator; that is,

$$M \subseteq A \cdot \frac{1}{d} \qquad \text{for some } 0 \neq d \in A.$$

Theorem 4.37 *A is a Dedekind domain if and only if the set of fractional ideals form a group under multiplication.*

Definition A fractional ideal M of A is called **invertible** if there is a fractional ideal M^{-1} such that $MM^{-1} = A$.

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 4.38 *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 4.39 *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

$$\begin{aligned}x &= \sum_i m_i n_i x \\ &= \sum_i x_i a_i,\end{aligned}$$

where $a_i = n_i x \in A$. Thus M is finitely generated over A. ■

Proposition 4.40 *If a finite product of fractional ideals is invertible if and only if each fractional ideal in the product is invertible.*

Proof Exercise. ■

Proposition 4.41 *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 $\{P_1, \dots, P_n\}$. 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 4.42 *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 4.40. By Proposition 4.41 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 4.40. 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 4.40 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 $x \in I$, $x = \sum_{i=1}^{n} (x b_i) a_i$. So $a_1, \ldots, a_n$ generate I. Therefore every nonzero ideal is finitely generated and A is Noetherian. ■

Theorem 4.43 *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 4.44 *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 $v_{\mathfrak{p}}(M_1) \leqslant v_{\mathfrak{p}}(M_2)$ for all primes $\mathfrak{p}$.*

Proof Exercise. ■

Corollary 4.45 *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 $v_{\mathfrak{p}}(M_1) \geqslant 0$ for all primes $\mathfrak{p}$.*

Theorem 4.46 *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. As before we that all nonzero ideals of A are invertible and hence finitely generated. So A is Noetherian. Consider the family

$$\mathcal{F} = \{\text{ideals } \mathfrak{a} \subseteq A : \mathfrak{a} \text{ is not a product of primes.}\}.$$

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 Nakayama's Lemma, Corollary 2.35, 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 4.47 *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 4.43.

($\Leftarrow$) By the previous theorem every nonzero ideal is invertible. By Proposition 4.42 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 $K = \mathrm{Frac}(A)$. 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 $v_P(dx^t) \geqslant 0$ for all $t > 0$. By Proposition 4.44, $v_P((d)) + tv_P((x)) \geqslant 0$ for all $t > 0$. Thus $v_P((x)) \geqslant 0$ for all $P \in \mathrm{Spec}(A) - \{(0)\}$. Therefore $x \in A$. So A is integrally closed. ■

4.4 The Krull-Akizuki Theorem

Definition Given a domain A and an A-module M we define the **rank** of M, denote $\mathrm{rank}_A(M)$, to be the following vector space rank

$$\mathrm{rank}_A(M) := \{\mathrm{rank}_K(K \otimes_A M)\},$$

where $K = \mathrm{Frac}(A)$. If A is not a domain we define the rank of M to be

$$\mathrm{rank}_A(M) := \max\{\mathrm{rank}_{A/\mathfrak{p}}(M/\mathfrak{p}M) : \mathfrak{p} \text{ is a minimal prime of } A\}$$

Lemma 4.48 *Let A be a Noetherian domain with $\dim(A) \leqslant 1$ and M a torsion free module over A of rank $r < \infty$. Then for any nonzero $a \in A$,*

$$\ell(M/aM) \leqslant r \cdot \ell(A/aA).$$

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 $K = \mathrm{Frac}(A)$. 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

$$s\alpha_i = \sum_{i=1}^{r} \mu_{ij}\alpha_j \quad \text{for} \quad r < i \leqslant n.$$

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 $Q \simeq M/F$, we have $sQ = 0$. Thus Q is a finitely generated module over A/sA. Since $\dim(A/sA) = 0$, $\ell(Q) < \infty$. 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

$$\ell(M/a^nM) \leqslant \ell(F/a^nF) + \ell(Q/a^nQ).$$

Since $M/aM \simeq a^{n-1}M/a^nM$ and since M is torsion free, we have that $\ell(M/a^nM) = n\ell(M/aM)$. Similarly $\ell(F/a^nF) = n \cdot \ell(F/aF) = nr \cdot \ell(A/aA)$. Since $\ell(Q) < \infty$, we must have $\ell(Q/a^nQ) \leqslant \ell(Q)$. Thus for all n,

$$\begin{aligned}
\ell(M/aM) &= \frac{1}{n}\ell(M/a^nM) \\
&\leqslant \frac{1}{n}\ell(F/a^nF) + \frac{1}{n}\ell(Q/a^nQ) \\
&= r \cdot \ell(A/aA) + \frac{1}{n}\ell(Q).
\end{aligned}$$

Therefore

$$\ell(M/aM) \leqslant r \cdot \ell(A/aA).$$

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 $\ell(M/aM) > r \cdot \ell(A/aA)$. Then we may choose a finitely generated submodule $M' \subseteq M$ such that $\ell(M'/aM') > r\ell(A/aA)$. But then

$$\begin{aligned}\ell(M'/aM') &> r \cdot \ell(A/aA)\\ &\geqslant \operatorname{rank}_A(M') \cdot \ell(A/aA),\end{aligned}$$

a contradiction of the finitely generated case. ■

Theorem 4.49 (Krull-Akizuki) *Let A be a Noetherian domain,* $\dim(A) \leqslant 1$, $K = \operatorname{Frac}(A)$*, L/K a finite field extension, $A \subseteq B \subseteq L$, and B a subring of L. Then B is Noetherian and* $\dim(B) \leqslant 1$.

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 $A \subseteq B \subseteq K = \operatorname{Frac}(A)$. Thus $\operatorname{rank}_A(B) = 1$. So we may apply Lemma 4.48 to get that $\ell(B/aB) \leqslant \ell(A/aA) < \infty$ 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 $\ell_B(\mathfrak{b}/a_0B) \leqslant \ell_A(\mathfrak{b}/a_0B) \leqslant \ell_A(B/a_0B) < \infty$. Thus $\mathfrak{b}/a_0B$ 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 4.50 *Let A be a Noetherian domain with $\dim(A) \leqslant 1$. Then the integral closure of A is Noetherian.*

Remark Many extension 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 $\dim(A) \leqslant 1$, then B is not necessarily a finitely generated A-module.

(2) If $\dim(A) \geqslant 2$ and C is a ring such that $A \subseteq C \subseteq L$ then C is not necessarily Noetherian.

(3) If $\dim(A) \geqslant 3$ then B is not necessarily Noetherian.

See [14] for examples of these.

We include a couple of similar results:

Theorem 4.51 *Let A be a Noetherian domain with $\dim(A) \leqslant 2$. Then the integral closure of A is Noetherian.*

Proof See [14], Theorem 33.12. ∎

Theorem 4.52 *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 4.53 *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 [17]. ∎

Theorem 4.54 *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. ■

4.5 Noether's Normalization Lemma

Theorem 4.55 (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

$$I \cap B = (x_1, \ldots, x_{h(0)})$$

and

$$\eta^{-1}(\mathfrak{a}_i) \cap B = (x_1, \ldots, x_{h(i)}) \qquad \text{where for } i < j \qquad h(0) \leqslant h(i) \leqslant h(j).$$

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 $\dim(k[X_1, \ldots, X_n]) = \dim(C) = n$, $\operatorname{Ker}(\eta) = 0$, for otherwise $\dim(C) = \dim(k[X_1, \ldots, X_n]/\operatorname{Ker}(\eta)) < n$.

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, $\operatorname{ht}(\mathfrak{a}_1 \cap C) = \operatorname{ht}(\mathfrak{a}_1) = 1$. 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 $d \leqslant n$. 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

$$\mathfrak{a}_i \cap C = (x_1, \ldots, x_{h(i)}) \qquad \text{with } h(i) \leqslant h(j) \text{ for } 1 \leqslant i \leqslant j \leqslant r-1.$$

Write $d = h(r-1)$. We may assume that $h(r-1) > 0$. Consider $\mathfrak{a} \cap k[x_{d+1}, \ldots, x_n]$ 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

$$\mathfrak{a} \cap k[t_{d+1}, \ldots, t_n] = (t_d, \ldots, t_{h(r)}) \qquad \text{where } h(r) \leqslant n.$$

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 4.56 *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 4.55, 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 $h(i) \leqslant h(j)$. 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 $\operatorname{tr}\deg_k(K) \leqslant n$. 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 4.57 *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 4.58 *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

$$\begin{array}{ll} \mathrm{P}_{k_0}^{\alpha_1}(X_1) & \text{where } k_0 = k, \\ \mathrm{P}_{k_1}^{\alpha_2}(X_2) & \text{where } k_1 = k[\alpha_1], \\ \vdots & \qquad\vdots \\ \mathrm{P}_{k_{n-1}}^{\alpha_n}(X_n) & \text{where } k_{n-1} = k[\alpha_1, \ldots, \alpha_{n-1}]. \end{array}$$

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

$$K := k[X_1, \ldots, X_n]/(f_1(X_1), f_2(X_1, X_2), \ldots, f_n(X_1, \ldots, X_n)) \simeq A/\mathfrak{m}.$$

Note that

$$\begin{aligned} K &= \frac{k[X_1, \ldots, X_n]}{(f_1(X_1), f_2(X_1, X_2), \ldots, f_n(X_1, \ldots, X_n))} \\ &\simeq \frac{k[\alpha_1, X_2, \ldots, X_n]}{(f_2(\alpha_1, X_2), \ldots, f_n(\alpha_1, X_2, \ldots, X_n))} \\ &\simeq \frac{k[\alpha_1, \alpha_2, \ldots, X_n]}{(f_3(\alpha_1, \alpha_2, X_3), \ldots, f_n(\alpha_1, \alpha_2, X_3, \ldots, X_n))} \\ &\vdots \\ &\simeq k[\alpha_1, \ldots, \alpha_n] \\ &\simeq A/\mathfrak{m}. \end{aligned}$$

So we are done. ■

Corollary 4.59 *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 4.60 *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 $k^n \simeq \mathrm{MaxSpec}(k[X_1, \ldots, X_n])$ is dense in $\mathrm{Spec}(k[X_1, \ldots, X_n])$.*

Corollary 4.61 *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 4.62 *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 4.63 *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 4.20. 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 4.54 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:

$$\begin{tikzcd}
& D \arrow[r] & \overline{L} & \\
C \arrow[ur] \arrow[rrr] & & & F=\overline{L}^G \arrow[ull] \\
& B \arrow[uu] \arrow[r] & L \arrow[uu] & \\
& A \arrow[u] \arrow[r] & K \arrow[u] & \\
& k[\mathbf{x}] \arrow[u] \arrow[r] \arrow[uuul] & E=k(\mathbf{x}) \arrow[u] \arrow[uuur] &
\end{tikzcd}$$

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:

$$\begin{tikzcd}
& C' \arrow[rr] & & F' \\
C \arrow[ur] \arrow[rr] & & F \arrow[ur] & \\
& k'[\mathbf{x}] \arrow[uu] \arrow[rr] & & E' \arrow[uu] \\
k[\mathbf{x}] \arrow[uu] \arrow[ur] \arrow[rr] & & E \arrow[uu] \arrow[ur] &
\end{tikzcd}$$

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 4.64 *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 4.65 *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 4.66 *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 4.67 *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 4.68 *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

$$\dim(A) = \boldsymbol{\mu}(\mathfrak{m}) := \{\text{the minimal number of generators of } \mathfrak{m}\}.$$

Example 5.1 *Let $A = k[X_1, \ldots, X_n]$. If*

$$\mathfrak{m} = (p_1(X_1), p_2(X_1, X_2), \ldots, p_n(X_1, \ldots, X_n)),$$

where $p_i(X_1, \ldots, X_i)$ is a polynomial in exactly i variables, then $\operatorname{ht}(\mathfrak{m}) = n$ and so $A_\mathfrak{m}$ is a regular local ring as

$$n = \operatorname{ht}(\mathfrak{m}) = \dim(A_\mathfrak{m}) = \boldsymbol{\mu}(\mathfrak{m}).$$

Now that we have a little background, consider this statement:

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.*

Before the advent of homological algebra, many books and papers went into proving this result, some taking up to 200 pages, even for the case of $A = \mathbb{C}[\![X_1, \ldots, X_n]\!]$. 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 $d_n \circ d_{n-1} = 0$ 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

$$H_n(X_\bullet) := \frac{\mathrm{Ker}(d_n)}{\mathrm{Im}(d_{n+1})}.$$

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:

$$\begin{tikzcd}
\cdots \arrow[r] & X_{n+1} \arrow[r, "d^X_{n+1}"] \arrow[d, "f_{n+1}"'] & X_n \arrow[r, "d^X_n"] \arrow[d, "f_n"'] & X_{n-1} \arrow[r] \arrow[d, "f_{n-1}"'] & \cdots \\
\cdots \arrow[r] & Y_{n+1} \arrow[r, "d^Y_{n+1}"'] & Y_n \arrow[r, "d^Y_n"'] & Y_{n-1} \arrow[r] & \cdots
\end{tikzcd}$$

Exercise 5.2 *Show that a map of complexes $f_\bullet : X_\bullet \to Y_\bullet$, defines a collection of homomorphisms:*

$$f_i : \mathrm{Ker}(d_i^X) \to \mathrm{Ker}(d_i^Y).$$
$$f_i : \mathrm{Im}(d_{i+1}^X) \to \mathrm{Im}(d_{i+1}^Y).$$
$$H_n(f_\bullet) : H_n(X_\bullet) \to H_n(Y_\bullet).$$

Definition Two maps of A-complexes

$$f_\bullet : X_\bullet \to Y_\bullet,$$
$$g_\bullet : X_\bullet \to Y_\bullet,$$

are called **homotopic** if there exist A-module maps $h_n : X_n \to Y_{n+1}$ such that in the diagram below

$$\begin{tikzcd}
\cdots \arrow[r] & X_{n+1} \arrow[r, "d_{n+1}^X"] \arrow[d, shift right, "f_{n+1}"'] \arrow[d, shift left, "g_{n+1}"] & X_n \arrow[r, "d_n^X"] \arrow[dl, "h_n"'] \arrow[d, shift right, "f_n"'] \arrow[d, shift left, "g_n"] & X_{n-1} \arrow[r] \arrow[dl, "h_{n-1}"'] \arrow[d, shift right, "f_{n-1}"'] \arrow[d, shift left, "g_{n-1}"] & \cdots \\
\cdots \arrow[r] & Y_{n+1} \arrow[r, "d_{n+1}^Y"'] & Y_n \arrow[r, "d_n^Y"'] & Y_{n-1} \arrow[r] & \cdots
\end{tikzcd}$$

we have

$$d_{n+1}^Y \circ h_n + h_{n-1} \circ d_n^X = f_n - g_n$$

for all $n \in \mathbb{Z}$. We denote this by $f_\bullet \sim g_\bullet$.

Exercise 5.3 *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 5.4 *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:

$$\begin{tikzcd}
\cdots \arrow[r] & H_{n+1}(X'_\bullet) \arrow[r, "H_{n+1}(f_\bullet)"] & H_{n+1}(X_\bullet) \arrow[r, "H_{n+1}(g_\bullet)"] & H_{n+1}(X''_\bullet) \arrow[dll, rounded corners, "\partial_{n+1}"] & \\
& H_n(X'_\bullet) \arrow[r, "H_n(f_\bullet)"] & H_n(X_\bullet) \arrow[r, "H_n(g_\bullet)"] & H_n(X''_\bullet) \arrow[dll, rounded corners, "\partial_n"] & \\
& H_{n-1}(X'_\bullet) \arrow[r, "H_{n-1}(f_\bullet)"] & H_{n-1}(X_\bullet) \arrow[r, "H_{n-1}(g_\bullet)"] & H_{n-1}(X''_\bullet) \arrow[r] & \cdots
\end{tikzcd}$$

Proof Consider the following commutative diagram with exact rows:

$$
\begin{tikzcd}
 & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\
0 \arrow[r] & X'_{n+1} \arrow[r, "f_{n+1}"] \arrow[d, "d'_{n+1}"] & X_{n+1} \arrow[r, "g_{n+1}"] \arrow[d, "d_{n+1}"] & X''_{n+1} \arrow[r] \arrow[d, "d''_{n+1}"] & 0 \\
0 \arrow[r] & X'_n \arrow[r, "f_n"] \arrow[d, "d'_n"] & X_n \arrow[r, "g_n"] \arrow[d, "d_n"] & X''_n \arrow[r] \arrow[d, "d''_n"] & 0 \\
0 \arrow[r] & X'_{n-1} \arrow[r, "f_{n-1}"] \arrow[d] & X_{n-1} \arrow[r, "g_{n-1}"] \arrow[d] & X''_{n-1} \arrow[r] \arrow[d] & 0 \\
 & \vdots & \vdots & \vdots &
\end{tikzcd}
$$

First we will show that

$$H_n(X'_\bullet) \xrightarrow{H_n(f_\bullet)} H_n(X_\bullet) \xrightarrow{H_n(g_\bullet)} H_n(X''_\bullet)$$

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 5.5 *Given a commutative diagram of complexes with short exact rows:*

$$\begin{tikzcd}
0 \arrow[r] & X'_\bullet \arrow[r] \arrow[d] & X_\bullet \arrow[r] \arrow[d] & X''_\bullet \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & Y'_\bullet \arrow[r] & Y_\bullet \arrow[r] & Y''_\bullet \arrow[r] & 0
\end{tikzcd}$$

we get a commutative diagram with long exact rows:

$$\begin{tikzcd}
\cdots \arrow[r] & H_{n+1}(X''_\bullet) \arrow[r] \arrow[d] & H_n(X'_\bullet) \arrow[r] \arrow[d] & H_n(X_\bullet) \arrow[r] \arrow[d] & H_n(X''_\bullet) \arrow[r] \arrow[d] & H_{n-1}(X'_\bullet) \arrow[r] \arrow[d] & \cdots \\
\cdots \arrow[r] & H_{n+1}(Y''_\bullet) \arrow[r] & H_n(Y'_\bullet) \arrow[r] & H_n(Y_\bullet) \arrow[r] & H_n(Y''_\bullet) \arrow[r] & H_{n-1}(Y'_\bullet) \arrow[r] & \cdots
\end{tikzcd}$$

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 5.6 *Show that the mapping cone of a map of complexes is a complex.*

Definition Given a complex $X_\bullet$, $X_\bullet(j)$ is used to denote a **shift**, where $X_i(j) := X_{i+j}$.

Exercise 5.7 *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:

$$\cdots \longrightarrow H_i(X_\bullet) \xrightarrow{H_i(f_\bullet)} H_i(Y_\bullet) \longrightarrow H_i(C_\bullet) \longrightarrow \cdots$$

Remark For more information on the mapping cone see [2, §2.6].

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:

$$\begin{tikzcd} & P \arrow[dl, dashed, "\widetilde{\varphi}"'] \arrow[d, "\varphi"] & \\ M \arrow[r, "\pi"'] & N \arrow[r] & 0 \end{tikzcd}$$

(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 $F \simeq P \oplus Q$ for some A-module Q.

Exercise 5.8 *Show that the conditions in the above definition are actually equivalent.*

Exercise 5.9 *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:

$$\begin{gathered} 0 \to S_1 \to F_0 \to M \to 0, \\ 0 \to S_{i+1} \to F_i \to S_i \to 0. \end{gathered}$$

Now we put the above short exact sequences together letting each S_i connect the short exact sequences:

$$\begin{tikzcd}
 & 0 \arrow[dr] & & 0 & & & & \\
 & & S_2 \arrow[ur] \arrow[dr] & & & & & \\
 & \cdots \arrow[rr, dashed, "d_2"] \arrow[ur] & & F_1 \arrow[rr, dashed, "d_1"] \arrow[dr] & & F_0 \arrow[r, "\pi"] & M \arrow[r] & 0 \\
 & & & & S_1 \arrow[ur] \arrow[dr] & & & \\
 & & & 0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

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 5.10 *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:

$$
\begin{tikzcd}
\cdots \arrow[r] & P_1 \arrow[r, "d_1^M"] & P_0 \arrow[r, "\pi_M"] & M \arrow[r] \arrow[d, "f"] & 0 \\
\cdots \arrow[r] & Q_1 \arrow[r, "d_1^N"] & Q_0 \arrow[r, "\pi_N"] & N \arrow[r] & 0
\end{tikzcd}
$$

Since P_0 is projective, we can obtain f_0 by:

$$
\begin{tikzcd}
& P_0 \arrow[dl, dashed, "f_0"'] \arrow[d, "f \circ \pi_M"] & \\
Q_0 \arrow[r, "\pi_N"'] & N \arrow[r] & 0
\end{tikzcd}
$$

Now since $S_1 = \mathrm{Ker}(\pi_N) = \mathrm{Im}(d_1^N)$, we can obtain f_1 by:

$$
\begin{tikzcd}
& P_1 \arrow[dl, dashed, "f_1"'] \arrow[d, "f_0 \circ d_1^M"] & \\
Q_1 \arrow[r, "d_1^N"'] & S_1 \arrow[r] & 0
\end{tikzcd}
$$

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 5.11 *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:

$$
\begin{tikzcd}
\cdots \arrow[r] & P_1 \arrow[r, "d_1^M"] \arrow[d, shift right, "f_1"'] \arrow[d, shift left, "g_1"] & P_0 \arrow[r, "\pi_M"] \arrow[d, shift right, "f_0"'] \arrow[d, shift left, "g_0"] & M \arrow[r] \arrow[d, "f"'] & 0 \\
\cdots \arrow[r] & Q_1 \arrow[r, "d_1^N"'] & Q_0 \arrow[r, "\pi_N"'] & N \arrow[r] & 0
\end{tikzcd}
$$

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

$$\begin{tikzcd} & P_0 \arrow[dl, dashed, "h_0"'] \arrow[d, "f_0 - g_0"] & \\ Q_1 \arrow[r, "d_1^N"'] & \mathrm{Im}(d_1^N) \arrow[r] & 0 \end{tikzcd}$$

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

$$\begin{tikzcd} & P_n \arrow[dl, dashed, "h_n"'] \arrow[d, "f_n - g_n - h_{n-1} \circ d_n^M"] & \\ Q_{n+1} \arrow[r, "d_{n+1}^N"'] & \mathrm{Im}(d_{n+1}^N) \arrow[r] & 0 \end{tikzcd}$$

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 5.12 (Horseshoe Lemma) *Let*

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

is an exact sequence of A-modules, and $P'_\bullet \to M'$ 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:

$$\begin{tikzcd}
0 \arrow[r] & P'_\bullet \arrow[r] \arrow[d] & P_\bullet \arrow[r] \arrow[d] & P''_\bullet \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M' \arrow[r] & M \arrow[r] & M'' \arrow[r] & 0
\end{tikzcd}$$

Proof Take projective resolutions $(P'_\bullet, \pi')$ and $(P''_\bullet, \pi'')$ of M' and M'' respectively and consider the following commutative diagram:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
\cdots \arrow[r] & P'_1 \arrow[r, "d'_1"] \arrow[d] & P'_0 \arrow[r, "\pi'"] \arrow[d] & M' \arrow[r] \arrow[d, "f"] & 0 \\
\cdots \arrow[r, dashed] & P'_1 \oplus P''_1 \arrow[r, dashed, "d_1"] \arrow[d] & P'_0 \oplus P''_0 \arrow[r, dashed, "\pi"] \arrow[d] & M \arrow[r] \arrow[d, "g"] & 0 \\
\cdots \arrow[r] & P''_1 \arrow[r, "d''_1"] \arrow[d] & P''_0 \arrow[r, "\pi''"] \arrow[d] \arrow[ur, dashed, "\eta_0"] & M'' \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

First we must define $\pi : P_0 \twoheadrightarrow M$ 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.

Now we will define d_1 and then complete the construction by induction. Since $\pi'' \circ d''_1 = 0$, we have that

$$\mathrm{Im}(\eta_0 \circ d''_1) \subseteq \mathrm{Ker}(g) = \mathrm{Im}(f).$$

Thus we have the commutative diagram:

$$\begin{tikzcd}
 & P''_1 \arrow[dl, dashed, "\eta_1"'] \arrow[d, "\eta_0 \circ d''_1"] & \\
P'_0 \arrow[r, "f \circ \pi'"] & \mathrm{Im}(f) \arrow[r] & 0
\end{tikzcd}$$

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:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
\cdots \arrow[r] & P_n' \arrow[r, "d_n'"] \arrow[d] & P_{n-1}' \arrow[r, "d_{n-1}'"] \arrow[d] & P_{n-2}' \arrow[r] \arrow[d] & \cdots \\
\cdots \arrow[r, dashed] & P_n' \oplus P_n'' \arrow[r, dashed, "d_n"] \arrow[d] & P_{n-1}' \oplus P_{n-1}'' \arrow[r, "d_{n-1}"] \arrow[d] & P_{n-2}' \oplus P_{n-2}'' \arrow[r] \arrow[d] & \cdots \\
\cdots \arrow[r] & P_n'' \arrow[r, "d_n''"] \arrow[d] & P_{n-1}'' \arrow[r, "d_{n-1}''"] \arrow[d] & P_{n-2}'' \arrow[r] \arrow[d] & \cdots \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

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 $\mathrm{Im}(\eta_{n-1} \circ d_n'') \in \mathrm{Ker}(d_{n-2}') = \mathrm{Im}(d_{n-1}')$. Again we are in the following situation:

$$\begin{tikzcd}
 & P_n'' \arrow[dl, dashed, "\eta_n"'] \arrow[d, "\eta_{n-1} \circ d_n''"] & \\
P_{n-1}' \arrow[r] & \mathrm{Im}(d_{n-1}') \arrow[r] & 0
\end{tikzcd}$$

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 5.13 *Show that given the following commutative diagram of A-modules with exact rows:*

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & M'' \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & N' \arrow[r] & N \arrow[r] & N'' \arrow[r] & 0 \end{tikzcd}$$

Then there exist associated projective resolutions that form a commutative diagram of A-complexes with exact rows:

$$\begin{tikzcd} 0 \arrow[r] & P'_\bullet \arrow[r] \arrow[d] & P_\bullet \arrow[r] \arrow[d] & P''_\bullet \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & Q'_\bullet \arrow[r] & Q_\bullet \arrow[r] & Q''_\bullet \arrow[r] & 0 \end{tikzcd}$$

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:

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "\iota"] \arrow[d, "\varphi"'] & M \arrow[dl, dashed, "\widetilde{\varphi}"] \\ & E & \end{tikzcd}$$

(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 5.14 *Show that the conditions in the above definition are actually equivalent.*

Theorem 5.15 (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:

$$\begin{tikzcd} 0 \arrow[r] & L \arrow[r] \arrow[d, "\varphi"'] & M \\ & E & \end{tikzcd}$$

Let L' be a submodule of M containing L and $\varphi' : L' \to E$ be a lift of φ. In this case, the ordering: $(L', \varphi') \leqslant (L'', \varphi'')$ 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 5.16 *Let A be a PID. An A-module is injective if and only if it is divisible.*

Example 5.17 *$\mathbb{Q}$ is an injective $\mathbb{Z}$-module as it is divisible. Moreover, $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module as well.*

Theorem 5.18 *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

$$Z/K \simeq M.$$

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

$$M \simeq Z/K \simeq \operatorname{Im}(\eta)/\operatorname{Im}(\eta|_K) \subseteq D.$$

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 $\mathrm{Hom}_{\mathbb{Z}}(A, -)$, we get an injective $\mathbb{Z}$-module homomorphism

$$\iota_* : \mathrm{Hom}_{\mathbb{Z}}(A, M) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(A, D),$$
$$\varphi \mapsto \iota \circ \varphi.$$

Noting that there is a canonical injection of A-modules

$$\mathrm{Hom}_A(A, M) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(A, M),$$

where the A-module structure on $\mathrm{Hom}_{\mathbb{Z}}(A, M)$ is given by

$$a \cdot f(x) := f(ax) \qquad \text{for } a \in A \text{ and } f \in \mathrm{Hom}_{\mathbb{Z}}(A, M),$$

we see that we have an embedding of A-modules

$$M \simeq \mathrm{Hom}_A(A, M) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(A, M) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(A, D).$$

Step 3. We will show that if D is a divisible $\mathbb{Z}$-module, then $\mathrm{Hom}_{\mathbb{Z}}(A, D)$ 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 5.15, we need to show that any A-module homomorphism

$$\psi : \mathfrak{a} \to \mathrm{Hom}_{\mathbb{Z}}(A, D), \qquad \text{extends to}$$
$$\Psi : A \to \mathrm{Hom}_{\mathbb{Z}}(A, D).$$

Now consider the $\mathbb{Z}$-module homomorphism:

$$\varphi : \mathfrak{a} \to D$$
$$a \mapsto \psi(a)(1_A)$$

One should check that this is indeed a $\mathbb{Z}$-module homomorphism. Since D is a divisible $\mathbb{Z}$-module, by Corollary 5.16, we see that it is an injective $\mathbb{Z}$-module, and so we write

$$\begin{tikzcd} 0 \arrow[r] & \mathfrak{a} \arrow[r, "\iota"] \arrow[d, "\varphi"'] & A \arrow[dl, dashed, "\widetilde{\varphi}"] \\ & D & \end{tikzcd}$$

and obtain a $\mathbb{Z}$-module homomorphism $\widetilde{\varphi}$ such that the diagram above commutes. Now define

$$\Psi : A \to \mathrm{Hom}_{\mathbb{Z}}(A, D),$$
$$a \mapsto f,$$

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 complex 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 5.18 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:

$$\begin{tikzcd}
 & & & & 0 \arrow[dr] & & 0 \\
 & & & & & C^2 \arrow[ur] \arrow[dr] & \\
0 \arrow[r] & M \arrow[r, "\iota"] & E^0 \arrow[rr, dashed, "d^1"] \arrow[dr] & & E^1 \arrow[rr, dashed, "d^2"] \arrow[ur] & & \cdots \\
 & & & C^1 \arrow[ur] \arrow[dr] & & & \\
 & & 0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

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 5.19 *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 5.20 (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:

$$\begin{tikzcd}
0 \arrow[r] & I_1^\bullet \arrow[r] & I_2^\bullet \arrow[r] & I_3^\bullet \arrow[r] & 0 \\
0 \arrow[r] & M_1 \arrow[r] \arrow[u] & M_2 \arrow[r] \arrow[u] & M_3 \arrow[r] \arrow[u] & 0
\end{tikzcd}$$

Exercise 5.21 *Show that given the following commutative diagram of A-modules with exact rows:*

$$\begin{tikzcd}
0 \arrow[r] & M_1 \arrow[r] \arrow[d] & M_2 \arrow[r] \arrow[d] & M_3 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & N_1 \arrow[r] & N_2 \arrow[r] & N_3 \arrow[r] & 0
\end{tikzcd}$$

Then there exist associated injective resolutions that form a commutative diagram of A-complexes with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & I_1^\bullet \arrow[r] \arrow[d] & I_2^\bullet \arrow[r] \arrow[d] & I_3^\bullet \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & J_1^\bullet \arrow[r] & J_2^\bullet \arrow[r] & J_3^\bullet \arrow[r] & 0
\end{tikzcd}$$

Exercise 5.22 *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

To start, let's recall some of Göthe's words:

Habe nun, ach! Philosophie,
Juristerei und Medizin,
Und leider auch Theologie!
Durchaus studiert, mit heissem Bemühn.
Da steh ich nun, ich armer Tor!
Und bin so klug als wie zuvor.
– Göthe, *Faust* act I, scene I

Construction of Tor

Definition Given a ring A and an A-module N, $\boldsymbol{\mathrm{Tor}_i^A(-, N)}$ 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:

$$\cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\pi} M \longrightarrow 0$$

Apply the functor $-\otimes_A N$ and chop off the $M \otimes_A N$ term 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

$$\mathrm{Tor}_0^A(M, N) \simeq M \otimes_A N.$$

Proposition 5.23 $\mathrm{Tor}_i^A(M, N)$ *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:

$$\begin{tikzcd}
\cdots \arrow[r] & P_i \arrow[r] \arrow[d, "\varphi_i"] & \cdots \arrow[r] & P_0 \arrow[r] \arrow[d, "\varphi_0"] & M \arrow[r] \arrow[d, "\mathbb{1}_M"] & 0 \\
\cdots \arrow[r] & Q_i \arrow[r] \arrow[d, "\psi_i"] & \cdots \arrow[r] & Q_0 \arrow[r] \arrow[d, "\psi_0"] & M \arrow[r] \arrow[d, "\mathbb{1}_M"] & 0 \\
\cdots \arrow[r] & P_i \arrow[r] & \cdots \arrow[r] & P_0 \arrow[r] & M \arrow[r] & 0
\end{tikzcd}$$

Note that the lifts $\varphi_\bullet$ and $\psi_\bullet$ of $\mathbb{1}_M$ are guaranteed to exist by Lemma 5.10. 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

$$H_i(P_\bullet \otimes_A N) \simeq H_i(Q_\bullet \otimes_A N).$$

Thus $\mathrm{Tor}_i^A(M,N)$ is well-defined. ■

Properties of Tor

Exercise 5.24 *If N is A-flat or if M is A-flat, show that*

$$\mathrm{Tor}_i^A(M,N) = 0$$

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 5.25 *Given an exact sequence of A-modules,*

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

we obtain a long exact sequence of Tor*'s:*

$$\begin{aligned}
\cdots &\longrightarrow \mathrm{Tor}_{n+1}^A(M',N) \longrightarrow \mathrm{Tor}_{n+1}^A(M,N) \longrightarrow \mathrm{Tor}_{n+1}^A(M'',N) \xrightarrow{\partial_{n+1}} \\
&\longrightarrow \mathrm{Tor}_{n}^A(M',N) \longrightarrow \mathrm{Tor}_{n}^A(M,N) \longrightarrow \mathrm{Tor}_{n}^A(M'',N) \xrightarrow{\partial_{n}} \\
&\longrightarrow \mathrm{Tor}_{n-1}^A(M',N) \longrightarrow \cdots\cdots\cdots\cdots \longrightarrow \mathrm{Tor}_{1}^A(M'',N) \xrightarrow{\partial_{1}} \\
&\longrightarrow M' \otimes_A N \longrightarrow M \otimes_A N \longrightarrow M'' \otimes_A N \longrightarrow 0
\end{aligned}$$

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, this complex is in fact split exact, and so 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 5.4, we obtain a long exact sequence of homologies, and hence the result. ■

Proposition 5.26 *Given a ring A and two A-modules M and N, we then have*

$$\mathrm{Tor}_i^A(M,N) \simeq \mathrm{Tor}_i^A(N,M).$$

Proof First note that

$$\mathrm{Tor}_0^A(M,N) \simeq M \otimes_A N \qquad \text{and} \qquad \mathrm{Tor}_0^A(N,M) \simeq N \otimes_A M.$$

Since

$$\begin{aligned} M \otimes_A N &\simeq N \otimes_A M \\ m \otimes n &\mapsto n \otimes m \end{aligned}$$

we have that $\mathrm{Tor}_0^A(M,N) \simeq \mathrm{Tor}_0^A(N,M)$. 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

$$\begin{aligned} \mathrm{Tor}_i^A(P,N) &= 0 \qquad\qquad \text{for } i > 0 \text{ and} \\ \mathrm{Tor}_i^A(N,P) &= 0 \qquad\qquad \text{for } i > 0. \end{aligned}$$

Hence by Proposition 5.25 we now have two long exact sequences of Tor's:

$$\begin{tikzcd} \cdots \arrow[r] & \mathrm{Tor}_{i+1}^A(S,N) \arrow[r] & 0 \arrow[r] & \mathrm{Tor}_{i+1}^A(M,N) \arrow[dlll, "\partial_{i+1}"] \\ & \mathrm{Tor}_i^A(S,N) \arrow[r] & 0 \arrow[r] & \mathrm{Tor}_i^A(M,N) \arrow[dlll, "\partial_i"] \\ & \mathrm{Tor}_{i-1}^A(S,N) \arrow[r] & 0 \arrow[r] & \mathrm{Tor}_{i-1}^A(M,N) \arrow[r] & \cdots \end{tikzcd}$$

And:

$$\begin{tikzcd} \cdots \arrow[r] & \mathrm{Tor}_{i+1}^A(N,S) \arrow[r] & 0 \arrow[r] & \mathrm{Tor}_{i+1}^A(N,M) \arrow[dlll, "\partial_{i+1}"] \\ & \mathrm{Tor}_i^A(N,S) \arrow[r] & 0 \arrow[r] & \mathrm{Tor}_i^A(N,M) \arrow[dlll, "\partial_i"] \\ & \mathrm{Tor}_{i-1}^A(N,S) \arrow[r] & 0 \arrow[r] & \mathrm{Tor}_{i-1}^A(N,M) \arrow[r] & \cdots \end{tikzcd}$$

Thus we see that

$$\begin{aligned} \mathrm{Tor}_i^A(M,N) &\simeq \mathrm{Tor}_{i-1}^A(S,N) \qquad\qquad \text{if } i > 1, \\ \mathrm{Tor}_i^A(N,M) &\simeq \mathrm{Tor}_{i-1}^A(N,S) \qquad\qquad \text{if } i > 1. \end{aligned}$$

We see now that it is enough to show that $\operatorname{Tor}_1^A(M,N) \simeq \operatorname{Tor}_1^A(N,M)$. Consider the commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Tor}_1^A(M,N) \arrow[r] & S \otimes_A N \arrow[r] \arrow[d, equal] & P \otimes_A N \arrow[r] \arrow[d, equal] & M \otimes_A N \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \operatorname{Tor}_1^A(N,M) \arrow[r] & N \otimes_A S \arrow[r] & N \otimes_A P \arrow[r] & N \otimes_A M \arrow[r] & 0
\end{tikzcd}$$

Note that the left-most terms are 0 because M and N are projective. And so we see that $\operatorname{Tor}_1^A(M,N) \simeq \operatorname{Tor}_1^A(N,M)$. ■

Proposition 5.27 *Given an exact sequence of A-modules,*

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

we obtain a long exact sequence of Tor*'s:*

$$\begin{tikzcd}
\cdots \arrow[r] & \operatorname{Tor}_{n+1}^A(M,N') \arrow[r] & \operatorname{Tor}_{n+1}^A(M,N) \arrow[r] & \operatorname{Tor}_{n+1}^A(M,N'') \arrow[dll, "\partial_{n+1}"] \\
& \operatorname{Tor}_{n}^A(M,N') \arrow[r] & \operatorname{Tor}_{n}^A(M,N) \arrow[r] & \operatorname{Tor}_{n}^A(M,N'') \arrow[dll, "\partial_{n}"] \\
& \operatorname{Tor}_{n-1}^A(M,N') \arrow[r] & \operatorname{Tor}_{n-1}^A(M,N) \arrow[r] & \operatorname{Tor}_{n-1}^A(M,N'') \arrow[r] & \cdots
\end{tikzcd}$$

Proof Note that this follows by Lemma 5.26 and Lemma 5.25. However, we can also give a direct proof. Let $Q_\bullet$ be a projective resolution of N. Since projective modules are flat, we have the short exact sequence of complexes:

$$0 \to M'_\bullet \otimes_A Q_\bullet \to M_\bullet \otimes_A Q_\bullet \to M''_\bullet \otimes_A N \to 0$$

By Lemma 5.4, we obtain a long exact sequence of homologies, and hence the result. ■

Exercise 5.28 $\operatorname{Tor}_i(M, \bigoplus_\alpha N_\alpha) \simeq \bigoplus_\alpha \operatorname{Tor}_i(M, N_\alpha)$.

Exercise 5.29 *Let B be a flat A-algebra. Then*

$$B \otimes_A \operatorname{Tor}_i^A(M,N) \simeq \operatorname{Tor}_i^B(M \otimes_A B, N \otimes_A B).$$

In particular, if U is a multiplicatively closed set in A, then

$$U^{-1} \operatorname{Tor}_i^A(M,N) \simeq \operatorname{Tor}_i^{U^{-1}}(U^{-1}M, U^{-1}N).$$

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:

$$\cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\pi} M \longrightarrow 0$$

Apply the functor $\mathrm{Hom}_A(-, N)$ and chop off the $\mathrm{Hom}_A(M, N)$ term 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

$$\mathrm{Ext}^0_A(M, N) = \frac{\mathrm{Ker}(d_1^*)}{0} \simeq \mathrm{Hom}_A(M, N).$$

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:

$$\begin{tikzcd}
\cdots \arrow[r] & P_i \arrow[r] \arrow[d, "\varphi_i"] & \cdots \arrow[r] & P_0 \arrow[r] \arrow[d, "\varphi_0"] & M \arrow[r] \arrow[d, "\mathbb{1}_M"] & 0 \\
\cdots \arrow[r] & Q_i \arrow[r] \arrow[d, "\psi_i"] & \cdots \arrow[r] & Q_0 \arrow[r] \arrow[d, "\psi_0"] & M \arrow[r] \arrow[d, "\mathbb{1}_M"] & 0 \\
\cdots \arrow[r] & P_i \arrow[r] & \cdots \arrow[r] & P_0 \arrow[r] & M \arrow[r] & 0
\end{tikzcd}$$

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

$$H^i(\mathrm{Hom}_A(P_\bullet, N)) \simeq H^i(\mathrm{Hom}_A(Q_\bullet, N)).$$

Thus $\mathrm{Ext}_i^A(M, N)$ is well-defined. ■

Second Construction

Definition Given a ring A and an A-module N, $\boldsymbol{\mathrm{Ext}^i_A(M, -)}$ 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

$$\mathrm{Ext}^0_A(M, N) = \frac{\mathrm{Ker}(d_*^0)}{0} \simeq \mathrm{Hom}_A(M, N).$$

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:

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] \arrow[d, "\mathbb{1}_N"] & I^0 \arrow[r] \arrow[d, "\varphi^0"] & \cdots \arrow[r] & I^i \arrow[r] \arrow[d, "\varphi^i"] & \cdots \\
0 \arrow[r] & N \arrow[r] \arrow[d, "\mathbb{1}_N"] & J^0 \arrow[r] \arrow[d, "\psi^0"] & \cdots \arrow[r] & J^i \arrow[r] \arrow[d, "\psi^i"] & \cdots \\
0 \arrow[r] & N \arrow[r] & I^0 \arrow[r] & \cdots \arrow[r] & I^i \arrow[r] & \cdots
\end{tikzcd}$$

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 $(-)^* = \operatorname{Hom}_A(M, -)$ 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

$$H^i(\operatorname{Hom}_A(M, I^\bullet)) \simeq H^i(\operatorname{Hom}_A(M, J^\bullet)).$$

Thus $\operatorname{Ext}_i^A(M, N)$ is well-defined. ■

Properties of Ext

Proposition 5.32 *The two constructions of* $\operatorname{Ext}^i_A(M, N)$ *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 $\operatorname{Hom}_A(P_\bullet, I^\bullet)$. We refer the reader to [16]. ■

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:*

$$\begin{array}{l}
0 \longrightarrow \operatorname{Hom}_A(M'', N) \longrightarrow \operatorname{Hom}_A(M, N) \longrightarrow \operatorname{Hom}_A(M', N) \xrightarrow{\partial_1} \\
\longrightarrow \operatorname{Ext}^1_A(M'', N) \longrightarrow \cdots\cdots\cdots\cdots \longrightarrow \operatorname{Ext}^{n-1}_A(M', N) \xrightarrow{\partial_{n-1}} \\
\longrightarrow \operatorname{Ext}^n_A(M'', N) \longrightarrow \operatorname{Ext}^n_A(M, N) \longrightarrow \operatorname{Ext}^n_A(M', N) \xrightarrow{\partial_n} \\
\longrightarrow \operatorname{Ext}^{n+1}_A(M'', N) \longrightarrow \operatorname{Ext}^{n+1}_A(M, N) \longrightarrow \operatorname{Ext}^{n+1}_A(M', N) \longrightarrow \cdots
\end{array}$$

Proof Let $P'_\bullet$, $P_\bullet$, and $P''_\bullet$ be projective resolutions of M', M, and M'' respectively. Hence we have an exact sequence of complexes:

$$0 \to P'_\bullet \to P_\bullet \to P''_\bullet \to 0$$

Since $P''_\bullet$ is projective, our complex is in fact split exact, and so we have following short exact sequence of complexes:

$$0 \to \operatorname{Hom}_A(P''_\bullet, N) \to \operatorname{Hom}_A(P_\bullet, N) \to \operatorname{Hom}_A(P'_\bullet, N) \to 0$$

By Lemma 5.4, 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:*

$$\begin{tikzcd}
\cdots \arrow[r] & \mathrm{Ext}_A^{n-1}(M,N') \arrow[r] & \mathrm{Ext}_A^{n-1}(M,N) \arrow[r] & \mathrm{Ext}_A^{n-1}(M,N'') \arrow[dll, "\partial_{n-1}"] \\
& \mathrm{Ext}_A^{n}(M,N') \arrow[r] & \mathrm{Ext}_A^{n}(M,N) \arrow[r] & \mathrm{Ext}_A^{n}(M,N'') \arrow[dll, "\partial_{n}"] \\
& \mathrm{Ext}_A^{n+1}(M,N') \arrow[r] & \mathrm{Ext}_A^{n+1}(M,N) \arrow[r] & \mathrm{Ext}_A^{n+1}(M,N'') \arrow[r] & \cdots
\end{tikzcd}$$

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 5.4, 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

$$0 \to \mathrm{Hom}_A(M,N') \to \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(M,N'') \to 0$$

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 5.15, 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) $\operatorname{Ext}^i_A(\bigoplus_\alpha M_\alpha,N)\simeq \prod_\alpha \operatorname{Ext}^i_A(M_\alpha,N)$.

(2) $\operatorname{Ext}^i_A(M,\prod_\alpha N_\alpha)\simeq \prod_\alpha \operatorname{Ext}^i_A(M,N_\alpha)$.

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*

$$B\otimes_A \operatorname{Ext}^i_A(M,N)\simeq \operatorname{Ext}^i_B(M\otimes_A B,N\otimes_A B).$$

If U *is a multiplicatively closed set in* A*,* A *is Noetherian and* M *is finitely generated, then*

$$U^{-1}\operatorname{Ext}^i_A(M,N)\simeq \operatorname{Ext}^i_{U^{-1}A}(U^{-1}M,U^{-1}N).$$

Hint: For help with this see [3, 6.7].

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:

$$\mathrm{pd}_A(M) := \inf\{n : \text{there exists a projective resolution of } M \text{ of length } n\}.$$

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) $\mathrm{pd}_A(M) \leqslant n$.

(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

$$\mathrm{Ext}^1_A(S_n,N) \simeq \mathrm{Ext}^2_A(S_{n-1},N) \simeq \cdots \simeq \mathrm{Ext}^n_A(S_1,N) \simeq \mathrm{Ext}^{n+1}_A(M,N) = 0.$$

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.

Proposition 5.42 *Consider an exact sequence of A-modules*

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

where P is projective. The following are true:

(1) *If M'' is projective, then so is M'.*

(2) *If $\mathrm{pd}_A(M'') \geqslant 1$, then $\mathrm{pd}_A(M'') = \mathrm{pd}_A(M') + 1$.*

Proof (1) If M'' is projective, then the above exact sequence is split, and so we have $P \simeq M' \oplus M''$. Since P is projective, it is a summand of a free module, and so we have

$$M' \oplus M'' \oplus Q \simeq F$$

showing that M' is also a summand of a free module and hence is also projective.

(2) For some A-module N, apply $\mathrm{Hom}_A(-, N)$ and look at the long exact sequence for Ext to see that

$$\mathrm{Ext}^i_A(M', N) \simeq \mathrm{Ext}^{i+1}_A(M'', N) \qquad \text{for } i \geqslant 1.$$

The result follows from Proposition 5.39. ■

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

$$P_\bullet: \qquad 0 \to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to M \to 0$$

We would be done if we knew that

$$P_\bullet \otimes_A A/xA: \qquad 0 \to P_n/xP_n \to \cdots \to P_0/xP_0 \to M/xM \to 0$$

was exact, by the above exercise.

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

$$\mathrm{Tor}_i^A(M, A/xA) = 0 \qquad \text{for } i \geqslant 2.$$

We must show that $\mathrm{Tor}_1^A(M, A/xA) = 0$. Applying $- \otimes_A M$ to ($\bigstar$) above we obtain

$$0 \longrightarrow \mathrm{Tor}_1^A(M, A/xA) \longrightarrow M \xrightarrow{x} M \longrightarrow M/xM \longrightarrow 0.$$

But we see that $\mathrm{Tor}_1^A(M, A/xA) = 0$ 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*

$$\mathrm{pd}_A(N) \leqslant \max\{\mathrm{pd}_A(M), \mathrm{pd}_A(T)\}.$$

Proof This follows easily from the Horseshoe Lemma. ■

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 5.46 *If A is a ring and N is an A-module, then the following are equivalent:*

(1) $\mathrm{id}_A(N) \leqslant n$.

(2) $\mathrm{Ext}_A^i(M, N) = 0$ *for all A-modules M and for all $i > n$.*

(3) $\mathrm{Ext}_A^{n+1}(M, N) = 0$ *for all A-modules M.*

(4) $\mathrm{Ext}_A^{n+1}(M, N) = 0$ *for all finitely generated A-modules M.*

(5) $\mathrm{Ext}_A^{n+1}(A/I, N) = 0$ *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 5.47 *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 5.48 *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.

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 5.46:

Corollary 5.49 *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 2.39 which states that if M is a finitely generated A-module, then

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

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 flat module or a projective module, you get a free module.

Theorem 5.50 *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) $\mathrm{Tor}^A_i(M,N) = 0$ *for all A-modules N and for all $i > 0$.*

(5) $\mathrm{Tor}^A_1(M,k) = 0$.

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 $\mathrm{Tor}_1^A(M,k) = 0$. However, since we map a basis of F onto a minimal set of generators of M, we see $F/\mathfrak{m}F \simeq M/\mathfrak{m}M$ and so $S/\mathfrak{m}S$ is 0. Hence by Corollary 2.35, Nakayama's Lemma, we see that $S = 0$ and so $M \simeq F$. ■

Proposition 5.51 *If $(A, \mathfrak{m}, k)$ is a local ring and M is a finitely generated A-module, then the following are equivalent:*

(1) $\mathrm{pd}_A(M) \leqslant n$.

(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 This proof is left as an exercise for the reader. Hint: See the proof of Proposition 5.39. ■

Later on we will be able to remove the condition that A is a local ring for the above proposition.

Corollary 5.52 *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 5.53 *If $(A, \mathfrak{m}, k)$ is a local ring, the following are equivalent:*

(1) $\mathrm{gd}(A) \leqslant n$.

(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 $\mathrm{pd}_A(k) \leqslant n$. So by Proposition 5.51, $\mathrm{Tor}_{n+1}^A(M,k) = 0$ 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 5.51 we have that $\mathrm{pd}_A(M) \leqslant n$ for all finitely generated A-modules M. Thus $\mathrm{gd}(A) \leqslant n$ by Corollary 5.49. ■

Corollary 5.54 (Main Point) *If $(A, \mathfrak{m}, k)$ is a local ring,*

$$\mathrm{gd}(A) = \mathrm{pd}_A(k).$$

There is an analogous result to Corollary 5.52 for injective dimension over local rings.

Theorem 5.55 *Let $(A, \mathfrak{m}, k)$ be a local ring and M a finitely generated A-module. Then*

$$\mathrm{id}_A(M) = \sup\{i : \mathrm{Ext}^i_A(k, M) \neq 0\}.$$

Proof We refer the reader to [4, Proposition 3.1.14]. ■

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 2.39, set

$$\begin{aligned} \beta_0 &:= \mathrm{rank}_k(M/\mathfrak{m}M), \\ S_1 &:= \mathrm{Ker}(A^{\beta_0} \to M), \end{aligned}$$

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

$$\begin{aligned} \beta_i &:= \mathrm{rank}_k(S_i/\mathfrak{m}S_i), \\ S_{i+1} &:= \mathrm{Ker}(A^{\beta_i} \to S_i), \end{aligned}$$

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:

$$\begin{aligned} 0 \to S_1 \to A^{\beta_0} \to M \to 0, \\ 0 \to S_{i+1} \to A^{\beta_i} \to S_i \to 0. \end{aligned}$$

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:

$$\begin{tikzcd}
0 \arrow[dr] & & 0 & & & & \\
& S_2 \arrow[ur] \arrow[dr] & & & & & \\
\cdots \arrow[ur] \arrow[rr, dashed, "d_2"] & & A^{\beta_1} \arrow[rr, dashed, "d_1"] \arrow[dr] & & A^{\beta_0} \arrow[r, "\pi"] & M \arrow[r] & 0 \\
& & & S_1 \arrow[ur] \arrow[dr] & & & \\
& & 0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

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 5.52, we see that the projective dimension of M is given by

$$\mathrm{pd}_A(M) = \sup\{n : \mathrm{Tor}_i^A(M,k) \neq 0\}.$$

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

$$\mathrm{Tor}_i^A(M,k) = \frac{\mathrm{Ker}(d_i \otimes 1)}{\mathrm{Im}(d_{i+1} \otimes 1)} = A^{\beta_i} \otimes_A k \simeq k^{\beta_i}.$$

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 $\mathrm{pd}_A(M)$. Hence a minimal free resolution is truly a resolution of minimal length.

Proposition 5.56 *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

$$F_0 \otimes_A k \simeq M \otimes_A k,$$
$$F_i \otimes_A k \simeq S_i \otimes_A k.$$

Thus by Corollary 2.39, 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. ■

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 5.57 *Examples of regular local rings:*

(1) *Consider* $A = k[\![X_1, \dots, X_n]\!]$ *where* k *is a field. Here* $\dim(A) = n$ *and* $\mathfrak{m} = (X_1, \dots, X_n)$. *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 5.58 *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 5.59 *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?

Theorem 5.60 *Let* $(A, \mathfrak{m}, k)$ *be local of dimension* n, *then the following are equivalent:*

(1) A *is regular.*

(2) $\operatorname{rank}_k(\mathfrak{m}/\mathfrak{m}^2) = n$.

(3)
$$k[X_1, \dots, X_n] \simeq \bigoplus_{i=0}^{\infty} \frac{\mathfrak{m}^i}{\mathfrak{m}^{i+1}} = \operatorname{Gr}_{\mathfrak{m}}(A).$$

Proof (1) $\Leftrightarrow$ (2) This follows from the definition of a regular local ring and Corollary 2.39.

(3) $\Rightarrow$ (2) If

$$k[X_1, \dots, X_n] \simeq \bigoplus_{i=0}^{\infty} \frac{\mathfrak{m}^i}{\mathfrak{m}^{i+1}},$$

then $\mathfrak{m}/\mathfrak{m}^2$ must correspond to degree 1 polynomials hence, $\mathfrak{m}/\mathfrak{m}^2$ is the k vector space generated by basis vectors $X_1, \dots, X_n$, showing that $\operatorname{rank}_k(\mathfrak{m}/\mathfrak{m}^2) = n$.

(1) $\Rightarrow$ (3) Consider the homomorphism

$$\varphi : k[X_1, \ldots, X_n] \to \mathrm{Gr}_{\mathfrak{m}}(A), \qquad \text{via}$$
$$\sum a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n} \mapsto \sum a_{i_1,\ldots,i_n} \overline{x}_1^{i_1} \cdots \overline{x}_n^{i_n},$$

where $(x_1, \ldots, x_n) = \mathfrak{m}$. Note that φ is onto. We must show that $\mathrm{Ker}(\varphi)$ is zero.

By Theorem 3.31, the Dimension Theorem, we have that

$$n = \dim(A) = \deg(P_{\mathfrak{m}}(A, i)) = \deg(\ell(A/\mathfrak{m}^i)).$$

Since

$$A \supseteq \mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \cdots \supseteq \mathfrak{m}^i$$

we have that

$$\ell(A/\mathfrak{m}^i) = \ell(A/\mathfrak{m}) + \ell(\mathfrak{m}/\mathfrak{m}^2) + \cdots + \ell(\mathfrak{m}^{i-1}/\mathfrak{m}^i).$$

Thus

$$\begin{aligned}\Delta P_{\mathfrak{m}}(A, i) &= \ell(A/\mathfrak{m}^{i+1}) - \ell(A/\mathfrak{m}^i) \\ &= \ell(\mathfrak{m}^i/\mathfrak{m}^{i+1}) \\ &= \chi(\mathrm{Gr}_{\mathfrak{m}}(A), i),\end{aligned}$$

and so $\deg(\chi(\mathrm{Gr}_{\mathfrak{m}}(A), i)) = n - 1$. Thus

$$0 = \Delta^{n-1}\chi(\mathrm{Gr}_{\mathfrak{m}}(A), i) = \ell_k(k).$$

Moreover, we have that k generates $\mathrm{Gr}_{\mathfrak{m}}(A)$ over $\mathrm{Gr}_{\mathfrak{m}}(A)$, and so by Theorem 3.3, the Hilbert-Serre Theorem, we see that the map above is injective. ■

Corollary 5.61 *If A is a regular local ring, then A is an integral domain.*

Proof To start, note that A is Hausdorff under the $\mathfrak{m}$-adic filtration and we have that $\mathrm{Gr}_{\mathfrak{m}}(A)$ is a domain. It is left as an exercise to show that this implies that A is a domain. ■

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 5.62 *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, $1 \leqslant i \leqslant j$, $A/(x_1, \ldots, x_i)$ 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 $\dim(A_i) \geqslant n - i$. 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 $\dim(A_i) \leqslant n - i$ 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. ∎

Corollary 5.63 *If A a regular local ring of dimension n and $x_1, \ldots, x_n$ is a regular system of parameters, then $(x_1, \ldots, x_i)$ is a prime ideal of height i.*

Proof Follows from Corollary 5.61 and Proposition 5.62. ∎

Definition Given a ring A and an A-module M, $x_1, \ldots, x_n \in A$ is called 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 $1 \leqslant i \leqslant n$.

Example 5.64 *If $A = k[X_1, \ldots, X_n]$, then $X_1, \ldots, X_n$ form an A-sequence.*

Exercise 5.65 *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 5.66 *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 3.40. ∎

Corollary 5.67 *If A is local and M is finitely generated A-module with $x_1, \ldots, x_i$ an M-sequence, then $i \leqslant \dim(M)$.*

It should be pointed out here that unless the ring is nice, the inequality above is strict.

Proposition 5.68 *$(A, \mathfrak{m})$ is a regular local ring if and only if $\mathfrak{m}$ is generated by an A-sequence.*

Proof ($\Rightarrow$) If A is a regular local ring with $\mathfrak{m} = (x_1, \ldots, x_n)$. Then by Corollary 5.61, we have that $A/(x_1, \ldots, x_i)$ is an integral domain, and so the map defined by x_{i+1} is an injection. Hence $(x_1, \ldots, x_n)$ form an A-sequence.

($\Leftarrow$) Suppose that $\mathfrak{m}$ is generated by an A-sequence $x_1, \ldots, x_d$. Then we see that $\dim(A) \leqslant d$, but from Corollary 5.67 we have that $\dim(A) \geqslant d$. Hence we see that A is a regular local ring. ■

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

$$\mathfrak{m}/a\mathfrak{m} \longrightarrow \mathfrak{m}/\mathfrak{m}^2 \xrightarrow{\varphi} A/\mathfrak{m} \xrightarrow{\simeq} aA/a\mathfrak{m}$$

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 5.54 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

$$\mathfrak{m}/a\mathfrak{m} \simeq A/\mathfrak{m} \bigoplus \mathfrak{m}/aA.$$

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 $i \geqslant 1$. 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 5.51. ■

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 2.35, 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 $i \geqslant 1$

$$\mathrm{Tor}_i^A(k, M) \simeq \mathrm{Tor}_{i+1}^A(A/xA, M).$$

However now we see by Proposition 5.51 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 5.68. 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 5.54, $\mathrm{gd}(A) = n$.

($\Leftarrow$) 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 2.35, 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 $\mathrm{rank}_k(\mathfrak{m}/\mathfrak{m}^2) = n+1$, 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, $\operatorname{gd}(A)$ is finite and hence $\operatorname{pd}_A(A/\mathfrak{p})$ 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 $\operatorname{pd}_{A_\mathfrak{p}}(A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p})$ is finite, and so $\operatorname{gd}(A_\mathfrak{p})$ is finite, and hence $A_\mathfrak{p}$ is a regular local ring. ∎

Theorem 5.76 (Auslander-Buchsbaum) *If A is regular local, then A is a UFD.*

Proof We omit the proof of this result and instead refer the reader to [6] or [12]. ∎

5.5.2 Regular Rings

Definition A Noetherian ring A is **regular** if $\operatorname{gd}(A)$ is finite.

Exercise 5.77 *If A is Noetherian and M is a finitely generated A-module, then show the following:*

(1) $\operatorname{pd}_A(M) = \sup\limits_{\mathfrak{m} \in \operatorname{MaxSpec}(A)} \operatorname{pd}_{A_\mathfrak{m}}(M_\mathfrak{m})$.

(2) *Suppose that* $\operatorname{pd}_{A_\mathfrak{m}}(M_\mathfrak{m})$ *is finite for all* $\mathfrak{m} \in \operatorname{MaxSpec}(A)$. *Then* $\operatorname{pd}_A(M)$ *is finite.*

Proposition 5.78 *If A is a Noetherian ring and M is a finitely generated A-module, then the following are equivalent:*

(1) $\operatorname{pd}_A(M) \leqslant n$.

(2) $\operatorname{Tor}_i^A(M, N) = 0$ *for all A-modules N and all $i > n$.*

(3) $\operatorname{Tor}_{n+1}^A(M, A/\mathfrak{m}) = 0$ *for all* $\mathfrak{m} \in \operatorname{MaxSpec}(A)$.

Proof Follows from the above exercise and Proposition 5.51. ∎

Proposition 5.79 *If A is Noetherian, the following are equivalent:*

(1) $\mathrm{gd}(A) \leqslant n$.

(2) *For all finitely generated A-modules M and N, $\mathrm{Tor}^A_{n+1}(M, N) = 0$.*

(3) *For all finitely generated A-modules M and all maximal ideals $\mathfrak{m} \subseteq A$, $\mathrm{Tor}^A_{n+1}(M, A/\mathfrak{m}) = 0$.*

(4) $\mathrm{Tor}^A_{n+1}(A/\mathfrak{m}, A/\mathfrak{m}) = 0$ *for all maximal ideals $\mathfrak{m} \subseteq A$.*

Proof Follows from the above exercise and Proposition 5.53. ∎

Corollary 5.80 *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 5.81 *If A is a regular ring, then $A_{\mathfrak{p}}$ is regular local for all $\mathfrak{p} \in \mathrm{Spec}(A)$.*

Exercise 5.82 *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 5.83 *If A is regular, then $A[x]$ is regular. Moreover*

$$\mathrm{gd}(A[x]) = \mathrm{gd}(A) + 1.$$

Example 5.84 *The following are examples of regular rings.*

(1) *If k is a field, then $k[X_1, \dots, X_n]$ is regular.*

(2) $\mathbb{Z}[X_1, \dots, X_n]$ *is regular.*

(3) *If A is a Dedekind domain, then $A[X_1, \dots, X_n]$ is regular.*

(4) *If k is a field, then $k[[X_1, \dots, X_n]][Y_1, \dots, Y_m]$ is regular.*

Appendix A

Diagram of Implications

$$
\begin{tikzcd}
 & \text{DVR} \arrow[dl, Rightarrow] \arrow[drr, Rightarrow] & & \\
\text{PID} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \text{UFD} \arrow[d, Rightarrow] & & \text{RLR} \arrow[ll, Rightarrow] \arrow[ddll, Rightarrow] \arrow[dd, Rightarrow] \\
\text{DD} \arrow[dr, Rightarrow] & \text{ND} & & \\
 & \text{RD} \arrow[u, Rightarrow] \arrow[d, Rightarrow] & & \text{LR} \arrow[ddl, Rightarrow] \\
 & \text{RR} \arrow[dr, Rightarrow] & & \\
 & & \text{NR} &
\end{tikzcd}
$$

In the diagram on the preceding page, the abbreviations are as follows:

DVR Discrete Valuation Ring

PID Principal Ideal Domain

DD Dedekind Domain

UFD Unique Factorization Domain

RLR Regular Local Ring

ND Normal Domain (Noetherian Integrally Closed Domain)

RD Regular Domain

RR Regular Ring

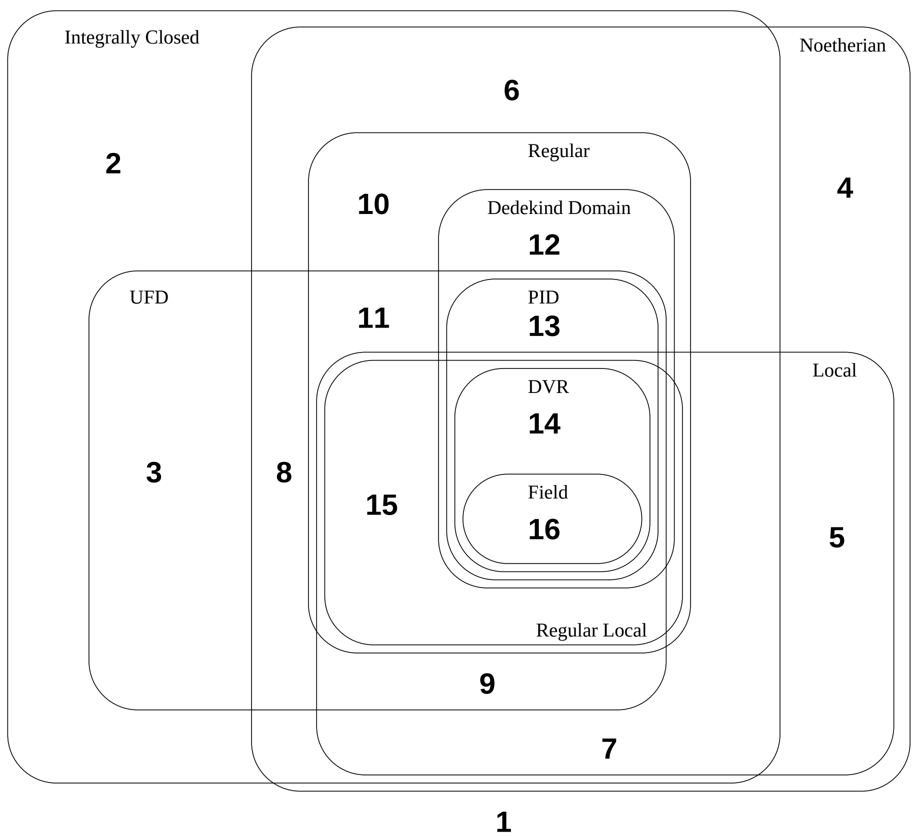
LR Local Ring

NR Noetherian ring

Appendix B

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:

- k
- $\mathbb{Q}$
- $\mathbb{R}$
- $\mathbb{C}$
- $\mathbb{Z}/p\mathbb{Z}$

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 C

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.

Bibliography

[1] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[2] Nicolas Bourbaki, *Éléments de mathématique*, Masson, Paris, 1980, Algèbre. Chapitre 10. Algèbre homologique. [Algebra. Chapter 10. Homological algebra].

[3] ———, *Commutative algebra. Chapters 1–7*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 1998, Translated from the French, Reprint of the 1989 English translation.

[4] Winfried Bruns and Jürgen Herzog, *Cohen-macaulay rings*, Cambridge Studies In Advances Mathematics, vol. 39, Cambridge University Press, Cambridge, 1993.

[5] Henri Cartan and Samuel Eilenberg, *Homological algebra*, Princeton Landmarks in Mathematics, Princeton University Press, Princeton, NJ, 1999, With an appendix by David A. Buchsbaum, Reprint of the 1956 original.

[6] David Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995, With a view toward algebraic geometry.

[7] Thomas W. Hungerford, *Algebra*, Holt, Rinehart and Winston, Inc., New York, 1974.

[8] Harry C. Hutchins, *Examples of commutative rings*, Polygonal Publ. House, Washington, N. J., 1981.

[9] Ernst Kunz, *Introduction to commutative algebra and algebraic geometry*, Birkhäuser Boston Inc., Boston, MA, 1985, Translated from the German by Michael Ackerman, With a preface by David Mumford.

[10] Serge Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[11] Hideyuki Matsumura, *Commutative algebra*, second ed., Mathematics Lecture Note Series, vol. 56, Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980.

[12] ———, *Commutative ring theory*, second ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1989, Translated from the Japanese by M. Reid.

[13] David Mumford, *The red book of varieties and schemes*, expanded ed., Lecture Notes in Mathematics, vol. 1358, Springer-Verlag, Berlin, 1999, Includes the Michigan lectures (1974) on curves and their Jacobians, With contributions by Enrico Arbarello.

[14] Masayoshi Nagata, *Local rings*, Interscience Tracts in Pure and Applied Mathematics, No. 13, Interscience Publishers a division of John Wiley & Sons New York-London, 1962.

[15] Jean-Pierre Serre, *Local algebra*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000, Translated from the French by CheeWhye Chin and revised by the author.

[16] Charles A. Weibel, *An introduction to homological algebra*, third ed., Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1997.

[17] Oscar Zariski and Pierre Samuel, *Commutative algebra, Volume I*, The University Series in Higher Mathematics, D. Van Nostrand Company, Inc., Princeton, New Jersey, 1958, With the cooperation of I. S. Cohen.

[18] ———, *Commutative algebra. Vol. II*, The University Series in Higher Mathematics, D. Van Nostrand Co., Inc., Princeton, N. J.-Toronto-London-New York, 1960.

Index