Commutative Algebra

Swayam Chube
Mentor: Aryaman Maithani

January 18, 2024

Abstract

Throughout this report, unless mentioned otherwise, all rings are assumed to be commutative. The term *noethering* is a portmanteau that is used in place of “noetherian ring” and is attributed to the accidental genius of Aryaman Maithani.

The main reference for this report is [AM69]. The section on projective modules and modules over a PID has been taken from [Lan02]. Some additional results about Dedekind domains have been taken from [Mil20]. The chapter on Completions has mainly been taken from [Gop84]. The section on Dimension Theory of Polynomial Algebras has been taken from [Ser12].

Contents

Chapter 1

Rings and Ideals

Definition 1.1 (Krull Dimension). A sequence $\{\mathfrak{p}_0, \ldots, \mathfrak{p}_n\}$ of prime ideals in A is said to be strictly ascending of length n if $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$. The *Krull dimension* of A is defined to be the supremum of the lengths of all strictly ascending sequences of prime ideals in A and is denoted by $\dim A$.

Proposition 1.2. *Let A and B be rings. Then, every prime ideal in $A \times B$ is of the form $\mathfrak{p} \times B$ where $\mathfrak{p} \subseteq A$ is a prime ideal or $A \times \mathfrak{q}$ where $\mathfrak{q} \subseteq B$ is a prime ideal.*

Proof. It is known that ideals in $A \times B$ are of the form $\mathfrak{a} \times \mathfrak{b}$ where $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in A and B respectively. Consequently, the quotient

$$A \times B/\mathfrak{a} \times \mathfrak{b} \cong A/\mathfrak{a} \times B/\mathfrak{b}$$

For $\mathfrak{a} \times \mathfrak{b}$ we require $A/\mathfrak{a} \times B/\mathfrak{b}$ to be an integral domain. This is possible if and only if either $\mathfrak{a}$ is a prime and $\mathfrak{b} = B$ or $\mathfrak{a} = A$ and $\mathfrak{b}$ is a prime. This completes the proof. ■

Theorem 1.3 (Chinese Remainder Theorem). *Let $\{\mathfrak{a}_i\}_{i=1}^n$ be comaximal ideals in A. Then,*

(a) $\displaystyle\bigcap_{i=1}^n \mathfrak{a}_i = \prod_{i=1}^n \mathfrak{a}_i$

(b) $\displaystyle A \Big/ \bigcap_{i=1}^n \mathfrak{a}_i \cong \prod_{i=1}^n A/\mathfrak{a}_i$

1.1 Nilradical and Jacobson radical

Definition 1.4 (Multiplicatively Closed). A subset $S \subseteq A$ is said to be *multiplicatively closed* if

(a) $1 \in S$

(b) for all $x, y \in S$, $xy \in S$

Proposition 1.5. *Let $S \subsetneq A \backslash \{0\}$ be a multiplicatively closed subset. Then, there is a prime ideal $\mathfrak{p}$ disjoint from S.*

1.2 Local Rings

Definition 1.6. A commutative ring A is said to be local if it has a unique maximal ideal.

Proposition 1.7. *A is local if and only if the subset of non-units form an ideal.*

Obviously, a field k is a local ring. On the other hand, the polynomial ring $k[x]$ is not local, since both x and $1 - x$ are non-units but their sum is a unit.

We contend that the ring $A = k[x_1, x_2, \ldots]/(x_1, x_2, \ldots)^2$ is local. Indeed, let π denote the canonical map $k[x_1, x_2, \ldots] \to A$ and $\mathfrak{m}$ be maximal in A. Then, $\pi^{-1}(\mathfrak{m})$ is maximal in $k[x_1, x_2, \ldots]$ and contains $(x_1, x_2, \ldots)^2$, therefore, contains $(x_1, x_2, \ldots)$. But the latter is maximal and therefore, $\pi^{-1}(\mathfrak{m}) = (x_1, x_2, \ldots)$ whence the maximal ideal is unique. Thus A is local.

1.3 Operations on Ideals

Obviously, the intersection $\mathfrak{a} \cap \mathfrak{b}$ of two ideals is an ideal. The sum of ideals is defined as the following collection

$$\sum_{i \in I} \mathfrak{a}_i = \left\{ \sum_{\text{finite } i \in I} a_i \,\middle|\, a_i \in \mathfrak{a}_i \right\}$$

It is not hard to argue that the sum is the smallest ideal containing the ideals $\{\mathfrak{a}_i\}_{i \in I}$. The product of two ideals is defined as

$$\mathfrak{a}\mathfrak{b} = \left\{ \sum_{\text{finite}} a_i b_i \,\middle|\, a_i \in \mathfrak{a},\ b_i \in \mathfrak{b} \right\}$$

Inductively, we may define powers of an ideal as $\mathfrak{a}^n = \mathfrak{a}\mathfrak{a}^{n-1}$ with the convention that $\mathfrak{a}^0 = (1) = A$.

Proposition 1.8. *Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \subseteq A$ be ideals. Then,*

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

Proof. Obviously, $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}(\mathfrak{b} + \mathfrak{c})$ and $\mathfrak{a}\mathfrak{c} \subseteq \mathfrak{a}(\mathfrak{b} + \mathfrak{c})$ and thus, $\mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c} \subseteq \mathfrak{a}(\mathfrak{b} + \mathfrak{c})$. On the other hand, any element of $\mathfrak{a}(\mathfrak{b} + \mathfrak{c})$ is a finite sum of the form $\sum_i a_i(b_i + c_i)$ which can be rearranged as $\sum_i a_i b_i + \sum_i a_i c_i \in \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$. This completes the proof. ■

Proposition 1.9. *(a) Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be prime ideals and let $\mathfrak{a}$ be an ideal contained in $\bigcup_{i=1}^n \mathfrak{p}_i$. Then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some $1 \le i \le n$.*

(b) Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals and let $\mathfrak{p}$ be a prime ideal containing $\bigcap_{i=1}^n \mathfrak{a}_i$. Then $\mathfrak{a}_i \subseteq \mathfrak{p}$ for some i.

For ideals $\mathfrak{a}, \mathfrak{b} \subseteq A$, define their ideal quotient as

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

Proposition 1.10. *Let* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \subseteq A$ *be ideals. Then*

1. $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$
2. $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c})$
3. $(\bigcap_{i\in I} \mathfrak{a}_i : \mathfrak{b}) = \bigcap_{i\in I}(\mathfrak{a}_i : \mathfrak{b})$

Proposition 1.11. *If every prime ideal in* A *is principal, then* A *is a principal ring.*

Proof. Suppose not. Let Σ be the poset of ideals in A that are not principal, ordered by inclusion and $\{\mathfrak{a}_i\}_{i\in I}$ be a chain in Σ. Let $\mathfrak{a} = \bigcup_{i\in I} \mathfrak{a}_i$. We claim that $\mathfrak{a}$ is not principal, for if it were, then $\mathfrak{a} = (a)$ for some $a \in A$. Then, $a \in \mathfrak{a}_i$ for some $i \in I$ whence $\mathfrak{a}_i = (a)$, a contradiction. Hence, every chain in Σ has an upper bound, therefore, Σ has a maximal element, say $\mathfrak{p}$.

We contend that $\mathfrak{p}$ is a prime ideal. Suppose not, then there are $a, b \notin \mathfrak{p}$ such that $ab \in \mathfrak{p}$. Add in later ■

Proposition 1.12. *Let* A *be a UFD. Then* A *is a PID if and only if* $\dim A \leq 1$.

1.3.1 Radical Ideals

Definition 1.13 (Radical Ideal). For an ideal $\mathfrak{a} \subseteq A$, we define its *radical* as

$$\sqrt{\mathfrak{a}} = \{x \in A \mid x^n \in \mathfrak{a} \text{ for some } n \in \mathbb{N}\}$$

An ideal which is the radical of some ideal is called a *radical ideal*.

Obviously, $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$. From our definition, it is not hard to see that the radical is the smallest radical ideal that contains a certain ideal. As a result, if $\mathfrak{a} \subseteq \mathfrak{b}$ are ideals, then $\sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{b}}$.

Proposition 1.14. *Let* $\mathfrak{a}, \mathfrak{b} \subseteq A$ *be ideals. Then,*

(i) $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$

(ii) $\sqrt{\mathfrak{a}\mathfrak{b}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$

(iii) $\sqrt{\mathfrak{a}^n} = \sqrt{\mathfrak{a}}$ *for every* $n \in \mathbb{N}$

(iv) $\sqrt{\mathfrak{a} + \mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}}$

Proof. (i) Trivial.

(ii) Since $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$, we must have $\sqrt{\mathfrak{a}\mathfrak{b}} \subseteq \sqrt{\mathfrak{a} \cap \mathfrak{b}}$. On the other hand, if $x \in \sqrt{\mathfrak{a} \cap \mathfrak{b}}$, there is a positive integer n such that $x^n \in \mathfrak{a} \cap \mathfrak{b}$, therefore, $x^{2n} \in \mathfrak{a}\mathfrak{b}$, and $x \in \sqrt{\mathfrak{a}\mathfrak{b}}$. This establishes the first equality.

As for the second inequality, if $x \in \sqrt{\mathfrak{a} \cap \mathfrak{b}}$, then there is a positive integer n such that $x^n \in \mathfrak{a} \cap \mathfrak{b}$, therefore, $x \in \sqrt{\mathfrak{a}}$ and $x \in \sqrt{\mathfrak{b}}$. Conversely, if $x \in \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$, then there are positive integers m and n such that $x^m \in \mathfrak{a}$ and $x^n \in \mathfrak{b}$, consequently, $x^{m+n} \in \mathfrak{a} \cap \mathfrak{b}$, and the conclusion follows.

(iii) Immediate from (ii).

(iv) Obviously, $\sqrt{\mathfrak{a}+\mathfrak{b}} \subseteq \sqrt{\sqrt{\mathfrak{a}}+\sqrt{\mathfrak{b}}}$. On the other hand, note that $\sqrt{\mathfrak{a}+\mathfrak{b}}$ is a radical ideal containing $\sqrt{\mathfrak{a}}$ and $\sqrt{\mathfrak{b}}$, therefore, contains $\sqrt{\mathfrak{a}}+\sqrt{\mathfrak{b}}$. Hence, $\sqrt{\mathfrak{a}+\mathfrak{b}} \supseteq \sqrt{\sqrt{\mathfrak{a}}+\sqrt{\mathfrak{b}}}$ and the conclusion follows.

■

Corollary 1.15. Ideals $\mathfrak{a}$ and $\mathfrak{b}$ are comaximal if and only if $\sqrt{\mathfrak{a}}$ and $\sqrt{\mathfrak{b}}$ are comaximal.

For a prime ideal $\mathfrak{p}$, note that $\sqrt{\mathfrak{p}} = \mathfrak{p}$ and due to (iii), $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$ for every positive integer n.

Proposition 1.16. *Let $\mathfrak{a} \subseteq A$ be an ideal with maximal radical. Then $A/\mathfrak{a}$ is a local ring of dimension* 0.

Proof. Let $\overline{\mathfrak{m}}$ be a maximal ideal in $A/\mathfrak{a}$. Since $\overline{\mathfrak{m}}$ is prime, its preimage in A is a prime ideal $\mathfrak{m}$ containing $\mathfrak{a}$, thus, it must contain $\sqrt{\mathfrak{a}}$, which is maximal, whence $\mathfrak{m} = \sqrt{\mathfrak{a}}$. Consequently $\overline{\mathfrak{m}} = \sqrt{\mathfrak{a}}/\mathfrak{a}$ and is uniquely determined.

On the other hand, if $\overline{\mathfrak{p}}$ is a prime ideal in $A/\mathfrak{a}$, using a similar argument as above, one may conclude that $\overline{\mathfrak{p}}$ is maximal and thus $\dim(A/\mathfrak{a}) = 0$. ■

1.4 Extension and Contraction of Ideals

Definition 1.17. Let $\phi : A \to B$ be a ring homomorphism. If $\mathfrak{a} \subseteq A$ is an ideal, then we define its extension $\mathfrak{a}^e = \phi(\mathfrak{a})A$. If $\mathfrak{b} \subseteq B$ is an ideal, then we define its contraction $\mathfrak{b}^c = \phi^{-1}(\mathfrak{b})$.

Proposition 1.18. *(a)* $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$ *and* $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$

(b) $\mathfrak{b}^c = \mathfrak{b}^{cec}$ *and* $\mathfrak{a}^e = \mathfrak{a}^{ece}$

(c) If C is the set of contracted ideals in A and E is the set of extended ideals in B, then $\mathfrak{a} \mapsto \mathfrak{a}^e$ is a bijection from C to E.

Proof. (a) Trivial.

(b) We have $\mathfrak{a}^e \subseteq (\mathfrak{a}^{ec})^e$ and $\mathfrak{a}^e \supseteq (\mathfrak{a}^e)^{ce}$. Similarly, $\mathfrak{b}^c \supseteq (\mathfrak{b}^c)^{ec}$ and $\mathfrak{b}^c \subseteq (\mathfrak{b}^c)^{ec}$ whence $\mathfrak{b}^c = \mathfrak{b}^{cec}$.

(c) Simply note that the maps $\mathfrak{a} \mapsto \mathfrak{a}^e$ and $\mathfrak{b} \mapsto \mathfrak{b}^c$ from C to E and E to C are inverses to one another.

■

1.5 The Zariski Topology

Definition 1.19 (Prime Spectrum). For a commutative ring A, define

$$\operatorname{Spec} A = \{\mathfrak{p} \mid \mathfrak{p} \text{ is a prime ideal in } A\}$$

This is called the *prime spectrum* of the ring. Similarly, define

$$\operatorname{MaxSpec} A = \{\mathfrak{m} \mid \mathfrak{m} \text{ is a maximal ideal in } A\}$$

For each $E \subseteq A$, define

$$V(E) = \{\mathfrak{p} \in \operatorname{Spec} A \mid E \subseteq \mathfrak{p}\}$$

Proposition 1.20. *(a) If $\mathfrak{a}$ is the ideal generated by E, then $V(E) = V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$*

(b) $V(0) = X$ and $V(1) = \varnothing$

(c) If $\{E_i\}_{i\in I}$ is a family of subsets of A, then

$$V\left(\bigcup_{i\in I} E_i\right) = \bigcap_{i\in I} V(E_i)$$

It is not hard to see that the collection

$$\mathcal{T} = \{\operatorname{Spec} A \backslash V(E) \mid E \subseteq A\}$$

is a topology on $\operatorname{Spec} A$. This is known as the *Zariski Topology*. In particular, $V(E)$ form closed subsets in $\operatorname{Spec} A$ under the Zariski topology.

Proposition 1.21. *For each $f \in A$, let $D(f) = \operatorname{Spec} A \backslash V(f)$. Then, the collection $\{D(f)\}_{f\in A}$ forms a basis for the Zariski topology on $\operatorname{Spec} A$.*

Proposition 1.22. *Let $f : A \to B$ be a ring homomorphism. Then, the map $f_* : \operatorname{Spec} B \to \operatorname{Spec} A$ given by $f_*(\mathfrak{q}) = f^{-1}(\mathfrak{p})$ is a continuous map. Further, if $g : B \to C$ is a ring homomorphism, then $(g \circ f)_* = f_* \circ g_*$.*

Proof. Let $\mathfrak{a} \subseteq A$ be an ideal. We shall show that $f_*^{-1}(V(\mathfrak{a}))$ is closed in B. Note that

$$\begin{aligned} f_*^{-1}(V_A(\mathfrak{a})) &= \{\mathfrak{p} \mid \mathfrak{a} \subseteq f_*(\mathfrak{p})\} \\ &= \{\mathfrak{p} \in \operatorname{Spec} B \mid \mathfrak{a} \subseteq f^{-1}(\mathfrak{p})\} \\ &= V_B((f(\mathfrak{a}))) \end{aligned}$$

whence the conclusion follows.

Next, for any $\mathfrak{p} \in \operatorname{Spec} C$, we have

$$(f_* \circ g_*)(\mathfrak{p}) = f_*(g^{-1}(\mathfrak{p})) = f^{-1}(g^{-1}(\mathfrak{p})) = (g \circ f)^{-1}(\mathfrak{p})$$

This completes the proof. ∎

This shows that Spec is a contravariant functor from **CRing** to **Top**.

1.5.1 On the Topological Properties

Proposition 1.23. $\operatorname{Spec} A$ *is Hausdorff if and only if* $\dim A = 0$.

Proof. ($\Longrightarrow$) We shall show that if $\operatorname{Spec} A$ is T_1, then $\dim A = 0$. Indeed, if $\operatorname{Spec} A$ is T_1, then $\{\mathfrak{p}\}$ is a closed set for very prime ideal $\mathfrak{p}$, therefore, there is an ideal $I \subseteq A$ such that $V(I) = \{\mathfrak{p}\}$. As a result, $V(\mathfrak{p}) = \{\mathfrak{p}\}$ and $\mathfrak{p}$ is maximal.

($\Longleftarrow$) Suppose $\dim A = 0$. Let $\mathfrak{p}$ and $\mathfrak{q}$ be distinct ideals. We contend that there are $f \notin \mathfrak{p}$ and $g \notin \mathfrak{q}$ such that fg is contained in every prime ideal in A, equivalently, fg is contained in $\mathfrak{N}(A)$. Suppose not, that is, for every pair $f \notin \mathfrak{p}$ and $g \notin \mathfrak{q}$, there is a prime ideal $\mathfrak{p}$ disjoint from $\{f, g\}$.

Let $X = A\backslash(\mathfrak{p} \cap \mathfrak{q})$. Let Σ be the collection of ideals $\mathfrak{a}$ contained in $\mathfrak{p} \cap \mathfrak{q}$ such that for every finite subset $F \subseteq X$, there is a prime ideal $\mathfrak{P}$ containing $\mathfrak{a}$ that is disjoint from F. It is not hard to see that $(0) \in \Sigma$ and that every ascending chain has an upper bound given by the union of all elements in the chain.

Let J be a maximal element in Σ whose existence is guaranteed due to Zorn's Lemma. We shall show that J is prime. Indeed, let $xy \in J$ with $y \notin J$. Then, $J + (y) \notin \Sigma$, therefore, there is a finite subset $F_0 \subseteq X$ such that for each prime ideal $\mathfrak{P}$ containing $J + (y)$, $\mathfrak{P} \cap F_0 \neq \varnothing$.

Now, let $F \subseteq X$ be finite, then so is $F \cup F_0$, therefore, there is a prime ideal I containing J such that $I \cap (F \cup F_0) = \varnothing$, which implies that $y \notin I$, lest $J + (y) \subseteq I$. But since $xy \in J \subseteq I$, we must have that $x \in I$. This shows that $J + (x) \subseteq I$, therefore, $(J + (x)) \cap F = \varnothing$ whence $J + (x) \in \Sigma$ and $x \in J$ due to the maximality. This shows that J is prime.

Finally, we see that if there is a prime ideal J contained in $\mathfrak{p} \cap \mathfrak{q}$, contradicting $\dim A = 0$. Thus, there is $f \notin \mathfrak{p}$ and $g \notin \mathfrak{q}$ such that fg is contained in $\mathfrak{N}(A)$. Consider the basic open sets $D(f)$ and $D(g)$, which contain $\mathfrak{p}$ and $\mathfrak{q}$ respectively and their intersection $D(f) \cap D(g) = D(fg)$ is the empty set since fg is contained in ever prime ideal, thus, Spec A is Hausdorff. ■

Corollary 1.24. If Spec A is T_1, then Spec A is Hasudorff.

1.6 Polynomial Rings

Add those exercises from AM

Chapter 2

Modules

2.1 Introduction

Throughout this section, R denotes a general ring which need not be commutative.

Definition 2.1 (Module). A left R-module is an abelian group $(M, +)$ along with a ring action, that is, a ring homomorphism $\mu : R \to \text{End}(M)$. Similarly, a right R-module is an abelian group $(M, +)$ along with a ring homomorphism $\mu : R^{\text{op}} \to \text{End}(M)$ where R^{op} is the opposite ring.

Henceforth, unless specified otherwise, an *R-module* refers to a *left R-module*. Trivially note that R is an R-module, so is any ideal in R and so is every quotient ring R/I where I is an ideal in R. When R is a field, an R-module is the same as a vector space.

Every abelian group G trivially forms a $\mathbb{Z}$-module. Using this and the forthcoming *Structure Theorem for Finitely Generated Modules over a PID*, we obtain the *Structure Theorem for Finitely Generated Abelian Groups*.

There is also the notion of a bimodule:

Definition 2.2. For

Definition 2.3 (Submodule). Let M be an R-module. An R-submodule of M is a subgroup N of M which is closed under the action of R.

Proposition 2.4 (Submodule Criteria). *Let M be an R-module. Then $\varnothing \subsetneq N \subseteq M$ is a submodule if and only if for all $x, y \in N$ and $r \in R$, $x + ry \in N$.*

Proof. Straightforward definition pushing. ■

Definition 2.5 (Module Homomorphism). Let M, N be R-modules. A *module homomorphism* is a group homomorphism $\phi : M \to N$ such that for all $x \in M$ and $r \in R$, $\phi(rx) = r\phi(x)$.

In other words, a module homomorphism is simply an R-linear map.

Proposition 2.6 (Homomorphism Criteria). *Let M, N be R-modules. Then $\phi : M \to N$ is an R-module* *homomorphism if and only if for all $x, y \in M$ and $r \in R$, $\phi(x + ry) = \phi(x) + r\phi(y)$.*

Proof. Straightforward definition pushing. ■

It is not hard to see, using the above proposition and the submodule criteria that the image of an R-module under a homomorphism is a submodule.

Definition 2.7 (Kernel, Cokernel). Let $\phi : M \to N$ be an R-module homomorphism. We define

$$\ker \phi = \{x \in M \mid \phi(x) = 0\} \qquad \operatorname{coker} \phi = N/\phi(M)$$

For an R-module M, define the annihilator of M in R as

$$\operatorname{Ann}_R(M) = \{r \in R \mid rx = 0 \;\forall x \in M\}$$

It is trivial to check that $\operatorname{Ann}_R(M)$ is a left ideal in R, and if R were commutative, it would be an ideal. When $\operatorname{Ann}_A(M) = 0$, M is said to be a *faithful* A-module.

Proposition 2.8. *If I is an ideal contained in $\operatorname{Ann}_A(M)$, then M is naturally an A/I-module.*

Proof. Define the action $(a + I) \cdot m = a \cdot m$. It is easy to check that this action is well defined. Further,

$$(a + I) \cdot ((b + I) \cdot m) = (a + I) \cdot (bm) = (ab) \cdot m = ((a + I)(b + I)) \cdot m$$

This completes the proof. ■

Proposition 2.9. *N is an A-submodule of M if and only if it is an $A/\operatorname{Ann}_A(M)$ submodule of M.*

Proof. Straightforward. ■

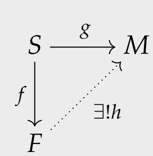
In particular, if $I = \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, then M forms a vector space over $A/\mathfrak{m}$.

2.2 Free Modules

Throughout this section, R denotes a general ring which need not be commutative.

We define the free module using a universal property and then provide a construction for it. This should establish uniqueness.

Definition 2.10 (Universal Property of Free Modules). Let S be a non-empty set. A *free module on S* is an R-module F together with a mapping $f : S \to F$ such that for every R-module M and every set map $g : S \to M$, there is a unique R-module homomorphism $h : F \to M$ such that the following diagram commutes:



Let F be the set of all set functions $\phi : S \to R$ which takes nonzero values at finitely many elements of S. This has the structure of an R-module. Define the set map $f : S \to F$ by

$$f(s)(t) = \begin{cases} 1 & s = t \\ 0 & \text{otherwise} \end{cases}$$

We contend that (F, f) is a free module on S. Indeed, let $g : S \to M$ be a set map where M is an R-module. Define the linear map $h : F \to M$ by

$$h(f(s)) = g(s)$$

Since every element in F can uniquely be written as a linear combination of elements in $\{f(s)\}_{s \in S}$, we have successfully defined a module homomorphism $h : F \to M$ such that $g = h \circ f$. The uniqueness of this map is quite obvious. Hence, (F, f) is a free module on S.

Definition 2.11 (Basis). Let M be an R-module. Then $S \subseteq M$ is said to be a *basis* if it is linearly independent and generates M.

It is important to note that not every minimal generating set is a basis. Take for example the $\mathbb{Z}$-module $\mathbb{Z}$. Notice that $\{2, 3\}$ is a minimal generating set but is not a basis for it is not linearly independent.

2.2.1 Over a PID

Throughout this (sub)section, let R denote a PID.

Theorem 2.12. *Let F be a free R-module. If $M \leq F$ is a submodule, then M is free and* $\dim M \leq \dim F$.

Proof. Let F have basis $\{x_i\}_{i \in I}$ and $\pi_i : F \to R$ denote the natural projection. Using the Well Ordering Theorem, we may suppose that $(I, \leqq)$ has a well order, in particular, we may suppose that I is a segment of ordinals. For each $i \in I$, denote

$$M_i := M \cap \left\langle \{x_j \mid j \leqq i\} \right\rangle.$$

We shall show, using transfinite induction that each M_α is free module with rank less than or equal to $|\alpha|$. Consider the base case, $\alpha = 1$. Now, M_1 is a submodule of Rx_1 whence is isomorphic to an ideal of R, which is either the zero ideal of principal, i.e. free of rank 1.

We now move to the induction step. First, we consider the case when i is a successor ordinal and due to the induction hypothesis, M_{i-1} is a free R-module of rank less than or equal to $|i - 1|$. Let

$$\mathfrak{a} = \{\pi_i(x) \mid x \in M_i\}.$$

Note that $\mathfrak{a}$ is an R-submodule of R whence an ideal of R. Thus, either $\mathfrak{a} = 0$ or $\mathfrak{a} = (a)$ for some $a \in R \backslash \{0\}$. In the former case, $M_i = M_{i-1}$ which completes the induction step. In the latter case, there is some $w \in M_i$ such that $\pi_i(w) = a$.

Now, consider any element $x \in M_i$. Then, x can be written as a linear combination

$$x = \sum_{j < i} a_j x_j + b x_i.$$

According to our choice of x, $b \in (a)$ whence, there is a suitable $r \in R$ suchthat $x - rw \in M_{i-1}$. That is, $M_i = M_{i-1} + (w)$. We contend that this sum is direct. To see this, suppose $cw \in M_{i-1}$ for some $c \in R$ and suppose $w = \sum_{j \leqq i} \alpha_j x_j$. Then,

$$\sum_{j \leqq i} c\alpha_j x_j = \sum_{j < i} \beta_j \alpha_j,$$

for some $\beta_j \in R$, implying that $cx_i = 0$, i.e. $c = 0$. Hence, $M_i = M_{i-1} \oplus (w)$.

Next, we deal with the case of limit ordinals. Suppose λ is a limit ordinal in I. Then, we have a function $f : \lambda \to M$ such that for each $i < \lambda$, the module M_i is free, generated by $\{f(j) \mid j \leqq i\}$. Whence, M_λ is generated by $\{f(j) \mid j < \lambda\}$ and is obviously free. This completes the inductive step and thus the proof of the theorem. ■

2.3 Finitely Generated Modules

Definition 2.13 (Finitely Generated Module). An R-module M is said to be finitely generated if there is a finite subset S of M which generates M. That is, there is no proper submodule N of M containing S.

A submodule of a finitely generated module need not be finitely generated, let $A = \mathbb{Z}[x_1, x_2, \ldots]$ and consider A as an A-module. The ideal $(x_1, x_2, \ldots)$ is not finitely generated.

Proposition 2.14. *An R-module M is finitely generated if and only if M is isomorphic to a quotient of $R^{\oplus n}$ for some positive integer n.*

Proof. We shall only prove the forward direction since the converse is trivial to prove. Suppose M is finitely generated. Then, it is generated by a finite subset $S = \{x_1, \ldots, x_m\}$. Define the R-module homomorphism $\phi : R^{\oplus n} \to M$ by $(r_1, \ldots, r_n) \mapsto r_1x_1 + \cdots + r_nx_n$. From the first isomorphism theorem, we have $M \cong R^{\oplus n} / \ker \phi$. ■

Proposition 2.15. *Let M be a finitely generated A-module and $\mathfrak{a}$ an ideal of A. Let $\phi \in \operatorname{End}(M)$ such that $\phi(M) \subseteq \mathfrak{a}M$. Then, there are $a_0, \ldots, a_{n-1} \in \mathfrak{a}$ such that*

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

as an element of $\operatorname{End}(M)$*, where a_k is treated as the homomorphism $x \mapsto a_kx$ in* $\operatorname{End}(M)$*.*

Proof. Let $\{x_1, \ldots, x_n\}$ be a generating set for M. Then, for all $1 \leq i \leq n$, there are coefficients $\{a_{i1}, \ldots, a_{in}\}$ in $\mathfrak{a}$ such that

$$\phi(x_i) = \sum_{j=1}^{n} a_{ij}x_j$$

We may rewrite this as

$$\sum_{j=1}^{n} (\phi\delta_{ij} - a_{ij})x_j = 0$$

Let B denote the matrix $(\phi\delta_{ij} - a_{ij})_{1 \leq i,j \leq n}$. Then, multiplying by $\operatorname{adj}(B)$, we see that $\det(B)(x_j) = 0$ for all $1 \leq j \leq n$ where $\det(B)$ is viewed as an element in $\operatorname{End}(M)$ and thus, is the zero map in $\operatorname{End}(M)$. It is not hard to see that $\det(B)$ is in the required form. ■

Corollary 2.16. Let M be a finitely generated A-module and $\mathfrak{a}$ an ideal of A such that $\mathfrak{a}M \subseteq M$, then there is $a \in \mathfrak{a}$ such that $(1 + a)M = 0$.

Proof. Substitute $\phi = \mathbf{id}$ in the above proposition. ■

Lemma 2.17 (Nakayama). *Let M be a finitely generated module and $\mathfrak{a} \subseteq \mathfrak{R}$ be an ideal such that $M = \mathfrak{a}M$. Then, $M = 0$.*

Proof. Let $\phi = \mathbf{id}$ be the identity homomorphism in $\operatorname{End}(M)$. Using Proposition 2.15, there are coefficients $a_0, \ldots, a_{n-1} \in \mathfrak{a}$ satisfying the statement of the proposition. As a result, $x = 1 + a_{n-1} + \ldots + a_0$ is the zero endomorphism. But since $a_{n-1} + \ldots + a_0 \in \mathfrak{a} \subseteq \mathfrak{R}$, x is a unit and hence, $M = 0$. ■

Corollary 2.18. Let M be a finitely generated A-module, N a submodule of M and $\mathfrak{a} \subseteq \mathfrak{R}$ an ideal. If $M = \mathfrak{a}M + N$ then $M = N$.

Proof. We have $M/N = \mathfrak{a}M/N$, consequently, $M/N = 0$ and $M = N$ due to Lemma 2.17. ■

A surprising application of Nakayama is the following.

Proposition 2.19. *Let M be a finitely generated A-module and $\varphi : M \to M$ a surjective homomorphism. Then, φ is an isomorphism.*

Proof. Notice that M also has the structure of an $A[x]$-module where the action of x is given by

$$x \cdot m = \varphi(m).$$

Further, note that M is still finitely generated as an $A[x]$ module. Due to the surjectivity of φ, we have $(x)M = M$. Due to Corollary 2.16, there is some $f(x) \in A[x]$ such that $(1 + xf(x))M = 0$, that is, for each $m \in M$, $(1 + xf(x))m = 0$. If $m \in \ker \varphi$, then it is immediate that $0 = m + f(\varphi)(\varphi(m)) = m$ and thus φ is injective. This completes the proof. ■

Lemma 2.20. *Let $(A, \mathfrak{m})$ be local and $k = A/\mathfrak{m}$. Let M be a finitely generated A-module. Let $\{\overline{x}_1, \ldots, \overline{x}_n\}$ be elements in $M/\mathfrak{m}M$ that form a basis for $M/\mathfrak{m}M$ as a k-vector space. Then, $\{x_1, \ldots, x_n\}$ generates M.*

Proof. Let N be the submodule generated by $\{x_1, \ldots, x_n\}$. Then, the composition $N \hookrightarrow M \twoheadrightarrow M/\mathfrak{m}M$ is surjective, consequently, $M = N + \mathfrak{m}M$ whence, it follows that $M = N$. ■

Proposition 2.21. *Let $\mathfrak{a} \trianglelefteq A$ be a finitely generated ideal. If $\mathfrak{a}$ is idempotent, then it is principal.*

Proof. We have $\mathfrak{a}^2 = \mathfrak{a}$ and viewing $\mathfrak{a}$ as an A-module, due to Corollary 2.16, there is some $a \in \mathfrak{a}$ such that $(1 - a)\mathfrak{a} = 0$. In particular, $\mathfrak{a} \subseteq (a)$, and thus, $\mathfrak{a} = (a)$. ■

2.4 Hom **Modules and Functors**

For R-modules M, N, we denote the set of all R-module homomorphisms from M to N by $\operatorname{Hom}_R(M, N)$. When the choice of the ring R is clear from the context, we shall denote this set by $\operatorname{Hom}(M, N)$.

Proposition 2.22. *Let M, N be A-modules. Then* $\operatorname{Hom}(M, N)$ *has the structure of an A-module.*

Proof. It is obvious that $\operatorname{Hom}(M, N)$ has the structure of an abelian group. Define the natural action by $(af)(x) = af(x)$. It is not hard to see that this action is well defined. ■

Proposition 2.23. *Let $\{M_\lambda\}_{\lambda\in\Lambda}$ be a collection of A-modules. Then, for any A-module N, we have a natural isomorphism*

$$\operatorname{Hom}_A\left(\bigoplus_{\lambda\in\Lambda} M_\lambda, N\right) \cong \prod_{\lambda\in\Lambda} \operatorname{Hom}_A(M_\lambda, N)$$

Proof. Since the direct sum is the coproduct in $A - \mathbf{Mod}$, the conclusion follows from the universal property. ■

Proposition 2.24. *If M is a finitely generated A-module and $\{N_i\}_{i\in I}$ is a collection of A-modules, then there is a natural isomorphism*

$$\operatorname{Hom}_A\left(M, \bigoplus_{i\in I} N_i\right) \cong \bigoplus_{i\in I} \operatorname{Hom}_A(M, N_i)$$

Proof. Consider the map

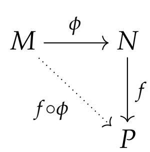
$$\Phi : \operatorname{Hom}_A\left(M, \bigoplus_{i\in I} N_i\right) \to \bigoplus_{i\in I} \operatorname{Hom}_A(M, N_i)$$

given by $\Phi(f) = (\pi_i \circ f)_{i\in I}$. That this map is well-defined follows from the fact that M is a finitely generated A-module. The rest is a routine verification of injectivity and surjectivity. ■

Theorem 2.25. *Let $\phi : M \to N$ be an A-module homomorphism. Then, for every R-module P, there is an induced A-module homomorphism $\overline{\phi} : \operatorname{Hom}(N, P) \to \operatorname{Hom}(M, P)$ and an induced A-module homomorphism $\widetilde{\phi} : \operatorname{Hom}(P, M) \to \operatorname{Hom}(P, N)$.*

Equivalently phrased, $\operatorname{Hom}(-, P)$ is a contravariant functor while $\operatorname{Hom}(P, -)$ is a covariant functor.

Proof. We shall prove only the first half of the assertion since the second half follows from a similar proof. Define $\overline{\phi}$ using the following commutative diagram:



To see that this is indeed an R-module homomorphism, we need only verify that for all $f, g \in \operatorname{Hom}(N, P)$ and all $r \in R$, $(f + rg) \circ \phi = f \circ \phi + rg \circ \phi$ which is trivial to check. ■

Theorem 2.26. $\operatorname{Hom}(M, -)$ *is a left exact functor.*

Proof. Let $0 \to N' \xrightarrow{f} N \xrightarrow{g} N''$ be an exact sequence. First, we shall show that $\overline{f}$ is injective. Indeed, let $u \in \ker \overline{f}$. Then, $f \circ u$ is the zero morphism. But since f is injective, we must have that u is the zero morphism.

Next, we shall show that $\operatorname{im} \overline{f} = \ker \overline{g}$. Obviously, $\overline{g} \circ \overline{f} = 0$ and thus it suffices to show $\ker \overline{g} \subseteq \ker \overline{f}$. Let $u \in \ker \overline{g}$. That is, $g \circ u = 0$. Then, we may define $v : M \to N'$ by $v(m) = f^{-1}(u(m))$, which is well defined since f is injective. It is not hard to see that v is a module homomorphism, implying the desired conclusion. ■

2.5 Exact Sequences

Definition 2.27. A sequence of module homomorphisms

$$M \xrightarrow{f} N \xrightarrow{g} P$$

is said to be exact at N if $\operatorname{im} f = \ker g$. A short exact sequence is a sequence of module homomorphisms:

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$$

which is exact at M, N and P.

It is not hard to see that the sequence in the definition is short exact if and only if f is injective, g is surjective and $\operatorname{im} f = \ker g$.

2.5.1 Diagram Chasing Poster Children

Throughout this (sub)section, A, B, C are R-modules where R is a commutative ring.

Lemma 2.28 (Splitting Lemma). *Let $0 \longrightarrow A \xrightarrow{\iota} B \xrightarrow{\pi} C \longrightarrow 0$ be a short exact sequence. Then the following are equivalent.*

(a) There is $\varphi : C \to B$ such that $\pi \circ \varphi = \mathbf{id}_C$

(b) There is $\psi : B \to A$ such that $\psi \circ \iota = \mathbf{id}_A$

(c) There is an isomorphism $\Phi : B \to A \oplus C$ making the following diagram commute.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{\iota} & B & \xrightarrow{\pi} & C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathbf{id}_A} & & \vdots{\scriptstyle \Phi} & & \downarrow{\scriptstyle \mathbf{id}_C} & & \\
0 & \longrightarrow & A & \longrightarrow & A \oplus C & \longrightarrow & C & \longrightarrow & 0
\end{array}$$

Proof. $(a) \implies (b)$. Define $\psi(b) = \iota^{-1}(b - \varphi(\pi(b)))$. That this map is well defined follows from $\operatorname{im} \iota = \ker \pi$ and that it is a homomorphism is trivial. It is not hard to see that $\psi \circ \iota = \mathbf{id}_A$.

$(b) \implies (c)$. Define the map $\Phi : B \to A \oplus C$ by $\Phi(b) = (\psi(b), \pi(b - \iota \circ \psi(b)))$. It is trivial to check that this is an R-module homomorphism. From the Short Five Lemma, it now follows that Φ is an isomorphism.

$(c) \implies (a)$. Trivial. ■

2.6 Tensor Product

Definition 2.29 (Bilinear Map). Let M, N, P be A-modules. A map $T : M \times N \to P$ is said to be bilinear if for each $x \in M$, the mapping $T_x : N \to P$ given by $y \mapsto T(x, y)$ is A-linear and for each $y \in N$, the mapping $T_y : M \to P$ given by $x \mapsto T(x, y)$ is A-linear.

Fix two A-modules M and N. Let $\mathscr{C}$ denote the category of bilinear maps $T : M \times N \to P$ where P is any A-module. A morphism between two bilinear maps $f : M \times N \to P_1$ and $g : M \times N \to P_2$ in this category is a module homomorphism $\phi : P_1 \to P_2$ such that the following diagram commutes:

$$\begin{array}{ccc} M \times N & \xrightarrow{f} & P_1 \\ {\scriptstyle g}\downarrow & \swarrow {\scriptstyle \phi} & \\ P_2 & & \end{array}$$

A universal object in $\mathscr{C}$ is called the tensor product of M and N and is denoted by $M \otimes N$. In other words, the tensor product is an initial object in the category $\mathscr{C}$.

Definition 2.30 (Universal Property of the Tensor Product). Let M, N, P be A-modules and $T : M \times N \to P$ be a bilinear map. Then, there is a unique A-module homomorphism $\phi : M \otimes N \to P$ such that the following diagram commutes:

$$\begin{array}{ccc} M \times N & \xrightarrow{T} & P \\ {\scriptstyle \varphi}\downarrow & \nearrow {\scriptstyle \exists! \phi} & \\ M \otimes_A N & & \end{array}$$

Of course, having the universal property would imply that the tensor product, if it exists, is unique upto a unique isomorphism. We shall now construct a tensor product of M and N.

Constructing the Tensor Product

Let F be the free A-module on $M \times N$. Let us denote the basis elements of F by $e_{(x,y)}$ where $x \in M$ and $y \in N$. Now, for all $x, x_1, x_2 \in M$, $y, y_1, y_2 \in N$ and $a \in A$, let D denote the submodule generated by elements of the form:

$$\begin{aligned} &e_{(x_1+x_2,y)} - e_{(x_1,y)} - e_{(x_2,y)} \\ &e_{(x,y_1+y_2)} - e_{(x,y_1)} - e_{(x,y_2)} \\ &e_{(ax,y)} - ae_{(x,y)} \\ &e_{(x,ay)} - ae_{(x,y)} \end{aligned}$$

Let $G = F/D$ and let $\varphi : M \times N \to G$ be the composition of the following maps:

$$M \times N \hookrightarrow F \twoheadrightarrow G$$

Let $T : M \times N \to P$ be a bilinear map. Consider the following commutative diagram:

$$\begin{array}{ccc} M \times N & \xrightarrow{T} & P \\ {\scriptstyle \iota}\downarrow & \nearrow {\scriptstyle \exists! f} & \uparrow {\scriptstyle \exists! \phi} \\ F & \xrightarrow[\pi]{} & G \end{array}$$

To show that existence of ϕ, we must show that $D \subseteq \ker f$, since we can then finish using the universal property of the kernel. But this is trivial to check and follows from the fact that T is a bilinear map and completes the construction.

Similarly, we define the tensor product for a finite sequence of A-modules $\{M_i\}_{i=1}^{n}$. That is, given a multilinear map $T : \prod_{i=1}^{n} M_i \to P$, there is a unique A-module homomorphism ϕ such that the following diagram commutes:

$$\begin{array}{ccc} M_1 \times \cdots \times M_n & \xrightarrow{T} & P \\ \Big\downarrow{\scriptstyle \varphi} & \nearrow{\scriptstyle \exists! \phi} & \\ M_1 \otimes \cdots \otimes M_n & & \end{array}$$

Proposition 2.31. *Let F and G be free A-modules with basis given by $\{f_i\}_{i\in I}$ and $\{g_j\}_{j\in J}$ respectively. Then, $F \otimes_A G$ is a free A-module with basis $\{f_i \otimes g_j\}_{i\in I,\, j\in J}$.*

Proof. It is not hard to see that the set $\{f_i \otimes g_j\}_{i\in I,\, j\in J}$ is generating for $F \otimes_A G$. Therefore, it suffices to show that this set is linearly independent. Suppose not, then there is a finite linear combination

$$\sum_{i\in I,\, j\in J} a_{ij} f_i \otimes g_j = 0$$

Pick some $i_0 \in I$ and $j_0 \in J$. Let $\phi : F \times G \to A$ be the bilinear map such that

$$\phi(f_i, g_j) = \begin{cases} 1 & i = i_0 \text{ and } j = j_0 \\ 0 & \text{otherwise} \end{cases}$$

This induces an A-module homomorphism $\varphi : F \otimes G \to A$ such that

$$\varphi(f_i \otimes g_j) = \begin{cases} 1 & i = i_0 \text{ and } j = j_0 \\ 0 & \text{otherwise} \end{cases}$$

whence, it follows that $a_{i_0 j_0} = 0$ and the collection $\{f_i \otimes g_j\}_{i\in I,\, j\in J}$ is linearly independent. ■

2.6.1 Properties of Tensor Product

Given two modules M and N with the canonical map $\varphi : M \times N \to M \otimes N$, we denote by $m \otimes n$, the element $\varphi(m, n)$ in $M \otimes N$.

Proposition 2.32. *Let M, N, P be A-modules and $\{M_i\}_{i\in I}$ a collection of A-modules. Then,*

(a) $M \otimes_A N \cong N \otimes_A M$

(b) $(M \otimes_A N) \otimes_A P \cong M \otimes_A (N \otimes_A P) \cong M \otimes_A N \otimes_A P$

(c) $(\bigoplus_{i\in I} M_i) \otimes_A N \cong \bigoplus_{i\in I} (M_i \otimes_A N)$

(d) $A \otimes_A M \cong M$

Proof. (a) First, we shall show that there are well defined homomorphisms $M \otimes N \to N \otimes M$ and $N \otimes M \to M \otimes N$ mapping $m \otimes n \mapsto n \otimes m$ and $n \otimes m \mapsto m \otimes n$ respectively. This is best done using the universal property. Let $T : M \times N \to N \times M$ be the isomorphism $m \times n \mapsto n \times m$. Consider now the following commutative diagram:

$$\begin{array}{ccc} M \times N & \xrightarrow{T} & N \times M \\ \Big\downarrow{\scriptstyle \varphi} & & \Big\downarrow{\scriptstyle \varphi'} \\ M \otimes N & & N \otimes M \end{array}$$

Since both φ' and T are bilinear, so is $\varphi \circ T$, consequently, there is a unique induced homomorphism $f : M \otimes N \to N \otimes M$ making the diagram commute, consequently, $f(m \otimes n) = \varphi'(T(m \times n)) = n \otimes m$.

Similarly, there is a homomorphism $g : N \otimes M \to M \otimes N$ such that $g(n \otimes m) = m \otimes m$. It is not hard to see that $g \circ f = \mathbf{id}_{M \otimes N}$ and $f \circ g = \mathbf{id}_{N \otimes M}$, consequently, they are isomorphisms.

(b) We shall show $(M \otimes_A N) \otimes_A P \cong M \otimes_A N \otimes_A P$ since the proof of the other isomorphism follows analogously. Fix some $z \in P$ and consider the map $f_z : M \times N \to M \otimes_A N \otimes_A P$ given by $(x, y) \mapsto x \otimes y \otimes z$. This is an A-linear map and thus induces a map $g_z : M \otimes_A N \to M \otimes_A N \otimes_A P$ given by $g_z(x \otimes y) = x \otimes y \otimes z$. The map $G : (M \otimes_A N) \times P \to M \otimes_A N \otimes_A P$ given by $G(x \otimes y, z) = g_z(x \otimes y) = x \otimes y \otimes z$ is a well defined A-linear map which induces a map $h : (M \otimes_A N) \otimes_A P \to M \otimes_A N \otimes_A P$ given by $(x \otimes y) \otimes z \mapsto x \otimes y \otimes z$.

On the other hand, the map $F : M \times N \times P \to (M \otimes_A N) \otimes_A P$ given by $(x, y, z) \mapsto x \otimes y \otimes z$ is A-linear and thus induces a map $f : M \otimes_A N \otimes_A P \to (M \otimes_A N) \otimes_A P$ given by $x \otimes y \otimes z \mapsto (x \otimes y) \otimes z$. Since the maps f and h are inverses to one another for elementary tensors, they are inverses to one another over their respective domains, whereby both are isomorphisms.

(c) Define the map $f : (\bigoplus_{i \in I} M_i) \times N \to \bigoplus (M_i \otimes_A N)$ by $f((m_i) \otimes n) = (m_i \otimes n)$, which is a bilinear map. This induces a map $\phi : (\bigoplus_{i \in I} M_i) \otimes_A N \to \bigoplus_{i \in I} (M_i \otimes_A N)$ such that $f((m_i) \otimes n) = (m_i \otimes n)$.

Now, consider the map $f_i : M_i \times N \to M \otimes N$ given by $f_i(m_i, n) = \iota_i(m_i) \otimes n$. This induces a map $g_i : M_i \otimes_A N \to M \otimes N$ such that $g_i(m_i \otimes n) = \iota_i(m_i) \otimes n$. We may now define a map $\psi : \bigoplus_{i \in I} (M_i \otimes_A N) \to (\bigoplus_{i \in I} M_i) \otimes_A N$ given by

$$\psi((m_i \otimes n_i)) = \sum g_i(m_i \otimes n_i)$$

Obviously the sum on the right is a finite sum. Further, since each each g_i is well defined, so is ψ.

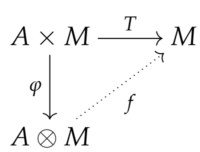
Lastly, we shall show that ϕ and ψ are inverses to one another. Indeed,

$$\psi \circ \phi((m_i) \otimes n) = \psi((m_i \otimes n)) = \sum \iota_i(m_i) \otimes n = (m_i) \otimes n$$

and

$$\phi \circ \psi((m_i \otimes n_i)) = \sum \phi(g_i(m_i \otimes n_i)) = (m_i \otimes n_i)$$

(d) Consider the map $T : A \times M \to M$ given by $(a, m) \mapsto am$. It is not hard to see that this map is bilinear, consequently, there is a map $f : A \otimes M \to M$ such that the following diagram commutes:



Note that $f(a \otimes m) = am$ by definition. Consider the map $g : M \to A \otimes M$ given by $g(m) = 1 \otimes m$. It is not hard to see that g is a well defined module homomorphism. Further, since $f \circ g$ and $g \circ f$ are the identity homomorphisms, they both must be isomorphisms.

■

Example 2.33. Show that $\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/\gcd(m, n)\mathbb{Z}$ for all $m, n \in \mathbb{N}$. In particular, if m and n are coprime, then $\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} = 0$.

Proof. Consider the module homomorphism $T : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z}$. ■

Let $f : M \to M'$ and $g : N \to N'$ be A-module homomorphisms. Then, the map $\Phi : M \times N \to M' \otimes N'$ given by $\Phi(m, n) = f(m) \otimes g(n)$. It is not hard to see that Φ is bilinear. Consequently, it induces a map $f \otimes g : M \otimes N \to M' \otimes N'$ such that

$$(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$$

Further, if $f' : M' \to M''$ and $g' : N' \to N''$ are A-module homomorphisms, then we have another map $f' \otimes g' : M' \otimes N' \to M'' \otimes N''$ such that

$$(f' \otimes g')(x \otimes y) = f'(x) \otimes g'(y)$$

Now, it is not hard to see that $(f' \circ f') \otimes (g' \circ g)$ and $(f' \otimes g') \circ (f \otimes g)$ agree on the elementary tensors, therefore, agree on all of $M \otimes N$.

2.6.2 Restriction and Extension of Scalars

Let $\phi : A \to B$ be a homomorphism of rings. We shall

- convert an B-module into an A-module. This is known as *restriction of scalars*.
- construct from an A-module a B-module. This is known as *extension of scalars*.

The first is rather easy to do. Begin with an B-module M and define the action of A by $a \cdot m = \phi(a) \cdot m$. That this is a valid ring action is easy to verify. As for the second, note that the homomorphism ϕ gives B the structure of an A-module whereby, we may consider the tensor product of A-modules $B \otimes_A M$. Now, for $b, b' \in B$, define

$$b' \cdot (b \otimes m) = bb' \otimes m$$

It is not hard to see that this is a ring, whereby, $B \otimes_A M$ is also a B-module.

2.7 Right Exactness

Proposition 2.34. *Let M, N, P be A-modules. Then, there is a natural isomorphism:*

$$\mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)) \cong \mathrm{Hom}_A(M \otimes_A N, P)$$

Proof. Consider the map

$$\theta : \mathrm{Hom}_A(M \otimes_A N, P) \longrightarrow \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P))$$

given by $\theta(\alpha)(m)(n) = \alpha(m \otimes n)$. Now, pick some $\eta \in \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P))$. Define the map $\zeta : M \times N \to P$ given by $\zeta(m, n) = \eta(m)(n)$. Obviously, ζ is bilinear and induces a map $\delta : M \otimes_A N \to P$ such that $\delta(m \otimes n) = \eta(m)(n)$. Call the map sending $\eta \mapsto \delta$ as β where

$$\beta : \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)) \to \mathrm{Hom}_A(M \otimes_A N, P)$$

and $\beta(\eta)(m \otimes n) = \eta(m)(n)$.

We contend that θ and β are inverses to one another. Indeed,

$$((\beta \circ \theta)(\alpha))(m \otimes n) = \theta(\alpha)(m)(n) = \alpha(m \otimes n)$$

and

$$((\theta \circ \beta)(\eta))(m)(n) = \beta(\eta)(m \otimes n) = \eta(m)(n)$$

whence the conclusion follows. ■

In particular, we see that the functor $- \otimes_A N$ is the left adjoint of the functor $\mathrm{Hom}_A(N, -)$, consequently, $\mathrm{Hom}_A(N, -)$ is the right adjoint of $- \otimes_A N$.

Theorem 2.35. *The functor $- \otimes_A N$ is right exact. That is, given a exact sequence*

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

the sequence

$$M' \otimes_A N \xrightarrow{f\otimes 1} M \otimes_A N \xrightarrow{g\otimes 1} M'' \otimes_A N \longrightarrow 0$$

Proof. Since the given sequence is exact, so is

$$\mathrm{Hom}_A(M'', \mathrm{Hom}_A(N,P)) \xrightarrow{\overline{g}} \mathrm{Hom}_A(M, \mathrm{Hom}_A(N,P)) \xrightarrow{\overline{f}} \mathrm{Hom}_A(M', \mathrm{Hom}_A(N,P)) \longrightarrow 0$$

but from Proposition 2.34, so is

$$\mathrm{Hom}_A(M'' \otimes_A N, P) \longrightarrow \mathrm{Hom}_A(M \otimes_A N, P) \longrightarrow \mathrm{Hom}_A(M' \otimes_A N, P) \longrightarrow 0$$

Since the above sequence is exact for all modules P, we have the desired conclusion. ■

The tensor product is not left exact. Conider the sequence of $\mathbb{Z}$-modules

$$0 \hookrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z}$$

where $f(m) = 2m$. Upon tensoring with $\mathbb{Z}/2\mathbb{Z}$, we get the sequence

$$0 \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \xrightarrow{f\otimes 1} \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$$

Note that

$$(f \otimes 1)(m \otimes \overline{n}) = 2m \otimes \overline{n} = m \otimes (2\overline{n}) = m \otimes 0 = 0$$

Therefore, the sequence cannot be exact.

Theorem 2.36. *There is a natural isomorphism*

$$(M \otimes_A B) \otimes_B (M' \otimes_A B) \cong (M \otimes_A M') \otimes_A B.$$

Proof. Note that the functor $(- \otimes_A B) \otimes_B (M' \otimes_A B)$ is right exact, since it is a composition of tensor products. First, note that the isomorphism is obvious when M is a free module. Now suppose M were arbitrary. Then, we have an exact sequence

$$\bigoplus_{j\in J} A \longrightarrow \bigoplus_{j\in J} A \longrightarrow M \longrightarrow 0.$$

Denote by $F' = \bigoplus_{j\in J} A$ and $F = \bigoplus_{i\in I} A$. Let

$$\theta_M : (M \otimes_A B) \otimes_B (M' \otimes_A B) \to (M \otimes_A M') \otimes_A B.$$

We have shown above that θ_M is an isomorphism whenever M is a free module. In particular, we have a commutative diagram with exact rows.

$$\begin{array}{ccccccc}
(F' \otimes_A B) \otimes_B (M' \otimes_A B) & \longrightarrow & (F \otimes_A B) \otimes_B (M' \otimes_A B) & \longrightarrow & (M \otimes_A B) \otimes_B (M' \otimes_A B) & \longrightarrow & 0 \\
\downarrow \cong & & \downarrow \cong & & \downarrow \theta_M & & \| \\
(F' \otimes_A M') \otimes_A B & \longrightarrow & (F \otimes_A M') \otimes_A B & \longrightarrow & (M \otimes_A M') \otimes_A B & \longrightarrow & 0
\end{array}$$

Conclude using the five lemma. ■

Theorem 2.37. *Let $\phi : A \to B$ be a ring homomorphism. Let M be an A-module and N a B-module. Note that N is also an A-module owing to the restriction of scalars. Then, there is a natural isomorphism*

$$(M \otimes_A B) \otimes_B N \xrightarrow{\sim} M \otimes_A N$$

of B-modules.

Proof. Easy proof using universal properties. ■

More generally, the following is true.

Theorem 2.38. *Let M be an A-module, P a B-module and N an (A,B)-bimodule. Then, $M \otimes_A N$ is naturally a B-module, $N \otimes_B P$ an A-module and there is an natural isomorphism of (A,B)-bimodules:*

$$(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P).$$

Proof. ■

As an application, we have the following.

Proposition 2.39. *Let A be a local ring and M, N finitely generated A-modules. Then, $M \otimes_A N = 0$ if and only if $M = 0$ or $N = 0$.*

Proof. Let k denote the residue field of A. Then,

$$\begin{aligned}(M \otimes_A k) \otimes_k (k \otimes_A N) &\cong ((M \otimes_A k) \otimes_k k) \otimes_A N \cong (M \otimes_A (k \otimes_k k)) \otimes_A N \cong (M \otimes_A k) \otimes_A N \\ &\cong (k \otimes_A M) \otimes_A N \cong k \otimes_A (M \otimes_A N) = 0.\end{aligned}$$

But a tensor product of vector spaces is 0 if and only if one of the two vector spaces is 0. Hence, either $M \otimes_A k = 0$ or $N \otimes_A k = 0$, whence, it follows from Lemma 2.17, that $M = 0$ or $N = 0$. ■

2.8 Flat Modules

Definition 2.40 (Flat Module). An A-module M is said to be flat if the functor $- \otimes_A N$ is exact.

We know that $- \otimes_A N$ is right exact, hence, it suffices to show that the functor is left exact.

Theorem 2.41. *Let N be a A-module. Then, the following are equivalent*

(a) N is flat

(b) If $0 \to M' \to M \to M'' \to 0$ is an exact sequence of A-modules, then the tensored sequence

$$0 \longrightarrow M' \otimes_A N \xrightarrow{f \otimes 1} M \otimes_A N \xrightarrow{g \otimes 1} M'' \otimes_A N \longrightarrow 0$$

is exact.

(c) If $f : M' \to M$ is injective, then $f \otimes 1 : M' \otimes N \to M \otimes N$ is injective

(d) If $f : M' \to M$ is injective and M, M' are finitely generated, then $f \otimes_A 1 : M' \otimes_A N \to M \otimes_A N$ is injective.

Proof.

$(a) \iff (b)$**:** Is well known.

$(b) \implies (c)$**:** Immediate from considering the short exact sequence $0 \to M' \to M \to M/M' \to 0$.

$(c) \implies (b)$**:** Since $- \otimes_A N$ is known to be right exact as well.

TODO: Complete this later

■

Proposition 2.42. *Let $\{M_i\}_{i\in I}$ be a collection of A-modules. Then, $M = \bigoplus_{i\in I} M_i$ is flat if and only if M_i is flat for each $i \in I$.*

Proof. From the fact that

$$M \otimes_A N \cong \bigoplus_{i\in I} (M_i \otimes_A N)$$

and the isomorphism is natural. ■

Corollary 2.43. Free modules are flat.

Proof. Obviously, A is a flat A-module, therefore, $\bigoplus_{\lambda\in\Lambda} A$ is free for every indexing set Λ. ■

Proposition 2.44. *Let B be an A-algebra and M a flat A-module. Then, $M \otimes_A B$ is a flat B-module.*

Proof. Follows from the natural isomorphism $(M \otimes_A B) \otimes_B N \cong M \otimes_A N$. ■

Lemma 2.45. *The following are equivalent.*

(a) *M is flat.*

(b) $\operatorname{Tor}_i^A(N, M) = 0$ *for all* $i > 0$ *and all A-modules N. Equivalently,* $\operatorname{Tor}_i^A(M, N) = 0$ *for all* $i > 0$ *and all A-modules N.*

(c) $\operatorname{Tor}_1^A(N, M) = 0$ *for all A-modules N. Equivalently,* $\operatorname{Tor}_1^A(M, N) = 0$ *for all A-modules N.*

(d) $\operatorname{Tor}_1^A(N, M) = 0$ *for all finitely generated A-modules N. Equivalently,* $\operatorname{Tor}_1^A(M, N) = 0$ *for all finitely generated A-modules N.*

The equivalent statements follow from the balancing property of Tor.

Proof. $(a) \implies (b)$ is immediate from the definition of Tor while $(b) \implies (c)$ and $(c) \implies (d)$ is something a third grader could figure out. It remains to show that $(c) \implies (a)$. Let N and N' be finitely generated A-modules and $f : N' \to N$ an injective homomorphism. Then, there is a short exact sequence

$$0 \hookrightarrow N' \xrightarrow{f} N \longrightarrow \operatorname{coker} f \twoheadrightarrow 0.$$

This sequence gives rise to a Tor long exact sequence

$$\operatorname{Tor}_1^A(N', M) \to \operatorname{Tor}_1^A(N, M) \to \operatorname{Tor}_1^A(\operatorname{coker} f, M) \to N' \otimes_A M \to N \otimes_A M \to \operatorname{coker} f \otimes_A M \to 0.$$

Since N and N' are finitely generated, so is $\operatorname{coker} f$, whence we have a an exact sequence

$$0 \to N' \otimes_A M \to N \otimes_A M \to \operatorname{coker} f \otimes_A M \to 0.$$

In particular, this means that $N' \otimes_A M \to N \otimes_A M$ is injective and M is flat. ■

Lemma 2.46. *If $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of A-modules with M'' flat, then M' is flat if and only if M is flat.*

Proof. Again, using the Tor long exact sequence, we have

$$\cdots \to \operatorname{Tor}_n^A(N', M) \to \operatorname{Tor}_n^A(N, M) \to 0 \to \operatorname{Tor}_{n-1}^A(N', M) \to \operatorname{Tor}_{n-1}^A(N, M) \to 0 \to \cdots .$$

The conclusion is now obvious. ■

Lemma 2.47. *M is flat if and only if $\operatorname{Tor}_1^A(N, M) = 0$ for every cyclic A-module N, equivalently, $\operatorname{Tor}_1^A(M, N) = 0$ for every cyclic A-module N.*

Proof. The forward direction is clear. We shall prove the converse. Let N be a finitely generated A-module, say generated by $\{x_1, \ldots, x_n\}$. Let N_i denote the submodule generated by $\{x_1, \ldots, x_i\}$ for $1 \le i \le n$. We have a short exact sequence

$$0 \longrightarrow N_i \longrightarrow N_{i+1} \longrightarrow N_{i+1}/N_i \longrightarrow 0.$$

Note that N_1 is cyclic and thus, $\operatorname{Tor}_1^A(N_1, M) = 0$. We shall inductively show that $\operatorname{Tor}_1^A(N_i, M) = 0$. The induction step follows from the Tor long exact sequence, since

$$\begin{array}{ccccc} \operatorname{Tor}_1^A(N_i, M) & \longrightarrow & \operatorname{Tor}_1^A(N_{i+1}, M) & \longrightarrow & \operatorname{Tor}_1^A(N_{i+1}/N_i, M) \\ \| & & & & \| \\ 0 & \longrightarrow & ? & \longrightarrow & 0 \end{array}$$

and thus $\operatorname{Tor}_1^A(N_{i+1}, M) = 0$. In particular,

$$\operatorname{Tor}_1^A(N, M) = \operatorname{Tor}_1^A(N_n, M) = 0.$$

This completes the proof. ■

Corollary 2.48. M is flat if and only if $\operatorname{Tor}_1^A(A/\mathfrak{a}, M) = 0$ for every ideal $\mathfrak{a} \trianglelefteq A$. Equivalently, $\operatorname{Tor}_1^A(M, A/\mathfrak{a}) = 0$ for every ideal $\mathfrak{a} \trianglelefteq A$.

Proof. Every cyclic A-module is isomorphic to $A/\mathfrak{a}$ as A-modules for some ideal $\mathfrak{a} \trianglelefteq A$. ■

Lemma 2.49. *M is flat if and only if $\operatorname{Tor}_1^A(A/\mathfrak{a}, M) = 0$ for every finitely generated ideal $\mathfrak{a} \trianglelefteq A$. Equivalently, $\operatorname{Tor}_1^A(M, A/\mathfrak{a}) = 0$ for every finitely genrated ideal $\mathfrak{a} \trianglelefteq A$.*

Proof. We shall show that for any A-module M, $\operatorname{Tor}_1^A(A/\mathfrak{a}, M) = 0$ for every finitely generated ideal $\mathfrak{a}$ is equivalent to $\operatorname{Tor}_1^A(A/\mathfrak{a}, M) = 0$ for every ideal $\mathfrak{a}$.

To see this, note that $\operatorname{Tor}_1^A(A/\mathfrak{a}, M) = 0$ if and only if the sequence

$$0 \longrightarrow \mathfrak{a} \otimes_A M \longrightarrow A \otimes_A M$$

is exact, where this equivalence follows from the Tor long exact sequence. . ■

complete this

Proposition 2.50. *Suppose M'' is a flat A-module and*

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

is a short exact sequence. If N is any A-module, then

$$0 \longrightarrow M' \otimes_A N \xrightarrow{f\otimes 1} M \otimes_A N \xrightarrow{g\otimes 1} M'' \otimes_A N \longrightarrow 0$$

is exact.

Proof 1. The short proof is to consider the tail of the Tor long exact sequence.

$$\cdots \to \mathrm{Tor}_1^A(M'', N) \to M' \otimes_A N \to M \otimes_A N \to M'' \otimes_A N \to 0.$$

Since M'' is flat, $\mathrm{Tor}_1^A(M'', N) = 0$ and the conclusion follows. ■

Proof 2. This is a beautiful proof using the Snake Lemma. Let F be a free module that surjects onto N with kernel N'. Then, we have a short exact sequence

$$0 \longrightarrow N' \longrightarrow F \longrightarrow N \longrightarrow 0.$$

We can now construct the following commutative diagram

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

The snake lemma gives an exact sequence ■

Lemma 2.51. *A finitely presented flat module over a local ring is free.*

Proof. Let M be a finitely presented (and therefeore, finitely generated) flat module over a local ring $(A, \mathfrak{m}, k)$. Let $x_1, \ldots, x_n \in M$ be such that $\overline{x}_1, \ldots, \overline{x}_n \in M/\mathfrak{m}M$ form a basis as a k-vector space. As we have seen earlier, $x_1, \ldots, x_n$ then generate M as an A-module. Let $F = A^{\oplus n}$ and $\varphi : F \twoheadrightarrow M$ denote the surjection that maps the i-th basis element of F to x_i. Then, $\ker\varphi$ is finitely generated due to Proposition 2.72. We have a short exact sequence

$$0 \longrightarrow \ker\varphi \longrightarrow F \xrightarrow{\varphi} M \longrightarrow 0.$$

Tensoring with k and invoking Proposition 2.50, we have

$$0 \longrightarrow \ker\varphi \otimes_A k \longrightarrow F \otimes_A k \longrightarrow M \otimes_A k \longrightarrow 0$$

is exact. But note that $F \otimes_A k \longrightarrow M \otimes_A k$ is a surjection of vector spaces of the same dimension. Therefore, an isomorphism of k-vector spaces, consequently, also an isomorphism of A-modules. In particular, this means that $\ker\varphi \otimes_A k = 0$. Finally, due to Lemma 2.17, $\ker\varphi = 0$ and $F \cong M$. This completes the proof. ■

Definition 2.52. A ring A is said to be *von Neumann regular* or *absolutely flat* if every A-module is flat.

Theorem 2.53. *The following are equivalent*

(a) *A is absolutely flat.*

(b) *Every principal ideal in A is idempotent.*

(c) *Every finitely generated ideal in A is a direct summand of A as A-modules.*

Proof. ■

Proposition 2.54. *A local ring is absolutely flat if and only if it is a field.*

Proof. Let $(A, \mathfrak{m}, k)$ be local and absolutely flat. Then, there is a short exact sequence

$$0 \to \mathfrak{m} \to A \to A/\mathfrak{m} \to 0.$$

Since $A/\mathfrak{m}$ is a flat A-module, we may tensor to obtain the short exact sequence

$$0 \to \mathfrak{m} \otimes_A A/\mathfrak{m} \to A \otimes_A A/\mathfrak{m} \to A/\mathfrak{m} \otimes_A A/\mathfrak{m} \to 0.$$

Note that $A/\mathfrak{m} \otimes_A A/\mathfrak{m} = A/\mathfrak{m}$ as A-modules and hence,

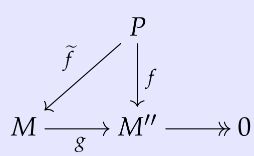
$$0 \to m \otimes_A A/\mathfrak{m} \to A/\mathfrak{m} \to A/\mathfrak{m} \to 0$$

is exact whence $m \otimes_A A/\mathfrak{m} = 0$, consequently, $m = 0$ due to Lemma 2.17. ■

2.9 Projective Modules

Theorem 2.55. *For an A-module P, the following are equivalent:*

(a) *Every map $f : P \to M''$ can be lifted to $\widetilde{f} : P \to M$ in the following commutative diagram:*



(b) *Every short exact sequence $0 \to M' \to M \to P \to 0$ splits*

(c) *There is a module M such that $P \oplus M$ is free*

(d) *The functor $\operatorname{Hom}_A(P, -)$ is exact.*

Proof.

$(a) \implies (b)$**:** Taking $M'' = P$ and $f = \mathbf{id}_P$, we have the desired conclusion.

$(b) \implies (c)$**:** Let F denote the free module on the set P. Then, the map $\Phi : F \to P$ given by $\Phi(e_x) = x$ for all $x \in P$ is a surjective A-module homomorphism. We have the following short exact sequence:

$$0 \to \ker \Phi \xrightarrow{\iota} F \xrightarrow{\Phi} P \to 0$$

This is known to split and thus, $F = \psi(P) \oplus \ker \Phi$ where $\psi : P \to F$ is the section.

$(c) \implies (d)$**:** Let $M' \to M \to M''$ be an exact sequence of modules and K be an A-module such that $P \oplus K = F \cong A^{\Lambda}$. Then, the induced sequence

$$\prod_{\lambda\in\Lambda} M' \to \prod_{\lambda\in\Lambda} M \to \prod_{\lambda\in\Lambda} M''$$

is exact. We have seen that there is a natural isomorphism $\mathrm{Hom}_A(A, M) \xrightarrow{\sim} M$, consequently, there is a natural isomorphism

$$\mathrm{Hom}_A(A^{\oplus\Lambda}, M) \xrightarrow{\sim} \prod_{\lambda\in\Lambda} M$$

whence it follows that the sequence

$$\mathrm{Hom}_A(A^{\oplus\Lambda}A, M') \to \mathrm{Hom}_A(A^{\oplus\Lambda}A, M) \to \mathrm{Hom}_A(A^{\oplus\Lambda}, M'')$$

But since $\mathrm{Hom}_A(A^{\oplus\Lambda}, M) \cong \mathrm{Hom}_A(P, M) \oplus \mathrm{Hom}_A(K, M)$, we have the desired conclusion.

$(d) \implies (a)$**:** Trivial.

■

Definition 2.56 (Projective Module). An A-module P satisfying any one of the four equivalent conditions of Theorem 2.55 is said to be a *projective A-module*.

In particular, from Theorem 2.55(c), we see that every free module is projective.

Lemma 2.57. *A finitely generated projective module P over a local ring $(A, \mathfrak{m})$ is free.*

Proof. Let $\{\overline{x}_1, \dots, \overline{x}_n\}$ be a basis for $M/\mathfrak{m}M$ as a k-vector space where $k = A/\mathfrak{m}$. As we have seen earlier, $\{x_1, \dots, x_n\}$ generates M. Let F be the free module with basis $\{e_1, \dots, e_n\}$ and $\Phi : F \to M$ be the module homomorphism given by $\Phi(e_i) = x_i$ and $K = \ker\Phi$. Since M is projective, there is a module homomorphism $\psi : M \to F$ satisfying $\Phi \circ \psi = \mathbf{id}_M$ and $F = K \oplus \psi(M)$.

We contend that $K = \mathfrak{m}K$. Indeed, let $x \in K$, then $x = \sum r_i e_i$ for a unique choice $\{r_1, \dots, r_n\}$. Then, $\sum r_i x_i = 0$, consequently, $r_i \in \mathfrak{m}$ for all i. Since $F = K \oplus \psi(M)$, we may write $e_i = u_i + v_i$ for some $u_i \in K$ and $v_i \in \psi(M)$. As a result,

$$x - \sum r_i u_i = \sum r_i v_i \in \ker\Phi \cap \psi(M) = \{0\}$$

and the conclusion follows.

Finally due to Lemma 2.17, we must have that $K = 0$ whence M is free. ■

Proposition 2.58. *Projective modules are flat.*

Proof. Follows from the fact that free modules are flat and projective modules are direct summands of free modules. ■

Theorem 2.59. *Let I denote the unit interval and $A = C(I)$, the ring of real valued continuous functions on I. Let M denote the A-module of continuous functions that vanish in a neighborhood of zero. Then, M is a projective A-module.*

Proof. Consider the functions $r_i : I \to \mathbb{R}$ given by

$$r_i(x) = \begin{cases} 0 & 0 \le x \le \frac{1}{2^i} \\ 2^i x - 1 & \frac{1}{2^i} \le x \le \frac{1}{2^{i-1}} \\ 1 & x \ge \frac{1}{2^{i-1}} \end{cases}.$$

For any $f \in M$, there is a sufficiently large i such that $r_i f = f$. Define the map $\Phi : M \to \bigoplus_{i=1}^{\infty} A$ by

$$\Phi(f) = \big((1 - r_{i-1})f\big)_{i \in \mathbb{N}}.$$

For sufficiently large i, $(1 - r_{i-1})f = 0$. Now, define $\Psi : \bigoplus_{i=1}^{\infty} A \to M$ by

$$\Psi((a_i)_{i \in \mathbb{N}}) = \sum_{i=1}^{\infty} r_i a_i.$$

For $f \in M$, we have

$$\Psi \circ \Phi(f) = \sum_{i=1}^{\infty} r_i(1 - r_{i-1})f = \sum_{i=1}^{\infty} (r_i - r_{i-1})f = f.$$

The last equality follows from the fact the sum was essentially finite. In particular, this means that M is a direct summand of a free module which completes the roof. ■

Remark 2.9.1. *It is also true that M is not a free A-module. I do not know of an elementary proof yet.*

2.10 Injective Modules

Theorem 2.60 (Baer's Criterion). *Let Q be an A-module. Then Q is injective if and only if for every ideal $\mathfrak{a}$ of A, every A-module homomorphism $f : \mathfrak{a} \to Q$ can be extended to an A-module homomorphism $\widetilde{f} : A \to Q$.*

Proof. ($\Longrightarrow$) Trivial.

($\Longleftarrow$) Let $M \subseteq N$ be A-modules. It suffices to show that every A-module homomorphism $f : M \to Q$ can be extended to an A-module homomorphism $f : N \to Q$. We shall first show that given $x \in N \backslash M$, the map f can be extended to a map $f' : M + (x) \to Q$. Indeed, let $\mathfrak{a} = (M : x)$. Consider the map $g : \mathfrak{a} \to Q$ given by $g(a) = f(ax)$. This is obviously an A-module homomorphism and according to the hypothesis, can be extended to an A-module homomorphism $\widetilde{g} : A \to Q$. Using this, we may define

$$f'(m + ax) = f(m) + \widetilde{g}(x) \; \forall a \in A.$$

It is straightforward to check that this is an A-module homomorphism which extends f.

Now, let $(\Sigma, \leqq)$ denote the poset of maps $\phi : M' \to Q$ where $M \le M' \le N$ are A-modules with the relation $\phi \leqq \psi$ if ψ is an extension of ϕ. It is not hard to argue that every chain in Σ has an upper bound. Thus, due to Zorn, there is a maximal element $\widetilde{f} : M' \to Q$ for some $M \le M' \le N$. If $M' \ne N$, then by choosing some $x \in N \backslash M'$, we may extend the map $\widetilde{f}$ to a map from $M' + (x)$ to Q, a contradiction. This completes the proof. ■

Proposition 2.61. *Let R be a PID. Then, M is an injective R-module if and only if it is divisible.*

Proof. Suppose M is injective. Let $a \in A \backslash \{0\}$ and $x \in M$. Then, the map $f : (a) \to M$ which maps $a \mapsto x$ can be extended to a map from A to M. If $f(1) = y$, then $ay = x$ whence M is divisible.

Conversely, if M is divisible, then given any map $f : (a) \to M$, if $f(a) = x$, then there is $y \in M$ such that $ay = M$. Now, the map $\widetilde{f} : A \to M$ given by $f(1) = y$ extends f whereby M is injective. This completes the proof. ■

2.11 Essential Extensions and Injective Hull

I'll add the theory later. First, an application.

Add theory about essential extensions

Theorem 2.62 (Schröder-Bernstein for Injective Modules). *Let R be a possibly non-commutative ring and M, N injective R-modules. If there are R-linear injections $f : M \hookrightarrow N$ and $g : N \hookrightarrow M$, then $M \cong N$.*

Proof. We may treat N as a submodule of M. Using injectivity of N, there is a submodule X of M such that $M = N \oplus X$. Let X_n denote the set $f^n(X)$ and $L = \bigoplus_{n=0}^{\infty} X_n$. Consider the map $\Phi : L \to M$ given by

$$\Phi(x_0, x_1, \dots) = \sum_{i=0}^{\infty} x_i.$$

We contend that Φ is injective. Indeed, suppose $(x_i) \in \ker \Phi$. Then, there is some positive integer n such that $x_j = 0$ for all $j > n$ and

$$x_0 + f(x_1) + \cdots + f^n(x_n) = 0.$$

Therefore, $x_0 \in \text{im}(f) \subseteq N$ whence $x_0 = 0$, consequently, $x_1 + f(x_2) + \cdots + f^{n-1}(x_n) = 0$, since f is an injection. Working inductively, we see that $x_i = 0$ for all i and Φ is injective.

We may now suppose that L is embedded inside M through the injection Φ. Since $f(L) \subseteq N$, there is an injective hull E of $f(L)$ that is contained inside N. Since E is injective, there is a submodule Y of N such that $N = E \oplus Y$.

We have

$$E(L) \cong E(X \oplus f(L)) \cong E(X) \oplus E(f(L)) \cong X \oplus E.$$

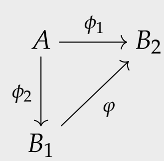
Recall that f is an injection and thus, $E(L) \cong E(f(L)) \cong E$. Henc, $E \cong X \oplus E$. This gives us

$$M \cong N \oplus X \cong Y \oplus E \oplus X \cong Y \oplus E \cong N.$$

This completes the proof. ∎

2.12 Algebras

Definition 2.63. An *A-algebra* is a ring homomorphism $\phi : A \to B$. This endows B with the structure of an A-module. The algebra is said to be of *finite type* if B is finitely generated as an A-module. A homomorphism between algebras (ϕ_1, B_1) and (ϕ_2, B_2) is a map $\varphi : B_1 \to B_2$ making the following diagram commute.



This gives rise to a locally small category $A - \textbf{Alg}$ with morphisms as defined above.

An A-algebra B is said to be **finite** if it is finitely generated as an A-module. On the other hand, it is said to be **finitely generated** or of **finite type** if it is the homomorphic image of a polynomial ring $A[x_1, \dots, x_n]$ for some positive integer n.

Proposition 2.64. *If C is a finite B-algebra and B is a finite A-algebra, then C is a finite A-algebra.*

Proposition 2.65. *If C is a B-algebra of finite type and B is an A-algebra of finite type, then C is an A-algebra of finite type.*

Proof. There is a surjective ring homomorphism $\varphi : A[x_1, \ldots, x_n] \to B$ and a surjective ring homomorphism $\psi : B[y_1, \ldots, y_m] \to C$. It is not hard to see that there is a surjective ring homomorphism $\Phi : A[x_1, \ldots, x_n, y_1, \ldots, y_m] \to C$ thereby completing the proof. ■

2.12.1 Tensor Product of Algebras

Consider the two A-algebras $f : A \to B$ and $f : A \to C$. Then, the map

$$\mu : B \times C \times B \times C \to B \otimes_A C$$

given by $\mu(b, c, b', c') = bb' \otimes cc'$ is A-multilinear, whereby it induces a map

$$\mu' : B \otimes_A C \otimes_A B \otimes_A C \to B \otimes_A C$$

given by $\mu'(b \otimes c \otimes b' \otimes c') = bb' \otimes cc'$. Let $D = B \otimes_A C$. Then, we have $\mu' : D \otimes_A D \to D$ given by $\mu'(b \otimes c, b' \otimes c') = bb' \otimes cc'$.

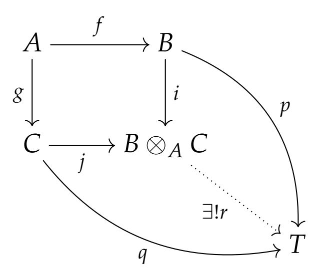
Let $\varphi : D \times D \to D \otimes_A D$ be the natural map. Then, the composition $\cdot = \mu' \circ \varphi : D \times D \to D$ is given by

$$(b \otimes c) \cdot (b' \otimes c') = bb' \otimes cc'$$

We contend that $(D \otimes_A D, +, \cdot, 0 \otimes 0, 1 \otimes 1)$ is a ring. To do this, we need only verify that multiplication distributes over addition. Indeed,

$$\begin{aligned}(b \otimes c) \cdot (b' \otimes c' + b'' \otimes c'') &= \mu' \left((b \otimes c) \otimes (b' \otimes c' + b'' \otimes c'')\right) \\ &= \mu'((b \otimes c \otimes b' \otimes c') + (b \otimes c \otimes b'' \otimes c'')) \\ &= bb' \otimes cc' + bb'' \otimes cc''\end{aligned}$$

Let $i : B \to B \otimes_A C$ be the map $b \mapsto b \otimes 1$ and $j : C \to B \otimes_A C$ be the map $c \mapsto 1 \otimes c$. Then the square in the following diagram commutes.



Let T be an A-algebra with A-algebra morphisms $p : B \to T$ and $q : C \to T$. We contend that there is a unique A-algebra morphism $r : B \otimes_A C \to T$ making the above diagram commute.

To construct the map r, consider the multilinear map $\Phi : B \times C \to T$ given by $\Phi(b, c) = p(b)q(c)$. This induces a map $r : B \otimes_A C \to T$ given by

$$r(b \otimes c) = p(b)q(c).$$

This map obviously makes the diagram commute. It remains to show that r is indeed an A-algebra morphism, for which, it suffices to show that it is a ring homomorphism. Indeed,

$$r((b \otimes c)(b' \otimes c')) = r(bb' \otimes cc') = p(bb')q(cc') = p(b)q(c)p(b')q(c') = r(b \otimes c)r(b' \otimes c').$$

Hence, the tensor tensor product is a *coproduct* in the category of A-algebras.

2.13 Structure Theorem for Modules over a PID

Throughout this section, let R be a PID.

Lemma 2.66. *A finitely generated torsion free R-module is free.*

Proof. Let M be a finitely generated torsion free R-module. Let $\{x_1, \ldots, x_m\}$ be a set of generators. Pick a maximal linearly independent subset $\{v_1, \ldots, v_n\}$ of $\{x_1, \ldots, x_m\}$. Then, for each x_i, there is a linear combination

$$a_i x_i + b_1 v_1 + \cdots + b_n v_n = 0$$

with $a_i \neq 0$ due to the maximality of $\{v_1, \ldots, v_n\}$. Therefore, $a_i x_i \in (v_1, \ldots, v_n) = (v_1) \oplus \cdots \oplus (v_n)$. Let $a = a_1 \cdots a_m$. Then, the map $\phi : M \to (v_1, \ldots, v_n)$ given by $\phi(m) = am$ is an injective map. Thus, M is isomorphic to a submodule of $(v_1, \ldots, v_n)$. But note that

$$(v_1, \ldots, v_n) = (v_1) \oplus \cdots \oplus (v_n)$$

is a free module and hence so is M. ∎

The statement is no longer true upon dropping the finitely generated condition, for example, $\mathbb{Q}$ as a $\mathbb{Z}$-module is not free but is torsion free.

Definition 2.67. Let E be an R-module. For $x \in E$, an element $r \in R$ such that $\text{Ann}_R(x) = (r)$ is said to be a *period* of x. An element $c \in R$ is said to be an *exponent* for E (resp. for x) if $cE = 0$ (resp. $cx = 0$). The elements $x_1, \ldots, x_n \in E$ are said to be *independent* if

$$(x_i) \cap (x_1, \ldots, \widehat{x_i}, \ldots, x_n) = 0$$

In this case, $(x_1, \ldots, x_n) = (x_1) \oplus \cdots \oplus (x_n)$.

Remark 2.13.1. *In order to show that $x_1, \ldots, x_n$ are independent, it suffices to show that given any linear combination $a_1 x_1 + \cdots + a_n x_n = 0$, we must have $a_i x_i = 0$ for all $1 \leq i \leq n$. Further note that the notion of independence is not the same as that of linear independence. That is, we may have an independent set which is not linearly independent, for each element in the set may be torsion.*

The following lemma essentially states that it is possible to lift an independent set in a quotient module to the original module.

Lemma 2.68 (Lifting Lemma). *Let E be a torsion module with exponent p^r for some prime $p \in R$ and $x_1 \in E$ be an element of period p^r. Let $\overline{E} = E/(x_1)$ and $\overline{y}_1, \ldots, \overline{y}_m$ be independent elements of $\overline{E}$. Then for each $1 \leq i \leq m$, there is a representative $y_i \in E$ of $\overline{y}_i$ such that the period of y_i is same as the period of $\overline{y}_i$. Further, $x_1, y_1, \ldots, y_m$ are independent.*

Proof. Let $\overline{y} \in \overline{E}$, then, $\text{Ann}(\overline{y}) \supseteq \text{Ann}(\overline{E}) \supseteq (p^r)$ whereby, $\text{Ann}(y) = (p^n)$ for some $n \leq r$. Thus, $p^n y \in (x_1)$ whence there is $p^s c \in R$ with $p \nmid c$ such that $p^n y = p^s c x_1$. Now, $p^s c x_1$ has period p^{r-s} and thus y has period p^{n+r-s}. This immediately implies that $n + r - s \leq s$ and equivalently $n \leq s$. Consider now the element $z = y - p^{s-n} c x_1$. This is a representative for $\overline{y}$ and its period is p^n. This shows that we may lift the y_i's to E.

Finally, we must show that the liftings are independent. Indeed, suppose

$$a x_1 + a_1 y_1 + \cdots + a_m y_m = 0$$

then moving to $\overline{E}$, we have $a_1 \overline{y}_1 + \cdots + a_m \overline{y}_m = 0$ but since $\overline{y}_1, \ldots, \overline{y}_m$ are independent, $a_i \overline{y}_i = 0$ for each $1 \leq i \leq m$. Now, if p^{r_i} is the period of $\overline{y}_i$ (we have argued earlier that this must be a power of p) and consequently, $p^{r_i} \mid a_i$. This immediately implies that $a_i y_i = 0$ and thus $a x_1 = 0$, which completes the proof. ∎

Let E be a finitely generated torsion module. For a prime $p \in R$, define

$$E[p] = \{x \in E \mid \exists n \in \mathbb{N},\ p^n x = 0\}$$

That this is a submodule is easy to verify. Further, it is finitely generated since it is the submodule of a finitely generated module over a PID.

Let $\operatorname{Ann}(E) = (\alpha)$ where $\alpha = u p_1^{t_1} \cdots p_r^{t_r}$ where $u \in R^\times$.

Lemma 2.69.

$$E \cong \bigoplus_{i=1}^{r} E[p_i]$$

Proof. Let $q_i = \alpha / p_i^{t_i}$. Then, $(q_1, \dots, q_r) = 1$ and hence, there are $\gamma_1, \dots, \gamma_r \in R$ such that $\gamma_1 q_1 + \cdots + \gamma_r q_r = 1$. For any $x \in E$, we have

$$x = \gamma_1 q_1 x + \cdots + \gamma_r q_r x$$

where $\gamma_i q_i x \in E[p_i]$ for each i. Thus, $E = \sum_{i=1}^{r} E[p_i]$.

We shall now show that this sum is direct. Indeed, suppose $x_i \in E[p_i]$ such that $x_1 + \cdots + x_r = 0$. Multiplying this equation by q_i, we have $q_i x_i = 0$, consequently, $\operatorname{Ann}(x_i) \supseteq (p_i^{t_i}, q_i) = (1)$, that is, $x_i = 0$ for each i. This completes the proof. ■

Since $E[p]$ is finitely generated, we may let $E = E[p]$ henceforth. Since $E[p]$ is finitely generated, take a generating set $\{x_1, \dots, x_n\}$. Since $(p^m) \subseteq \operatorname{Ann}(x_i)$ for some $m \in \mathbb{N}$, we must have $\operatorname{Ann}(x_i) = (p^{n_i})$ for some n_i. As a result,

$$\operatorname{Ann}(E) \supseteq \bigcap_{i=1}^{r} \operatorname{Ann}(x_i) \neq 0$$

whence $\operatorname{Ann}(E) = (p^n)$ for some positive integer n. We shall now show that E has a decomposition. Let $\mathfrak{M}(E)$ denote the minimum cardinality of a generating set of E. Obviously this exists since E has at least one generating set.

Let $x_1 \in E$ be an element in a generating set with cardinality $\mathfrak{M}(E)$ such that $\operatorname{Ann}(x_1)$ divides the annihilator ideal of every other element in the aforementioned generating set. This can be done because the generating set has finite cardinality.

Let $\overline{E} = E/(x_1)$. Obviously, $\mathfrak{M}(\overline{E}) < \mathfrak{M}(E)$ whereby, there is a decomposition $\overline{E} \cong (\overline{y}_1) \oplus \cdots \oplus (\overline{y}_m)$ with $(\overline{y}_i) \cong R/(p^{r_i})$. Due to the Lemma 2.68, there are corresponding elements $y_1, \dots, y_m \in E$ such that the period of y_i is that of $\overline{y}_i$, and $x_1, y_1, \dots, y_m$ are independent. This shows that the following short exact sequence spilts:

$$0 \to (x_1) \to E \to \overline{E} \to 0$$

whence $E \cong (x_1) \oplus (y_1) \oplus \cdots \oplus (y_m)$. This completes the proof of the existence of a decomposition.

2.13.1 The Jordan Canonical Form

Let k be an algebraically closed field

2.14 Finitely Presented Modules

I need to place this section somewhere nice.

Definition 2.70 (Finitely Presented). An A-module M is said to be finitely presented if there are positive integers m and n and an exact sequence $A^m \to A^n \to M \to 0$.

Obviously, every finitely presented module is finitely generated. Further, if A is a *noethering*, then an A-module is finitely generated if and only if it is finitely presented.

Proposition 2.71. *If M is finitely presented, then for every A-module N and multiplicative subset S of A,*

$$S^{-1}\operatorname{Hom}_A(M,N) \cong \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N)$$

Proof. There is a natural map $T : S^{-1}\operatorname{Hom}_A(M,N) \to \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N)$ given by $(\phi/s)(m/t) = \phi(m)/st$. We shall show that this map is an isomorphism when M is finitely presented. To do so, we must first show that this is an isomorphism when $M = A^n$ for some positive integer n. Indeed, since localization commutes with direct sums, we have

$$S^{-1}\operatorname{Hom}_A(A^{\oplus n}, N) \cong S^{-1}\prod \operatorname{Hom}_A(A,N) \cong \prod \operatorname{Hom}_{S^{-1}A}(S^{-1}A, S^{-1}N) \cong \operatorname{Hom}_{S^{-1}A}(S^{-1}A^{\oplus n}, N).$$

Since M is finitely presented, we have an exact sequence $A^m \to A^n \to M \to 0$ for some positive integers m and n. We have a commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & S^{-1}\operatorname{Hom}_A(M,N) & \longrightarrow & S^{-1}\operatorname{Hom}_A(A^n,N) & \longrightarrow & S^{-1}\operatorname{Hom}_A(A^m,N) \\
\| & & \downarrow & & \downarrow\wr & & \downarrow\wr \\
0 & \longrightarrow & \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N) & \longrightarrow & \operatorname{Hom}_{S^{-1}A}(S^{-1}A^n, S^{-1}N) & \longrightarrow & \operatorname{Hom}_{S^{-1}A}(S^{-1}A^m, S^{-1}N)
\end{array}$$

and the conclusion follows from the five lemma (just add another column of zeros to the left). ■

Proposition 2.72. *Let N be finitely generated and M a finitely presented A-module. If $f : N \twoheadrightarrow M$ is a surjection, then* $\ker f$ *is finitely generated.*

Proof. Let $A^m \to A^n \to M \to 0$ be an exact sequence. Then, there is a commutative diagram

$$\begin{array}{ccccccccc}
 & & A^m & \longrightarrow & A^n & \longrightarrow & M & \longrightarrow & 0 \\
 & & \exists h \,\vdots & & \exists g\,\vdots & & \|\,\mathbf{id}_M & & \\
0 & \longrightarrow & \ker f & \longrightarrow & N & \xrightarrow[f]{} & M & \longrightarrow & 0
\end{array}$$

with exact rows. Since A^m and A^n are projective A-modules, the map $\mathbf{id}_M$ can be lifted to maps $g : A^n \to N$ and $h : A^m \to \ker f$. Due to the Snake Lemma, there is an exact sequence

$$0 = \ker \mathbf{id}_M \to \operatorname{coker} h \to \operatorname{coker} g \to \operatorname{coker} \mathbf{id}_M = 0$$

whence $\operatorname{coker} h \cong \operatorname{coker} g$. But since N is finitely generated, so is $\operatorname{coker} g$ and hence so is $\operatorname{coker} h$. Finally, we have an exact sequence

$$A^m \to \ker f \to \operatorname{coker} h$$

where A^m and $\operatorname{coker} h$ are finitely generated. Thus, $\ker f$ is finitely generated. ■

cite 2 out of 3 lemma

Chapter 3

Localization

3.1 Rings of Fractions

Define the relation $\sim_S$ on $A \times S$ by $(a,s) \sim_S (a',s')$ if there is $t \in S$ such that $t(s'a - sa') = 0$. That this is an equivalence relation is easy to verify. We shall use a/s to denote the equivalence class $[(a,s)]$ in $A \times S/\sim_S$.

Consider the operations:

$$\frac{a}{s} + \frac{a'}{s'} = \frac{s'a + sa'}{ss'} \qquad \frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}$$

It is not hard to see that these are well defined and endow $A \times S/\sim_S$ with a ring structure. We denote this ring by $S^{-1}A$ and is called the *ring of fractions* of A by S.

There is a natural ring homomorphism $\varphi : A \to S^{-1}A$ given by $\varphi(x) = x/1$. When A is an integral domain and $S = A \backslash \{0\}$, $S^{-1}A$ is precisely the field of fractions. Recall that if $\mathfrak{p}$ is a prime ideal in A, then $S = A \backslash \mathfrak{p}$ is a multiplicatively closed subset of A. We denote the ring $S^{-1}A$ by $A_\mathfrak{p}$.

Theorem 3.1. *The ring $A_\mathfrak{p}$ is local.*

Proof. Let $S = A \backslash \mathfrak{p}$ and define

$$\mathfrak{m} = \left\{ \frac{a}{s} \,\middle|\, a \in \mathfrak{p},\ s \in S \right\}$$

It is not hard to see that $\mathfrak{m}$ is an ideal in $A_\mathfrak{p}$. We contend that $\mathfrak{m}$ is the ideal of non-units in $A_\mathfrak{p}$. Indeed, if $a/s \in \mathfrak{m}$ is a unit, then there is $b/t \in A_\mathfrak{p}$ such that $(ab)/(st) = 1$, consequently, there is $w \in S$ such that $w(ab - st) = 0$, whence $wst \in \mathfrak{p}$, a contradiction.

On the other hand, if $a/s \notin \mathfrak{m}$, then a/s is a unit since $(a/s) \cdot (s/a) = 1$. Now, since the collection of all non-units forms an ideal, the ring must be local due to Proposition 1.7. ■

Proposition 3.2. *Let $\mathfrak{m}$ be the unique maximal ideal of $A_\mathfrak{p}$. Then, $A_\mathfrak{p}/\mathfrak{m} \cong Q(A/\mathfrak{p})$ where the latter is the field of fractions of $A/\mathfrak{p}$.*

Proof. TODO: Add in later ■

Similarly, when we let $S = \{a^n\}_{n \geq 0}$ for some $a \in A$, we denote $S^{-1}A$ by A_a.

There is a degenerate case, when we allow $0 \in S$, notice that the ring $S^{-1}A$ is the zero ring, since for all $a/s \in S^{-1}A$, we have $0(as) = 0$, therefore, $a/s = 0/s$.

Proposition 3.3. *Let $\{A_i\}_{i\in I}$ be a collection of commutative rings and $\{S_i \subseteq A_i\}$ be a collection of multiplicatively closed sets. Then,*

$$\left(\prod_{i\in I} S_i\right)^{-1}\left(\prod_{i\in I} A_i\right) \cong \prod_{i\in I}(S_i^{-1}A_i)$$

Proof. Define the map $\phi : \prod_{i\in I}(S_i^{-1}A_i) \to \left(\prod_{i\in I} S_i\right)^{-1}\left(\prod_{i\in I} A_i\right)$ given by

$$\phi\left(\left(\frac{a_i}{s_i}\right)_{i\in I}\right) = \frac{(a_i)_{i\in I}}{(s_i)_{i\in I}}$$

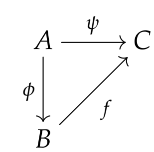
It is straightforward to argue that this map is well defined and surjective. We now contend that this is an isomorphism, for which it suffices to show that $\ker\phi$ is trivial. Indeed, if $(a_i/s_i)_{i\in I} \in \ker\phi$, then there is $(t_i)_{i\in I}$ such that $(t_ia_i)_{i\in I} = (0)_{i\in I}$ whereby, $t_ia_i = 0$ for each i and $a_i/s_i = 0$. This completes the proof. ∎

Corollary 3.4. Let $\{A_i\}$ be a collection of rings then every localization of $\prod_{i\in I} A_i$ is of the form $(A_i)_{\mathfrak{p}_i}$ for some $i \in I$ where $\mathfrak{p}_i \subseteq A_i$ is a prime ideal.

Proof. Follows from the fact that prime ideals in $\prod_{i\in I} A_i$ are of the form $\pi_i^{-1}(\mathfrak{p}_i)$ where $\mathfrak{p}_i$ is a prime ideal in A_i and $\pi : \prod_{i\in I} A_i \to A_i$ is the natural projection map. ∎

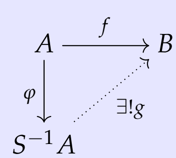
3.1.1 Universal Property

Fix a multiplicative subset $S \subseteq A$. Let $\mathscr{C}$ denote the category with objects as pairs (ϕ, B) where $\phi : A \to B$ is a ring homomorphism such that $\phi(s)$ is a unit in B for all $s \in S$. A morphism in this category is a map $f : (\phi, B) \to (\psi, C)$ making the following diagram commute.



The ring of fractions is an initial object in this category. Therefore, we have the following universal property. We shall verify in the "proof" that our construction of the field of fractions does satisfy this property and is therefore an initial object in $\mathscr{C}$.

Proposition 3.5. *Let $f : A \to B$ be a ring homomorphism such that $f(s)$ is a unit in B for all $s \in S$. Then there is a unique ring homomorphism $g : S^{-1}A \to B$ making the following diagram commute*



Proof. Define the map $g : S^{-1}A \to B$ by $g(a/s) = g(a)g(s)^{-1}$. To see that this map is well defined, note that if $a/s = a'/s'$, then there is $t \in S$ such that $t(s'a - sa') = 0$, consequently, $g(t)(g(s')g(a) - g(s)g(a')) = 0$. As a result, $g(a)g(s)^{-1} = g(a')g(s')^{-1}$. From this, it follows immediately that g is a ring homomorphism making the diagram commute.

As for uniqueness, note that for all $a/s \in S^{-1}A$,

$$g(a/s) = g(a/1)g(1/s) = g(a/1)g(s/1)^{-1} = f(a)f(s)^{-1}$$

which is fixed by the choice of f. This completes the proof. ∎

3.2 Modules of Fractions

Let M be an A-module and $S \subseteq A$ be a multiplicatively closed subset. Define the relation $\sim_S$ on $M \times S$ by $(m, s) \sim_S (m', s')$ if and only if there is $t \in S$ such that $t(s'm - sm') = 0$. That this is an equivalence relation is easy to verify. We shall use m/s to denote the equivalence class $[(m, s)]$ in $M \times S / \sim_S$.

As in the previous section, there is a natural A-module homomorphism $\varphi : M \to S^{-1}M$ given by $\varphi(m) = m/1$. This map is called the *localization map*.

It is not hard to see that $S^{-1}M$ forms an A-module. Further, it also has the structure of an $S^{-1}A$ module under the action

$$\frac{a}{s} \cdot \frac{m}{t} = \frac{a \cdot m}{st}$$

Let $f : M \to N$ be an A-module homomorphism. Consider the map $S^{-1}f : S^{-1}M \to S^{-1}N$ given by

$$S^{-1}f\left(\frac{m}{s}\right) = \frac{f(m)}{s}$$

We must first show that this is well defined. Indeed, if $m/s = m'/s'$, then there is $t \in S$ such that $t(s'm - sm') = 0$, consequently, $t(s'f(m) - sf(m')) = 0$, as a result, $f(m)/s = f(m')/s'$ in $S^{-1}M$.

We now contend that $S^{-1}f$ is an $S^{-1}A$ module homomorphism. Indeed, we have

$$S^{-1}f\left(\frac{m}{s} + \frac{a}{t}\frac{m'}{s'}\right) = S^{-1}f\left(\frac{ts'm + asm'}{sts'}\right) = \frac{f(ts'm + asm')}{sts'} = \frac{ts'f(m) + asf(m')}{sts'} = \frac{f(m)}{s} + \frac{f(m')}{s'}$$

Finally, let $f : M \to N$ and $g : N \to P$ be A-module homomorphisms. Then,

$$S^{-1}(g \circ f)\left(\frac{m}{s}\right) = \frac{g(f(m))}{s} \qquad S^{-1}g\left(S^{-1}f\left(\frac{m}{s}\right)\right) = S^{-1}g\left(\frac{f(m)}{s}\right) = \frac{g(f(m))}{s}$$

Theorem 3.6. *$S^{-1} : A - \mathbf{Mod} \to S^{-1}A - \mathbf{Mod}$ is an exact functor.*

Proof. Let $M' \xrightarrow{f} M \xrightarrow{g} M''$ be an exact sequence. Then, for any $m'/s' \in S^{-1}M'$, we have

$$S^{-1}g\left(S^{-1}f\left(\frac{m'}{s'}\right)\right) = S^{-1}g\left(\frac{f(m')}{s'}\right) = \frac{g(f(m'))}{s'} = 0$$

As a result, $\text{im}(S^{-1}f) \subseteq \ker(S^{-1}g)$. On the other hand, for $m/s \in \ker S^{-1}g$, we have $g(m)/s = 0$, consequently, there is $t \in S$ such that $tg(m) = 0$, equivalently, $g(tm) = 0$, whence, there is $m' \in M'$ such that $f(m') = tm$. Then, we have

$$f\left(\frac{m'}{st}\right) = \frac{f(m')}{st} = \frac{tm}{st} = \frac{m}{s}$$

whence, $\ker(S^{-1}g) \subseteq \text{im}(S^{-1}f)$. This completes the proof. ∎

Proposition 3.7. *Let $N, P, \{M_i\}_{i \in I}$ be submodules of an A-module M. Then, for a multiplicatively closed $S \subseteq M$,*

(a) $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$

(b) $S^{-1}\left(\sum_{i \in I} M_i\right) = \sum_{i \in I} S^{-1}M_i$

(c) $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$ *as* $S^{-1}A$ *modules.*

Proof. (a) We have the exact sequences $0 \to N \cap P \to N$ and $0 \to N \cap P \to P$. Due to Theorem 3.6, the sequences $0 \to S^{-1}(N \cap P) \to S^{-1}N$ and $0 \to S^{-1}(N \cap P) \to S^{-1}N$ are exact, consequently, $S^{-1}(N \cap P) \subseteq S^{-1}N \cap S^{-1}P$.

On the other hand, if $n/s = p/t$ for some $n \in N$, $p \in P$ and $s, t \in S$, there is some $u \in S$ such that $u(tn - sp) = 0$, equivalently, $m = utn = usp \in N \cap P$. Thus, $m/(stu) = n/s = p/t$, and the conclusion follows.

(b) Let $\overline{M} = \sum_{i \in I} M_i$. Then, there is the exact sequence $0 \to M_i \to \overline{M}$. Then, due to Theorem 3.6, the sequence $0 \to S^{-1}M_i \to S^{-1}\overline{M}$ is exact. Consequently, $\sum\limits_{i \in I} S^{-1}M_i \subseteq S^{-1}\overline{M}$.

On the other hand, any element in $S^{-1}\overline{M}$ is of the form $(m_{i_1} + \cdots + m_{i_n})/s = m_{i_1}/s + \cdots + m_{i_n}/s$ for some $m_{i_n} \in M_{i_n}$ and $s \in S$. The conclusion follows.

(c) Consider the short exact sequence $0 \to N \to M \to M/N \to 0$. Due to Theorem 3.6, we obtain the short exact sequence of $S^{-1}A$-modules $0 \to S^{-1}N \to S^{-1}M \to S^{-1}(M/N) \to 0$ whereby the conclusion follows.

■

Proposition 3.8. *Let* $S \subseteq A$ *be a multiplicative subset. Then, there is a natural isomorphism* $S^{-1}M \cong S^{-1}A \otimes_A M$.

Proof. Consider the map $T : S^{-1}A \times M \to S^{-1}M$, given by $T(a/s, m) = am/s$. This is a bilinear map whereby it induces a map $f : S^{-1}A \otimes_A M \to S{-}1M$ given by $f(a/s \otimes m) = am/s$. This is surjective, since $f(1/s \otimes m) = m/s$. We shall show $\ker f = 0$. Indeed, suppose the finite sum $\sum_i a_i/s_i \otimes m_i$ is in $\ker f$. Let $s = \prod_i s_i$ and $t_i = \prod_{j \neq i} s_i$. Then,

$$\sum_i a_i/s_i \otimes m_i = 1/s \otimes \left(\sum_i a_i t_i m_i \right)$$

The image under f of this tensor is $(\sum_i a_i t_i m_i)/s$ which is zero, whence there is $u \in S$ such that $u \sum_i a_i t_i m_i = 0$, but this implies

$$1/s \otimes \left(\sum_i a_i t_i m_i \right) = 1/su \otimes \left(u \sum_i a_i t_i m_i \right) = 0$$

This completes the proof. ■

Corollary 3.9. For every multiplicative subset $S \subseteq A$, $S^{-1}A$ is a flat A-module.

Corollary 3.10. Let $\{M_i\}_{i \in I}$ be a collection of A-modules. If $S \subseteq A$ is a multiplicative subset, then

$$S^{-1} \left(\bigoplus_{i \in I} M_i \right) \cong \bigoplus_{i \in I} S^{-1}M_i$$

as $S^{-1}A$-modules. As a result,

$$S^{-1} \left(\sum_{i \in I} M_i \right) \cong \sum_{i \in I} S^{-1}M_i$$

as $S^{-1}A$-modules.

Proof. The first assertion follows from the fact that the tensor product commutes with direct sums. As for the second assertion, consider the exact sequence

$$\bigoplus_{i\in I} M_i \longrightarrow \sum_{i\in I} M_i \longrightarrow 0$$

and localize. ■

Proposition 3.11. *Let $S \subseteq A$ be a multiplicative subset. Then, there is a natural isomorphism $S^{-1}(M \otimes_A N) = S^{-1}M \otimes_{S^{-1}A} S^{-1}N$.*

Proof. Define the map

$$\Phi : S^{-1}M \times S^{-1}N \to S^{-1}(M \otimes_A N)$$

given by

$$\Phi\left(\frac{m}{s}, \frac{n}{t}\right) = \frac{m \otimes n}{st}.$$

This is obviously $S^{-1}A$-linear and thus induces a map

$$\Psi : S^{-1}M \otimes_{S^{-1}A} S^{-1}N \to S^{-1}(M \otimes_A N)$$

given by

$$\Psi\left(\frac{m}{s} \otimes \frac{n}{t}\right) = \frac{m \otimes n}{st}.$$

We contend that this is an isomorphism of vector spaces. Define the map

$$\Gamma : S^{-1}(M \otimes_A N) \to S^{-1}M \otimes_{S^{-1}A} S^{-1}N$$

by

$$\Gamma\left(\frac{m \otimes n}{s}\right) = \frac{m}{s} \otimes \frac{n}{1}.$$

It is not hard to see that $\Gamma \circ \Psi$ and $\Psi \circ \Gamma$ are the identity maps whence they are isomorphisms. ■

3.3 Local Properties

A property P defined on the class of modules is said to be local if for every A-module M,

M satisfies P if and only if $M_{\mathfrak{p}}$ satisfies P for each $\mathfrak{p} \in \operatorname{Spec} A$.

Proposition 3.12. *Let M be an A-module. Then, the following are equivalent:*

(a) $M = 0$

(b) $M_{\mathfrak{p}} = 0$ *for each* $\mathfrak{p} \in \operatorname{Spec} A$

(c) $M_{\mathfrak{m}} = 0$ *for each* $\mathfrak{m} \in \operatorname{MaxSpec} A$

Proof. That $(a) \implies (b) \implies (c)$ is obvious. We shall show $(c) \implies (a)$. Suppose not, then there is $x \in M\backslash\{0\}$. Since $\operatorname{Ann}_A(x)$ is a proper ideal in A, it is contained in some maximal ideal, say $\mathfrak{m}$. Since $M_{\mathfrak{m}} = 0$, there is $s \in A\backslash\mathfrak{m}$ such that $sx = 0$, a contradiction. This completes the proof. ■

Proposition 3.13. *Let $\phi : M \to N$ be an A-module homomorphism. Then, the following are equivalent:*

(a) ϕ is injective (surjective).

(b) $\phi_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ is injective (surjective).

(c) $\phi_\mathfrak{m} : M_\mathfrak{m} \to N_\mathfrak{m}$ is injective (surjective).

Proof. $(a) \implies (b)$ follows from the exactness of localization applied to the exact sequence $0 \to M \to N$ ($M \to N \to 0$) and $(b) \implies (c)$ is trivial. We shall show $(c) \implies (a)$. We have the exact sequence $0 \to \ker\phi \to M \to N \to \operatorname{coker}\phi \to 0$. Upon localizing, for all maximal ideals $\mathfrak{m}$, we have the exact sequence

$$0 \longrightarrow (\ker\phi)_\mathfrak{m} \longrightarrow M_\mathfrak{m} \longrightarrow N_\mathfrak{m} \longrightarrow (\operatorname{coker}\phi)_\mathfrak{m} \longrightarrow 0$$

Since we have $\phi_\mathfrak{m}$ is injective (surjective), we have $(\ker\phi)_\mathfrak{m}$ ($(\operatorname{coker}\phi)_\mathfrak{m}$) is zero for all maximal ideals $\mathfrak{m}$, whence we are done using to the previous proposition. ■

Proposition 3.14. *Flatness is a local property. That is, the following are equivalent.*

(a) M is a flat A-module.

(b) $M_\mathfrak{p}$ is a flat $A_\mathfrak{p}$-module for every $\mathfrak{p} \in \operatorname{Spec}(A)$.

(c) $M_\mathfrak{m}$ is a flat $A_\mathfrak{m}$-module for every $\mathfrak{m} \in \operatorname{MaxSpec}(A)$.

Proof. $(a) \implies (b)$ follows from the exactness of localization and $(b) \implies (c)$ is obvious. We shall show $(c) \implies (a)$. ■

show that c=>a

Proposition 3.15. *Let M be a finitely presented A-module. Then, the following are equivalent:*

(a) M is projective

(b) $M_\mathfrak{p}$ is projective for all $\mathfrak{p} \in \operatorname{Spec} A$

(c) $M_\mathfrak{m}$ is projective for all $\mathfrak{p} \in \operatorname{MaxSpec} A$

Proof. $(a) \implies (b)$. If M is projective, there is a positive integer n and an A-module N such that $M \oplus N \cong A^n$. As a result, $M_\mathfrak{p} \oplus M_\mathfrak{p} \cong A_\mathfrak{p}^{\oplus n}$ and is projective.

$(c) \implies (a)$. ■

A surprising consequence of the previous proposition is the following.

Proposition 3.16. *A finitely presented flat A-module is projective.*

Proof. Follows from Proposition 3.15 and Lemma 2.51. ■

Proposition 3.17. *"Being an integral domain" is not a local property.*

Proof. Let A be a nonzero integral domain and consider the ring $R = A \times A$. This is not an integral domain. Due to Proposition 3.3, every localization of R is isomorphic to $A_\mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Spec} A$, consequently, is an integral domain. ■

3.4 Extension and Contraction of Ideals

Definition 3.18. If $\mathfrak{a} \subseteq A$ is an ideal, $S \subseteq A$ a multiplicatively closed subset and $\varphi : A \to S^{-1}A$ the natural map. Define $S^{-1}\mathfrak{a}$ to be the extension of $\mathfrak{a}$ under the natural map φ.

Theorem 3.19. *Let $S \subseteq A$ be a multiplicatively closed set. Then,*

(a) Every ideal in $S^{-1}A$ is an extended ideal.

(b) If $\mathfrak{a} \subseteq A$ is an ideal, then

$$\mathfrak{a}^{ec} = \bigcup_{s \in S} (\mathfrak{a} : s)$$

Hence, $\mathfrak{a}^e = (1)$ if and only if $\mathfrak{a} \cap S \neq \varnothing$

(c) There is a bijection

$$\{\mathfrak{p} \in \operatorname{Spec} A \mid S \cap \mathfrak{p} = \varnothing\} \leftrightarrow \operatorname{Spec}(S^{-1}A)$$

given by $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$, which is just the extension map.

Proof. (a) Let $\mathfrak{a} \subseteq S^{-1}A$ be an ideal. We shall show that $\mathfrak{a}^{ce} = \mathfrak{a}$. We know that $\mathfrak{a}^{ce} \subseteq \mathfrak{a}$ therefore, it suffices to show the reverse inclusion. Let $x/s \in \mathfrak{a}$. Then, $x/1 \in \mathfrak{a}$, and $x \in \mathfrak{a}^c$. As a result, $x/1 \in \mathfrak{a}^{ce}$ and $x/s \in \mathfrak{a}^{ce}$, implying the desired conclusion.

(b)

(c) Let $\mathfrak{p}$ be a prime ideal in A that does not meet S. Let $a/s, b/t \in S^{-1}A$ such that $ab/st \in S^{-1}\mathfrak{p}$, whereby there is an element $p \in \mathfrak{p}$ and $r \in S$ such that $ab/st = p/r$ whence there is $u \in S$ such that $uabr = ustp$. Since $ur \notin \mathfrak{p}$, we must have $ab \in \mathfrak{p}$, consequently, either $a/s \in S^{-1}\mathfrak{p}$ or $b/t \in S^{-1}\mathfrak{p}$, implying the desired conclusion.

Conversely, since the contraction of any prime ideal in $S^{-1}\mathfrak{p}$ is also a prime ideal not meeting S, lest the prime ideal in $S^{-1}A$ contain a unit. Now, if $\mathfrak{p}$ is a prime ideal, then

$$\mathfrak{p} \subseteq \mathfrak{p}^{ec} = \bigcup_{s \in S} (\mathfrak{p} : s) \subseteq \mathfrak{p}$$

On the other hand, from (a), we see that if $\mathfrak{q}$ is a prime ideal in $S^{-1}A$, then $\mathfrak{q}^{ce} = \mathfrak{q}$, whereby the bijection is established.

∎

Proposition 3.20. *The operation S^{-1} on ideals of A commutes with formation of finite sums, products, intersections and radicals.*

Corollary 3.21. $S^{-1}(\mathfrak{N}(A)) = \mathfrak{N}(S^{-1}A)$

Proof. Since $\mathfrak{N}(A) = \sqrt{(0)}$. ∎

From the above proposition, we see that "$\mathfrak{N}(A) = (0)$" is a local property.

Proposition 3.22. *If M is finitely generated, then $S^{-1} \operatorname{Ann}_A(M) = \operatorname{Ann}_A(S^{-1}M)$.*

Proof. Induction on the number of generators. Sort of straightforward. Use the fact that

$$\operatorname{Ann}(N_1 + N_2) = \operatorname{Ann}(N_1) \cap \operatorname{Ann}(N_2)$$ ■

Theorem 3.23. *Let $f : A \to B$ be ring homomorphism. Then, $\mathfrak{p} \in \operatorname{Spec}(A)$ is a contraction of a prime ideal in B if and only if $\mathfrak{p}^{ec} = \mathfrak{p}$.*

Proof. We shall prove only the converse, since the other direction is trivial. Suppose $\mathfrak{p}^{ec} = \mathfrak{p}$. Let $S = f(A \backslash \mathfrak{p})$, which is obviously a multiplicatively closed subset of B. Obviously, $\mathfrak{p}^e \cap S = \varnothing$ whence $S^{-1}\mathfrak{p}^e$ is a proper ideal in $S^{-1}B$. Let $\mathfrak{m} \subseteq S^{-1}B$ be a maximal ideal containing $S^{-1}\mathfrak{p}^e$. Let $\mathfrak{q}$ be the contraction of $\mathfrak{m}$ in B. This is a prime ideal containing $\mathfrak{p}^e$ and $\mathfrak{q} \cap S = \varnothing$, whence, $\mathfrak{q}^c$ must be contained in $\mathfrak{p}$ but it also contains $\mathfrak{p}$ therefore, is equal to $\mathfrak{p}$. This completes the proof. ■

Theorem 3.24. *A is absolutely flat if and only if $A_{\mathfrak{m}}$ is a field for every $m \in \operatorname{MaxSpec}(A)$.*

Proof. The forward direction is obvious. We shall show the converse. Let M be an A-module. Then, $M_{\mathfrak{m}}$ is an $A_{\mathfrak{m}}$-vector space and thus a flat $A_{\mathfrak{m}}$-module. Since flatness is a local property, we see that M must be a flat A-module. ■

3.5 Support of a Module

Definition 3.25. For an A-module M, the support of a module $\operatorname{Supp}(M)$ is defined to be the set of all prime ideals $\mathfrak{p} \in \operatorname{Spec}(A)$ such that $M_{\mathfrak{p}} \neq 0$.

Theorem 3.26. *For an A-module M and an ideal $\mathfrak{a} \trianglelefteq A$, the following are true.*

(a) *If $M \neq 0$, then* $\operatorname{Supp}(M) \neq \varnothing$.

(b) $\operatorname{Supp}(A/\mathfrak{a}) = V(\mathfrak{a})$.

(c) *If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence, then* $\operatorname{Supp}(M) = \operatorname{Supp}(M') \cup \operatorname{Supp}(M'')$.

(d) *If $M = \sum_{i \in I} M_i$, then* $\operatorname{Supp}(M) = \bigcup_{i \in I} \operatorname{Supp}(M_i)$.

(e) *If M is finitely generated, then* $\operatorname{Supp}(M) = V(\operatorname{Ann}_A(M))$.

(f) *If M and N are finitely generated, then* $\operatorname{Supp}(M \otimes_A N) = \operatorname{Supp}(M) \cap \operatorname{Supp}(N)$.

(g) *If M is finitely generated, then* $\operatorname{Supp}(M/\mathfrak{a}M) = V(\mathfrak{a} + \operatorname{Ann}_A(M))$.

Proof. (a) Follows from the fact that being zero is a local property.

(b) Note that $(A/\mathfrak{a})_{\mathfrak{p}} = A_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}}$ and $\mathfrak{a}_{\mathfrak{p}} \subsetneq A_{\mathfrak{p}}$ if and only if $\mathfrak{a} \subseteq \mathfrak{p}$.

(c) Consider the localized short exact sequence

$$0 \longrightarrow M'_{\mathfrak{p}} \longrightarrow M_{\mathfrak{p}} \longrightarrow M''_{\mathfrak{p}} \longrightarrow 0.$$

If $\mathfrak{p} \in \operatorname{Supp}(M)$, then it must lie in either $\operatorname{Supp}(M')$ or $\operatorname{Supp}(M'')$. On the other hand, if $\mathfrak{p} \notin \operatorname{Supp}(M)$, then the above sequence is

$$0 \longrightarrow M'_{\mathfrak{p}} \longrightarrow 0 \longrightarrow M''_{\mathfrak{p}} \longrightarrow 0$$

whence $\mathfrak{p} \notin \operatorname{Supp}(M') \cup \operatorname{Supp}(M'')$.

(d) Follows from the fact that localization commutes with arbitrary sums.

(e) First suppose $M = (x_1)$. Then, $\mathfrak{p} \in \operatorname{Supp}(M)$ if and only if $\operatorname{Ann}_A(x_1) \subseteq \mathfrak{p}$. Thus the assertion holds for cyclic modules. Then, using the previous assertion,

$$\operatorname{Supp}((x_1, \dots, x_n)) = \bigcup_{i=1}^{n} V(\operatorname{Ann}_A(x_i)) = V\left(\bigcap_{i=1}^{n} \operatorname{Ann}_A(x_i)\right) = V(\operatorname{Ann}_A(M)).$$

(f) Suppose $\mathfrak{p} \notin \operatorname{Supp}(M \otimes_A N)$, then $M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}} = 0$ and $M_{\mathfrak{p}}, N_{\mathfrak{p}}$ are finitely generated $A_{\mathfrak{p}}$-modules. Due to Proposition 2.39, $M_{\mathfrak{p}} = 0$ or $N_{\mathfrak{p}} = 0$, whence $\mathfrak{p} \notin \operatorname{Supp}(M) \cap \operatorname{Supp}(N)$, that is, $\operatorname{Supp}(M) \cap \operatorname{Supp}(N) \subseteq \operatorname{Supp}(M \otimes_A N)$. On the other hand, if $\mathfrak{p} \notin \operatorname{Supp}(M) \cap \operatorname{Supp}(N)$, then $M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}} = 0$ and the conclusion follows.

(g) We have, due to the previous assertion,

$$\operatorname{Supp}(A/\mathfrak{a} \otimes_A M) = \operatorname{Supp}(A/\mathfrak{a}) \cap \operatorname{Supp}(M) = V(\mathfrak{a}) \cap V(\operatorname{Ann}_A(M)) = V(\mathfrak{a} + \operatorname{Ann}_A(M)).$$ ■

Place This Somewhere

Lemma 3.27. *Let M be a finitely generated A-module. Let $\mathfrak{a} \trianglelefteq A$ be an ideal and $x_1, \dots, x_n \in M$ generate $M/\mathfrak{a}M$. Then, there is $f \in 1 + \mathfrak{a}$ such that $x_1/1, \dots, x_n/1$ generate M_f as an A_f-module.*

Proof. Consider the map $\phi : A^n \to M$ mapping e_i to x_i. Note that $\operatorname{coker} \phi \otimes_A A/\mathfrak{a} = 0$ and thus, due to Corollary 2.16, there is some $f \in 1 + \mathfrak{a}$ such that $f \operatorname{coker} \phi = 0$. The conclusion now follows. ■

Lemma 3.28. *Let M be a finitely generated A-module. Then, the following are equivalent:*

(a) M is projective.

(b) M is strongly locally free.

(c) For every $\mathfrak{p} \in \operatorname{Spec}(A)$, the module $M_{\mathfrak{p}}$ is free and has locally constant dimension with respect to the Zariski topology.

Proof. $(a) \implies (b)$.
$(b) \implies (a)$. simplify this
$(b) \implies (c)$ Trivial.
$(c) \implies (b)$ Let $\mathfrak{m} \subseteq A$ be a maximal ideal and let $x_1, \dots, x_r \in M$ map to an $A/\mathfrak{m}$-basis of $M/\mathfrak{m}M$. Then, due to the previous lemma, there is some $f \in 1 + \mathfrak{m}$ such that $x_1/1, \dots, x_r/1$ generate M_f over A_f.

Since ρ_M is locally constant, it is equal to r on an open set containing $\mathfrak{m} \in \operatorname{Spec}(A)$. Choose a basic open set $D(g)$ with $g \notin \mathfrak{m}$ on which ρ_M is constant and equal to r. Define the map $\Psi : A_{fg}^r \to M_{fg}$ given by

$$\Phi(a_1, \dots, a_r) = \sum_{i=1}^{r} a_i \frac{x_i}{1}.$$

We contend that this is an isomorphism. Note the primes in A_{fg} are precisely the extensions of the primes in $D(fg)$. Let $\mathfrak{p} \in D_{fg}$. Then, the localization $\Psi_{\mathfrak{p}}$, at the extension of $\mathfrak{p}$ in A_{fg} is the map

$$\Psi_{\mathfrak{p}} : A_{\mathfrak{p}}^r \to M_{\mathfrak{p}} \qquad \Psi\left(a_1, \ldots, a_r\right) = \sum_{i=1}^{r} a_i \frac{x_i}{1}.$$

Note that $\mathfrak{p} \in D(fg) \subseteq D(f)$ and thus, $\Psi_{\mathfrak{p}}$ is surjective since $x_1/1, \ldots, x_r/1$ generate M_f over A_f. Further, since $M_{\mathfrak{p}}$ is finitely generated and isomorphic to $A_{\mathfrak{p}}^r$, the surjection $\Psi_{\mathfrak{p}}$ must be an isomorphism whence Ψ is an isomorphism.

Hence, for each maximal $\mathfrak{m}$, we have found some $h \notin \mathfrak{m}$ such that M_h is a free A_h-module. The set of all such h's must generate (1) else they would be contained in a maximal ideal. This proves (b). ■

Chapter 4

Primary Decomposition

4.1 Primary Decomposition of Ideals

A primary ideal is a generalization of the ideals $p^n\mathbb{Z}$ in $\mathbb{Z}$, as is evident from the following definition.

Definition 4.1 (Primary Ideals). An ideal $\mathfrak{q} \subseteq A$ is said to be *primary* if for every ordered pair $x, y \in A$,

$$xy \in \mathfrak{q} \implies x \in \mathfrak{q} \text{ or } y^n \in \mathfrak{q} \text{ for some } n > 0$$

From the definition, we see that every prime ideal is primary. It is not hard to see that

- $\mathfrak{q}$ is primary if and only if every zero divisor in $A/\mathfrak{q}$ is nilpotent.
- $\mathfrak{q}$ is primary if and only if (0) is primary in $A/\mathfrak{q}$.

Proposition 4.2. *If $\mathfrak{q}$ is primary, then $\sqrt{\mathfrak{q}}$ is prime. Further, $\sqrt{\mathfrak{q}}$ is the smallest prime ideal containing $\mathfrak{q}$.*

Proof. Suppose $xy \in \sqrt{\mathfrak{q}}$, then there is $n > 0$ such that $x^n y^n \in \mathfrak{q}$, consequently, there is an $m > 0$ such that $x^n \in \mathfrak{q}$ or $y^{mn} \in \mathfrak{q}$, therefore, $x \in \sqrt{\mathfrak{q}}$ or $y \in \sqrt{\mathfrak{q}}$, whence $\sqrt{\mathfrak{q}}$ is prime. The second assertion is trivial. ■

If $\mathfrak{q}$ is a primary ideal, then $\mathfrak{p} = \sqrt{\mathfrak{q}}$ is called the *associated prime ideal* of $\mathfrak{q}$ and $\mathfrak{q}$ is said to be $\mathfrak{p}$-*primary*.

Consider the ring $A = k[x, y]$ and the ideal $\mathfrak{q} = (x, y^2)$. The quotient ring $A/\mathfrak{q}$ is isomorphic to $k[y]/(y^2)$ where every zero divisor is nilpotent consequently, $\mathfrak{q}$ is primary. The radical ideal $\mathfrak{p} = \sqrt{\mathfrak{q}} = (x, y)$ is a prime ideal such that $\mathfrak{p}^2 \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$, therefore, $\mathfrak{q}$ is not a prime power.

On the other hand, consider the ring $A = k[x, y, z]/(xy - z^2)$ and the prime ideal $\mathfrak{p} = (\overline{x}, \overline{z}) \subseteq A$. We contend that $\mathfrak{p}^2 \subseteq A$ is not primary. Indeed, note that $\overline{xy} = \overline{z}^2 \in \mathfrak{p}^2$ but $\overline{x} \notin \mathfrak{p}^2$ and $\overline{y} \notin \mathfrak{p}^2$, and the conclusion follows.

Proposition 4.3. *If $\sqrt{\mathfrak{a}}$ is maximal, then $\mathfrak{a}$ is primary.*

Proof. Let $\mathfrak{m} = \sqrt{\mathfrak{a}}$ and $\phi : A \to A/\mathfrak{a}$ denote the natural map. Then, $\phi(\sqrt{\mathfrak{a}})$ is the maximal ideal in $A/\mathfrak{a}$ and is also the nilradical of $A/\mathfrak{a}$, consequently, $A/\mathfrak{a}$ is local and every non-unit is nilpotent. Hence, $\mathfrak{a}$ is primary. ■

Proposition 4.4. *Let $\phi : A \to B$ be a ring homomorphism. If $\mathfrak{q} \trianglelefteq B$ is a primary ideal in B, then $\mathfrak{q}^c$ is a primary ideal in A.*

Proof. There is an injection $A/\mathfrak{q}^c \hookrightarrow B/\mathfrak{q}$. If (0) is primary in $B/\mathfrak{q}$ then it is primary in $A/\mathfrak{q}^c$. ■

Lemma 4.5. *If $\{\mathfrak{q}_i\}_{i=1}^n$ are $\mathfrak{p}$-primary, then so is $\mathfrak{q} = \bigcap_{i=1}^n \mathfrak{q}_i$.*

Proof. Obviously,

$$\sqrt{\mathfrak{q}} = \bigcap_{i=1}^{n} \sqrt{\mathfrak{q}_i} = \mathfrak{p}$$

Let $xy \in \mathfrak{q}$. If $y \in \mathfrak{p}$, then we are done, since $\mathfrak{p} = \sqrt{\mathfrak{q}}$. Else, $y^n \notin \mathfrak{q}_i$ for every positive integer n, since $\mathfrak{p} = \sqrt{\mathfrak{q}_i}$ whereby $x \in \mathfrak{q}_i$ for each $1 \leq i \leq n$ and the conclusion follows. ■

Lemma 4.6. *Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal and $x \in A$. Then*

(a) if $x \in \mathfrak{q}$, then $(\mathfrak{q} : x) = (1)$.

(b) if $x \notin \mathfrak{q}$, then $(\mathfrak{q} : x)$ is $\mathfrak{p}$-primary.

(c) if $x \notin \mathfrak{p}$, then $(\mathfrak{q} : x) = \mathfrak{q}$.

Proof. (a) Trivial.

(b) If $y \in (\mathfrak{q} : x)$, then $xy \in \mathfrak{q}$, therefore, $y \in \mathfrak{p}$. Thus, we have $\mathfrak{q} \subseteq (\mathfrak{q} : x) \subseteq \mathfrak{p}$. Taking radicals, $\mathfrak{p} \subseteq \sqrt{(\mathfrak{q} : x)} \subseteq \mathfrak{p}$, whereby $\sqrt{(\mathfrak{q} : x)} = \mathfrak{p}$.

On the other hand, if $yz \in (\mathfrak{q} : x)$, then $xyz \in \mathfrak{q}$. If $z \in \mathfrak{p}$, then we are done. Else, $xy \in \mathfrak{q}$ and $y \in (q : x)$ whence $(q : x)$ is $\mathfrak{p}$-primary.

(c) If $y \in (q : x)$, then $yx \in \mathfrak{q}$. Since $x \notin \mathfrak{p}$, we must have $y \in \mathfrak{q}$. This completes the proof.

■

Definition 4.7 (Primary Decomposition). A *primary decomposition* of an ideal $\mathfrak{a} \subseteq A$ is an expression of $\mathfrak{a}$ as a *finite* intersection of primary ideals.

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

The ideal $\mathfrak{a}$ is said to be *decomposable* if it has a primary decomposition. Moreover, if for all $1 \leq i \leq n$, $\sqrt{\mathfrak{q}_i}$ are distinct and

$$\bigcap_{j \neq i} \mathfrak{q}_j \not\subseteq \mathfrak{q}_i$$

then the primary decomposition is said to be *minimal*.

Using Lemma 4.5, it is not hard to see that every decomposable ideal has a minimal decomposition.

Theorem 4.8 (First Uniqueness Theorem). *Let $\mathfrak{a} \subseteq A$ be a decomposable ideal and*

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

be a minimal primary decomposition with $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$. Then, the $\mathfrak{p}_i$'s are precisely the prime ideals the occur in the set $\{\sqrt{(\mathfrak{a} : x)} \mid x \in A\}$.

Proof. First, note that

$$\sqrt{(\mathfrak{a} : x)} = \sqrt{\bigcap_{i=1}^{n} (\mathfrak{q}_i : x)} = \bigcap_{i=1}^{n} \sqrt{(\mathfrak{q}_i : x)} = \bigcap_{x \notin q_i} \mathfrak{p}_i$$

Using Proposition 1.9, $\sqrt{(\mathfrak{a} : x)} = \mathfrak{p}_j$ for some index j.

Conversely, for every $1 \leq j \leq n$, there is $x_j \in \bigcap_{i \neq j} \mathfrak{q}_i \backslash \mathfrak{q}_j$. This obviously exists since the decomposition is minimal. It now follows from Proposition 1.9 and the decomposition of $\sqrt{(\mathfrak{a} : x)}$ we derived above that $\sqrt{(\mathfrak{a} : x)} = \mathfrak{p}_j$. ■

Proposition 4.9. *Let $\mathfrak{a}$ be a decomposable ideal. Then any prime ideal $\mathfrak{p} \supseteq \mathfrak{a}$ contains a minimal prime ideal belonging to $\mathfrak{a}$, and thus the minimal prime ideals belonging to $\mathfrak{a}$ are precisely the minimal prime ideals in the set of all prime ideals containing $\mathfrak{a}$.*

Proof. Let $\mathfrak{p}$ be a minimal prime ideal containing $\mathfrak{a}$. Consider a minimal primary decomposition of $\mathfrak{a}$ given by

$$\mathfrak{p} \supseteq \mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i.$$

Let $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$, then

$$\mathfrak{p} \supseteq \sqrt{\mathfrak{a}} = \bigcap_{i=1}^{n} \mathfrak{p}_i$$

and due to Proposition 1.9, there is an index j such that $\mathfrak{p} \supseteq \mathfrak{p}_j$ whence $\mathfrak{p}_j = \mathfrak{p}$. Thus, every minimal prime ideal containing $\mathfrak{a}$ belongs to $\mathfrak{a}$. ■

Proposition 4.10. *Let S be a multiiplcatively closed subset of A and $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal.*

(a) If $S \cap \mathfrak{p} \neq \varnothing$, then $S^{-1}\mathfrak{q} = S^{-1}A$.

(b) If $S \cap \mathfrak{p} = \varnothing$, then $S^{-1}\mathfrak{q}$ is $S^{-1}\mathfrak{p}$-primary and its contraction in A is $\mathfrak{q}$.

Proof. (a) is trivial. (b) : Recall that we have

$$\mathfrak{q}^{ec} = \bigcup_{s \in S} (\mathfrak{q} : s) = \bigcup_{s \in S} \mathfrak{q}$$

where the last equality follows from the fact that $S \cap \mathfrak{q} = \varnothing$. It remains to show that $S^{-1}\mathfrak{q}$ is primary. Indeed, let $x/s \cdot y/t \in S^{-1}\mathfrak{q}$. Then, there is $z \in \mathfrak{q}$ and $w, u \in S$ such that $w(xyu - stz) = 0$. But since $wu \notin \mathfrak{q}$, we must have $xy \in \mathfrak{q}$, whereby $x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some positive integer n, implying that either $x/s \in S^{-1}\mathfrak{q}$ or $y^n/t^n \in S^{-1}\mathfrak{q}$. This completes the proof. ■

Definition 4.11 (Isolated Set of Associated Primes). A set Σ of prime ideals associated with $\mathfrak{a}$ is said to be *isolated* if it satisfies the following condition:

if $\mathfrak{p}'$ is a prime ideal belonging to $\mathfrak{a}$ with $\mathfrak{p}' \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \Sigma$, then $\mathfrak{p}' \in \Sigma$

Theorem 4.12 (Second Uniqueness Theorem). *Let $\mathfrak{a}$ be a decomposable ideal with a primary decomposition $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$. Let $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$. Suppose $\Sigma = \{\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_m}\}$ is an isolated set of associated primes of $\mathfrak{a}$, then $\bigcap_{j=1}^m \mathfrak{q}_{i_j}$ is independent of the chosen decomposition.*

Proof. Let $S = A \backslash \bigcup_{j=1}^m \mathfrak{p}_{i_j}$. Then, $\mathfrak{p}_k \cap S = \varnothing$ if and only if $\mathfrak{p}_k \subseteq \bigcap_{j=1}^m \mathfrak{p}_j$ whence due to Proposition 1.9, there is a prime $\mathfrak{p}_{i_t}$ containing $\mathfrak{p}_k$ and equivalently, $\mathfrak{p}_k \in \Sigma$.

Whence, upon localizing with S, we have

$$S^{-1}\mathfrak{a} = \bigcap_{i=1}^n S^{-1}\mathfrak{q}_i = \bigcap_{j=1}^m S^{-1}\mathfrak{q}_{i_j}$$

Contracting both sides, we have

$$\mathfrak{a}^{ec} = \left(\bigcap_{j=1}^m S^{-1}\mathfrak{q}_{i_j}\right) = \bigcap_{j=1}^m \mathfrak{q}_{i_j}^{ec} = \bigcap_{j=1}^m \mathfrak{q}_{i_j}$$

and the conclusion follows. ∎

Corollary 4.13. In particular, the primary ideals which correspond to the minimal primes associated to $\mathfrak{a}$ are uniquely determined.

Proposition 4.14. *Let X be an infinite compact Hausdorff space. Then, (0) is not decomposable in $C(X)$, the ring of continuous functions on X.*

Proof. Suppose $(0) = \bigcap_{i=1}^n \mathfrak{q}_i$. Recall that the maximal ideals in X are in bijection with the points of X. Denote the maximal ideal corresponding to a point $x \in X$ by $\mathfrak{m}_x$.

For each $\mathfrak{q}_i$, choose a maximal ideal $\mathfrak{m}_{x_i}$ containing it. Choose some $x \in X \backslash \{x_1, \ldots, x_n\}$. Choose an open set V containing $\{x_1, \ldots, x_n\}$ and an open set U containing x such that $U \cap V = \varnothing$.

Using Urysohn's Lemma, choose continuous functions $f, g : X \to [0,1]$ such that $f(x) = 1$ and $\text{Supp}(f) \subseteq U$ and $g(x_i) = 1$ for every i and $\text{Supp}(g) \subseteq V$. By our choice of g, note that $g^m \notin \mathfrak{q}_i$ for every $1 \le i \le n$ and every positive integer m. Since $fg = 0$, we must have $f \in \mathfrak{q}_i$ for every $1 \le i \le n$, implying that $f = 0$, a contradiction. This completes the proof. ∎

Definition 4.15 (Symbolic Power). Let $\mathfrak{p} \in \operatorname{Spec} A$. The *$n$-th symbolic power of* $\mathfrak{p}$ is defined to be the contraction of the ideal $\mathfrak{p}^n A_{\mathfrak{p}}$ in A, denoted $\mathfrak{p}^{(n)}$.

Being the contraction of a primary ideal in $A_{\mathfrak{p}}$, the symbolic power is always a primary ideal. Moreover, $\sqrt{\mathfrak{p}^{(n)}} = \mathfrak{p}$ whence, it is $\mathfrak{p}$-primary.

Proposition 4.16. *With notation as above,*

(a) $\mathfrak{p}^{(n)}$ *is a* $\mathfrak{p}$*-primary ideal.*

(b) if $\mathfrak{p}^n$ *has a primary decomposition, then* $\mathfrak{p}^{(n)}$ *is its* $\mathfrak{p}$*-primary component.*

Proof. (a) follows from the fact that the contraction of primary ideals is primary.

(b) Note that $\mathfrak{p}^n$ obviously would have a $\mathfrak{p}$-primary component and that would be given by the contraction of $S^{-1}\mathfrak{p}^n$ where $S = A \backslash \mathfrak{p}$. The conclusion follows. ∎

4.2 Associated Primes of Modules

Definition 4.17. Let $a \in A$ and M and A-module. The homomorphism $a_M : M \to M$ given by $x \mapsto ax$ for all $x \in M$ is called the *principal homomorphism*. We say that a_M is *locally nilpotent* if for each $x \in M$, there is an integer $n \in \mathbb{N}$ such that $a^n x = 0$.

Remark 4.2.1. *If M is finitely generated, then a_M is locally nilpotent if and only if it is nilpotent.*

Proposition 4.18. *Let $a \in A$ and M an A-module. Then a_M is locally nilpotent if and only if $a \in \mathfrak{p}$ for each $\mathfrak{p} \in \operatorname{Supp}_A(M)$, that is, $a \in \bigcap_{\mathfrak{p} \in \operatorname{Supp}_A(M)} \mathfrak{p}$.*

Proof. Suppose a_M is locally nilpotent and $\mathfrak{p} \in \operatorname{Supp}(M)$. Then, there is some $x \in M$ such that $x/1 \neq 0$ in $M_\mathfrak{p}$, that is, $\mathfrak{a} = \operatorname{Ann}_A(x) \subseteq \mathfrak{p}$. Since a_M is locally nilpotent, there is a positive integer n such that $a^n \in \mathfrak{a}$ whence $a \in \mathfrak{p}$.

Conversely, suppose a_M is not locally nilpotent whence there is some $x \in M$ such that $a^n x \neq 0$ for all $n \in \mathbb{N}$. Let $\mathfrak{p}$ be a prime ideal not intersecting $\{1, a, a^2, \dots\}$ and containing $\operatorname{Ann}_A(x)$[1]. Then, $x/1 \neq 0$ in $M_\mathfrak{p}$ whence $M_\mathfrak{p} \neq 0$ and $\mathfrak{p} \in \operatorname{Supp}(M)$, but $a \notin \mathfrak{p}$. This completes the proof. ■

Definition 4.19 (Associated Primes). For an A-module M, a prime $\mathfrak{p} \in \operatorname{Spec}(A)$ is said to be *associated* with M if there is $x \in M$ such that $\mathfrak{p} = \operatorname{Ann}_A(x)$. The set of all associated primes of a module M is denoted by $\operatorname{Ass}(M)$.

Equivalently, a prime $\mathfrak{p}$ is an associated prime of M if there is an injection of A-modules, $A/\mathfrak{p} \hookrightarrow M$.

Proposition 4.20. *If the poset*

$$\Sigma = \{\operatorname{Ann}_A(x) \mid x \in M \backslash \{0\}\}$$

has a maximal element, then it is prime.

Proof. Let $\mathfrak{p}$ be a maximal element of Σ under inclusion. Let $a, b \in A$ with $ab \in \mathfrak{p}$. If either a or b is zero, then, trivially, $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Suppose now that both a, b are nonzero. Let $x \in M$ be such that $\mathfrak{p} = \operatorname{Ann}_A(x)$ and suppose $b \notin \mathfrak{p}$. Then, $\mathfrak{p} \subseteq \operatorname{Ann}_A(bx) \neq (1)$ and due to maximality, we must have $\mathfrak{p} = \operatorname{Ann}_A(bx)$, and thus $a \in \mathfrak{p}$. This completes the proof. ■

Corollary 4.21. Modules over noetherings have associated primes.

Lemma 4.22. *Let A be a noethering and M an A-module with $a \in A$. Then, a_M is injective if and only if a does not lie in any of the associated primes of M.*

Proof. If a_M is injective, then a is not in the annihilator of any nonzero element, therefore, not an element of any associated prime. On the other hand, suppose a_M is not injective. Then, there is some nonzero $x \in M$ such that $a \in \operatorname{Ann}_A(x)$. Consider the poset of all proper annihilators containing $\operatorname{Ann}_A(x)$. Since A is a noethering, this has a maximal element, say $\mathfrak{p}$. Note that $\mathfrak{p}$ is also maximal in the poset of all proper annihilators whence is prime and hence a is contained in an associated prime. This completes the proof. ■

[1] That we can do this is an easy application of Zorn's Lemma

Lemma 4.23. *Let A be a noethering and M and A-module. Then, every $\mathfrak{p} \in \operatorname{Supp}(M)$ contains an associated prime.*

Proof. If $\mathfrak{p} \in \operatorname{Supp}(M)$, then there is some $x \in M$ such that $(Ax)_\mathfrak{p} \neq 0$, consequently, $(Ax)_\mathfrak{p}$ has an associated prime, say $\mathfrak{q}$. First, we contend that $\mathfrak{q} \subseteq \mathfrak{p}$. Suppose not, then there is some $a \in \mathfrak{q} \backslash \mathfrak{p}$. Since $\mathfrak{q}$ is an associated prime, there is some $0 \neq y/s \in (Ax)_\mathfrak{p}$ such that $\mathfrak{q} = \operatorname{Ann}_{A_\mathfrak{p}}(y/s)$. In particular, $by/s = 0$. But $b/1$ is invertible in $A_\mathfrak{p}$ whence $y/s = 0$, a contradiction. Thus $\mathfrak{q} \subseteq \mathfrak{p}$.

Next, we shall show that $\mathfrak{q}$ is an associated prime of M. Since A is a noethering, $\mathfrak{q}$ is finitely generated, say by $b_1, \ldots, b_n$. Then, $b_i y/s = 0$ for each i, consequently, there is some $s_i \notin \mathfrak{p}$ such that $s_i b_i y = 0$. Let $t = s_1 \cdots s_n \notin \mathfrak{p}$. We contend that $\mathfrak{q} = \operatorname{Ann}_A(ty)$. Obviously, $\mathfrak{q} \subseteq \operatorname{Ann}_A(ty)$. On the other hand, if $b \in \operatorname{Ann}_A(ty)$, then $bty = 0$ whereby $by/s = 0$ and $b \in \mathfrak{q}$. This completes the proof. ∎

Corollary 4.24. Let A be a noethering and M an A-module with $a \in A$. The following are equivalent:

(a) a_M is locally nilpotent.

(b) for each $\mathfrak{p} \in \operatorname{Ass}(M)$, $a \in \mathfrak{p}$.

(c) for each $\mathfrak{p} \in \operatorname{Supp}(M)$, $a \in \mathfrak{p}$.

Proof. $(a) \implies (b)$ is immediate from the definition while $(c) \implies (a)$ has been proven. Both these implications do not require the noethering hypothesis. The implication $(b) \implies (c)$ has been proven above and requires the noethering hypothesis. ∎

Lemma 4.25. *Let N be a submodule of M. Then,*

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

Proof. It is obvious that $\operatorname{Ass}(N) \subseteq \operatorname{Ass}(M)$. Now, let $\mathfrak{p} \in \operatorname{Ass}(M)$. Then, there is some $x \in M$ such that $\mathfrak{p} = \operatorname{Ann}_A(x)$. If $x \in N$, then we are done. If not, then consider $Ax \cap N$. If $Ax \cap N = 0$, then, Ax is isomorphic to the image of Ax under the projection M/N. Therefore, $\mathfrak{p}$ is an associated prime of some submodule of M/N. On the other hand, if $Ax \cap N \neq 0$, then there is some $y = ax \in N$ for some $a \in A$.

Obviously $\mathfrak{p}$ annihilates y. If $b \in A$ annihilates y, then $bax = 0$ whence $ba \in \mathfrak{p}$. But since $y \neq 0$, $a \notin \mathfrak{p}$ and thus $b \in \mathfrak{p}$. This completes the proof. ∎

Lemma 4.26. *Let $S \subseteq A$ be a multiplicative subset and N an $S^{-1}A$-module. Then,*

$$\operatorname{Ass}_{S^{-1}A}(N) = S^{-1} \operatorname{Ass}_A(N) \backslash \{S^{-1}A\},$$

where

$$S^{-1} \operatorname{Ass}_A(N) := \{S^{-1}\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Ass}_A(N)\}.$$

Proof. ∎

Lemma 4.27. *Let A be a noethering, M a non-zero A-module and S a multiplicative subset of A. Then,*

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

Proof. ∎

Corollary 4.28. Let A be a noethering. Then,

$$\mathfrak{p} \in \operatorname{Ass}_A(M) \iff \mathfrak{p}A_{\mathfrak{p}} \in \operatorname{Ass}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}).$$

Proof. Take $S = A \backslash \mathfrak{p}$ and the conclusion follows from the above lemma. ∎

Proposition 4.29. *Let A be a noethering and $M \neq 0$ a finitely generated (and hence, noetherian) A-module. Then, there is a filtration*

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

such that $M_i/M_{i+1} \cong A/\mathfrak{p}_i$ for some $\mathfrak{p}_i \in \operatorname{Spec}(A)$.

Proof. Since A is a noethering, $\operatorname{Ass}_A(M)$ is non-empty. Pick a prime $\mathfrak{p}_0 \in \operatorname{Ass}_A(M)$. Then, there is an injection $A/\mathfrak{p}_0 \hookrightarrow M$. Then, there is a submodule N_0 of M that is isomorphic to $A/\mathfrak{p}_0$. If $M = N_0$, then we are done. If not, then consider M/N_0. This also has an associated prime $\mathfrak{p}_1$ and hence, there is a submodle N_1 of M containing N_0 such that $M/N_1 \cong A/\mathfrak{p}_1$. Continuing this way, we obtain a sequence (the finiteness of this sequence requires M to be noetherian):

$$N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_n = M$$

where $M/N_i \cong A/\mathfrak{p}_i$ for some $\mathfrak{p}_i \in \operatorname{Spec}(A)$. This completes the proof. ∎

Lemma 4.30. *Let A be a noethering. Then, the set of all zero divisors on M is given by*

$$\bigcup_{\mathfrak{p} \in \operatorname{Ass}_A(M)} \mathfrak{p}.$$

Proof. If $a \in A$ is a zero divisor on M, then, the set

$$\{\mathfrak{a} \trianglelefteq A \mid a \in \mathfrak{a} \text{ and } \mathfrak{a} = \operatorname{Ann}_A(x) \text{ for some } x \in M\}$$

admits a maximal element (due to noetherian-ness), say $\mathfrak{p}$. This is an associated prime and contains a. The converse is trivial. ∎

Lemma 4.31. *Let A be a noethering and M a finitely generated (equivalently, noetherian) A-module. Then, $\operatorname{Ass}_A(M)$ is finite.*

Proof. As we have seen earlier, M admits a filtration

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

where $M_i/M_{i+1} \cong A/\mathfrak{p}_i$ for some $\mathfrak{p}_i \in \operatorname{Spec}(A)$. We have short exact sequences

$$0 \longrightarrow M_{i+1} \longrightarrow M_i \longrightarrow M_i/M_{i+1} \longrightarrow 0.$$

Then,

$$\operatorname{Ass}_A(M_i) \subseteq \operatorname{Ass}_A(M_{i+1}) \cup \operatorname{Ass}_A(M_i/M_{i+1}) = \operatorname{Ass}_A(M_{i+1}) \cup \{\mathfrak{p}_i\}.$$

Inductively, we see that

$$\operatorname{Ass}_A(M) \subseteq \{\mathfrak{p}_0, \ldots, \mathfrak{p}_{n-1}\}.$$

∎

Lemma 4.32. *Let A be any ring. Then,*

$$\text{Ass}_A(M) \subseteq \text{Supp}_A(M).$$

Proof. Let $\mathfrak{p} \in \text{Ass}_A(M)$. Then, there is an injection $A/\mathfrak{p} \hookrightarrow M$. Localizing at $\mathfrak{p}$, we have an injection $Q(A/\mathfrak{p}) \hookrightarrow M_\mathfrak{p}$. Thus, $M_\mathfrak{p} \neq 0$ and $\mathfrak{p} \in \text{Supp}_A(M)$. ∎

Lemma 4.33. *Let A be a noethering. The minimal elements of $\text{Ass}_A(M)$ and $\text{Supp}_A(M)$ are the same.*

Proof. Let $\mathfrak{p} \in \text{Ass}_A(M)$ be minimal. We have seen that $\mathfrak{p} \in \text{Supp}_A(M)$. Suppose $\mathfrak{q} \in \text{Supp}_A(M)$ with $\mathfrak{q} \subseteq \mathfrak{p}$. Note that

$$\text{Ass}_{A_\mathfrak{q}}(M_\mathfrak{q}) = \left(\text{Ass}_A(M)\right)_\mathfrak{q} \setminus \{A_\mathfrak{q}\} = \varnothing.$$

Therefore, $M_\mathfrak{q} = 0$ and $\mathfrak{q} \notin \text{Supp}_A(M)$. This shows that the minimal primes of $\text{Ass}_A(M)$ are a subset of the minimal primes of $\text{Supp}_A(M)$.

Conversely, suppose $\mathfrak{p} \in \text{Supp}_A(M)$ is minimal. Then,

$$\varnothing \neq \text{Ass}_{A_\mathfrak{p}}(M_\mathfrak{p}) = \left(\text{Ass}_A(M)\right)_\mathfrak{p} \setminus \{A_\mathfrak{p}\},$$

where the first "equality" follows from the fact that $M_\mathfrak{p} \neq 0$. Hence, there is a prime ideal $\mathfrak{q} \subseteq \mathfrak{p}$ that is an associated prime of M and hence, also lies in the support of M. It follows that $\mathfrak{q} = \mathfrak{p}$ whence $\mathfrak{p} \in \text{Ass}_A(M)$. This completes the proof. ∎

4.3 Primary Decomposition of Modules

Definition 4.34. Let M be an A-module. A submodule Q of M is said to be *primary* if $Q \neq M$ and for each $a \in A$, the homomorphism $a_{M/Q}$ is either injective or nilpotent.

Equivalently, the above definition implies that if $a_{M/Q}$ is a zero-divisor, then it is nilpotent.

Proposition 4.35. *Let Q be a primary submodule of M. Then,*

$$\mathfrak{p} := \{a \in A \mid a_{M/Q} \text{ is nilpotent}\}$$

is a prime ideal.

Proof. Let $ab \in \mathfrak{p}$, that is, $(ab)_{M/Q}$ is nilpotent. If $a \notin \mathfrak{p}$, then $a_{M/Q}$ is injective and thus $b_{M/Q}$ is nilpotent, i.e. $b \in \mathfrak{p}$. This completes the proof. ∎

Chapter 5

Integral Extensions

Definition 5.1 (Integral Extension). Let $A \subseteq B$ be a subring. Then, $\alpha \in B$ is said to be *integral* over A if it satisfies a monic polynomial in $A[x]$. The extension $A \hookrightarrow B$ is said to be integral if every element of B is integral over A.

Similarly, if $\mathfrak{a} \subseteq A$ is an ideal, then $\alpha \in B$ is said to be *integral* over $\mathfrak{a}$ if it satisfies a monic polynomial in $A[x]$ with coefficients in $\mathfrak{a}$.

Theorem 5.2. *Let $A \subseteq B$ be a subring and $\alpha \in B$. Then, the following are equivalent:*

(a) *α is integral over A*

(b) *$A[\alpha]$ is a finitely generated A-module*

(c) *$A[\alpha]$ is contained in a subring C of B such that C is a finitely generated A-module*

(d) *There is a faithful $A[\alpha]$-module M which is finitely generated as an A-module.*

Proof. $(a) \implies (b)$**:** If $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$. Then, it is not hard to argue that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ generated $A[\alpha]$ over A.

$(b) \implies (c)$**:** Take $C = A[\alpha]$

$(c) \implies (d)$**:** C is a faithful $A[\alpha]$ module which is a finitely generated A-module.

$(d) \implies (a)$**:** Let $\phi : M \to M$ be the map $m \mapsto \alpha \cdot m$. We have $\phi(M) \subseteq AM$, consequently, due to Proposition 2.15 (since $\mathfrak{a} = A$ is an ideal in A), there are $a_i \in A$ such that

$$(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0) \cdot m = 0$$

for each $m \in M$. But since M is a faithful $A[\alpha]$-module, we must have $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$, whereby α is integral over A. ■

Corollary 5.3. If B is a finite A-algebra, then B/A is an integral extension. In particular, every element of B is integral over A.

Proposition 5.4. *Let G be a finite group of ring automorphisms of A and let*

$$A^G := \{a \in A \mid g \cdot a = a, \forall g \in G\}.$$

Then, A/A^G *is an integral extension.*

Proof. It is easy to see that A^G is a subring of A. For any $a \in A$, consider the monic polynomial

$$f(x) = \prod_{\sigma \in G} (x - \sigma(a)).$$

This is obviously a polynomial with coefficients in A^G and has x as a root. Thus, x is integral over A^G. ■

Proposition 5.5. *Let* $\{\alpha_i\}_{i=1}^n$ *be elements of B, each integral over A. Then the ring* $A[\alpha_1, \ldots, \alpha_n]$ *is a finitely generated A-module, equivalently, a finite A-algebra.*

Proof. Let A_k denote the subring $A[\alpha_1, \ldots, \alpha_k]$ for $k \geq 1$. We shall induct on k with the convention $A_0 = A$. Obviously A_0 is a finite A-algebra. We have $A_{k+1} = A_k[\alpha_{k+1}]$ and thus is a finite A_k-algebra. But since A_k is a finite A-algebra, so is A_{k+1}, thereby completing the proof. ■

Corollary 5.6. The set C of elements of B which are integral over A is a subring of B containing A.

Proof. Let $\alpha, \beta \in C$. Then, $A[\alpha, \beta]$ is a finite A-algebra. Now, $A \subseteq A[\alpha - \beta] \subseteq A[\alpha, \beta]$ and $A \subseteq A[\alpha\beta] \subseteq A[\alpha, \beta]$ whereby both $\alpha - \beta, \alpha\beta \in C$ and C is a ring. ■

The set C as defined above is called the *integral closure of A in B*. If $C = A$, then A is said to be *integrally closed in B*.

Theorem 5.7. *Let* $A \subseteq B \subseteq C$ *such that* B/A *and* C/B *are integral extensions. Then* C/A *is an integral extension.*

Proof. Let $\alpha \in C$. Then,

$$\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_0 = 0$$

for some $b_i \in B$. Then, α is integral over $B' = A[b_0, \ldots, b_{n-1}]$, consequently, $B'[\alpha]$ is a finite B'-algebra. But since B' is a finite A-algebra, $B'[\alpha]$ is a finite A-algebra and α is integral over A. ■

Corollary 5.8. Let $A \subseteq B$ and C be the integral closure of A in B. Then, C is integrally closed in B.

Proof. Let $\alpha \in B$ be integral over C. Then, $C[\alpha]$ is integral over C, whereby $C[\alpha] = C$. ■

Proposition 5.9. *Let* $A \subseteq B$ *be an integral extension. Then,*

(a) *if* $\mathfrak{b} \subseteq B$ *is an ideal and* $\pi : B \to B/\mathfrak{b}$ *is the canonical surjection, then* $B/\mathfrak{b}$ *is integral over* $\pi(A)$*. In particular, due to the First Isomorphism Theorem, we see that* $B/\mathfrak{b}$ *is integral over a copy of* $A/\mathfrak{a}$ *where* $\mathfrak{a} = \mathfrak{b} \cap A$.

(b) *if* $S \subseteq A$ *is multiplicatively closed, then* $S^{-1}B$ *is integral over* $S^{-1}A$.

Proof. (a) Let $\beta \in B/\mathfrak{b}$, then there is some $\alpha \in B$ such that $\pi(\alpha) = \beta$. Then, there are $a_0, \ldots, a_{n-1} \in A$ such that

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

whereby

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

and the conclusion follows.

(b) Let $\alpha/s \in S^{-1}B$. Since α is integral over A, there are $a_0, \ldots, a_{n-1} \in A$ such that

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

then

$$(\alpha/s)^n + (a_{n-1}/s)(\alpha/s)^{n-1} + \cdots + a_0/s^n = 0$$

which completes the proof. ■

5.1 The Cohen-Seidenberg Theorems

5.1.1 Going Up Theorem

Proposition 5.10. *Let $A \subseteq B$ be an integral extension of integral domains. Then A is a field if and only if B is a field.*

Proof. $\Longrightarrow$ If $x \in B\backslash\{0\}$ is integral over A, then

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

for some $a_i \in A$. Then, $x(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1) = -a_0$, in particular, x is a unit in B.

$\Longleftarrow$ Let $x \in A\backslash\{0\}$. Then, $x^{-1} \in B$ is integral over A and satisfies an equation of the form

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

Multiplying this equation by x^{n-1}, we have

$$x^{-1} = -(a_{n-1} + a_{n-2}x + \cdots + a_0x^{n-1}) \in A,$$

whence A is a field. ■

Proposition 5.11. *Let $A \subseteq B$ be an integral extension, $\mathfrak{q} \subseteq B$ a prime ideal and $\mathfrak{p} = \mathfrak{q}^c = \mathfrak{q} \cap A$. Then $\mathfrak{q}$ is maximal if and only if $\mathfrak{p}$ is maximal.*

Proof. Due to Proposition 5.9, $B/\mathfrak{q}$ is integral over a copy of $A/\mathfrak{p}$. The conclusion now follows from the above proposition. ■

Proposition 5.12. *Let $A \subseteq B$ be an integral extension. Let $\mathfrak{q}, \mathfrak{q}' \subseteq B$ be prime ideals of B such that $\mathfrak{q} \subseteq \mathfrak{q}'$. If $\mathfrak{q} \cap A = \mathfrak{q}' \cap A = \mathfrak{p}$, then $\mathfrak{q} = \mathfrak{q}'$.*

Proof. Let $S = A \backslash \mathfrak{p}$ and treat all rings and ideals as A-modules. Then, $S^{-1}A \subseteq S^{-1}B$ is an integral extension and since $\mathfrak{q} \cap S = \mathfrak{q}' \cap S = \varnothing$, the ideals $S^{-1}\mathfrak{q}$ and $S^{-1}\mathfrak{q}'$ are prime ideals in B such that

$$S^{-1}\mathfrak{q} \cap S^{-1}A = S^{-1}(\mathfrak{q} \cap A) = S^{-1}\mathfrak{p} = S^{-1}(\mathfrak{q}' \cap A) = S^{-1}\mathfrak{q}' \cap S^{-1}A$$

where all the above equalities follow from treating $\mathfrak{p}, \mathfrak{q}, \mathfrak{q}', A$ as A-submodules of B, in particular, due to Proposition 3.7.

But note that $S^{-1}\mathfrak{p}$ is maximal in A whence $S^{-1}\mathfrak{q} = S^{-1}\mathfrak{q}'$ due to the previous proposition. But recall that under localization, the contraction after extension of prime ideals is the prime ideal itself, whereby the contraction of $S^{-1}\mathfrak{q}$ is $\mathfrak{q}$ whence $\mathfrak{q} = \mathfrak{q}'$. ∎

Lemma 5.13. *Let $A \subseteq B$ be rings, B integral over A, and let $\mathfrak{p}$ be a prime ideal of A. Then there is a prime ideal $\mathfrak{q}$ of B such that $\mathfrak{q} \cap A = \mathfrak{p}$.*

5.1.2 Going Down Theorem

Definition 5.14. An integral domain is said to be *normal* if it is integrally closed in its field of fractions.

For example, $\mathbb{Z}$ is integrally closed since the only algebraic integers in $\mathbb{Q}$ are the integers.

Lemma 5.15. *Let $A \subseteq B$ be rings and C the integral closure of A in B. Let $S \subseteq A$ be multiplicatively closed. Then $S^{-1}C$ is the integral closure of $S^{-1}A$.*

Proof. Since C is integral over A, we have that $S^{-1}C$ is integral over $S^{-1}A$. It remains to show that any element that is integral over $S^{-1}A$ is contained in $S^{-1}C$. Indeed, let $b/s \in S^{-1}B$ be an element in $S^{-1}A$ that is contained in the integral closure. Then, there are a_i/s_i such that

$$(b/s)^n + a_{n-1}/s_{n-1}(b/s)^{n-1} + \cdots + a_0/s_0 = 0$$

Let $t = s_1 \cdots s_{n-1}$ and multiply the equation throughout by $(st)^n$ to obtain

$$\frac{(bt)^n + b_{n-1}(bt)^{n-1} + \cdots + b_0}{1} = 0.$$

Thus, there is $u \in S$ such that

$$u\left[(bt)^n + b_{n-1}(bt)^{n-1} + \cdots + b_0\right] = 0$$

Again, multiply the equation by u^{n-1} to obtain

$$(ubt)^n + c_{n-1}(ubt)^{n-1} + \cdots + c_0 = 0,$$

consequently, ubt is integral over A, therefore, lies in C. As a result, $b/s = (ubt)/(sut) \in S^{-1}C$. This completes the proof. ∎

Lemma 5.16. *Let A be an integral domain and $S \subseteq A$ a multiplicatively closed subset. If A is normal, then $S^{-1}A$ is normal.*

Proof. Let K denote the field of fractions of A. Since A is an integral domain, the natural map $A \to S^{-1}A$ is an inclusion. Moreover, the inclusion $A \to K$ maps every element of A to a unit and thus induces an inclusion $S^{-1}A \to K$. We can now treat $A \subseteq S^{-1}A \subseteq K$. Since K is a field, the field of fractions of $S^{-1}A$ must also be contained in K. Therefore, it suffices to show that $S^{-1}A$ is integrally closed in K. But from Lemma 5.15, we see that $S^{-1}A$ is the integral closure of $S^{-1}A$ in $S^{-1}K = K$. This completes the proof. ∎

Proposition 5.17. *Let A be an integral domain. Then, the following are equivalent:*

(a) *A is normal*

(b) *$A_\mathfrak{p}$ is normal for all $\mathfrak{p} \in \operatorname{Spec} A$*

(c) *$A_\mathfrak{m}$ is normal for all $\mathfrak{m} \in \operatorname{MaxSpec} A$*

Proof. $(a) \implies (b)$ follows from the previous lemma and $(b) \implies (c)$ is obvious. We shall show that $(c) \implies (a)$. Let K be the field of fractions of A and C denote the integral closure of A in K. Let $\iota : A \hookrightarrow C$ be the inclusion map. We shall show that ι is a surjection. Note that both A and C are integral domains and $C_\mathfrak{m}$ is the integral closure of $A_\mathfrak{m}$ in K and therefore, in $Q(A_\mathfrak{m})$, consequently, $A_\mathfrak{m} = C_\mathfrak{m}$ due to (c). As a result, $\iota_\mathfrak{m}$ is a surjection for all maximal ideals $\mathfrak{m}$ implying that ι is a surjection. ■

Lemma 5.18. *Let C be the integral closure of A in B and let $\mathfrak{a} \subseteq A$ be an ideal. Then, the integral closure of $\mathfrak{a}$ in B is $\sqrt{\mathfrak{a}^e}$ where the extension is taken through the inclusion $A \hookrightarrow C$.*

Proof. If $x \in C$ is integral over $\mathfrak{a}$, then x satisfies an equationo the form

$$x^r + a_{r-1}x^{r-1} + \cdots + a_0$$

with $a_i \in \mathfrak{a}$. Thus, $x^r \in \mathfrak{a}^e$ whence $x \in \sqrt{\mathfrak{a}^e}$.

Conversely, suppose $x \in \sqrt{a^e}$, then there is a positive integer n such that $x^n \in \mathfrak{a}^e$. Then, $x^n = a_1x_1 + \cdots + a_mx_m$ where each $a_i \in \mathfrak{a}$ and $x_i \in C$. Let $M = A[x_1, \ldots, x_m]$. Since each x_i is integral over A, M is a finitely generated A-module. Let $\phi : M \to M$ be the homomorphism given by $\phi(y) = x^n y$. Then, $\phi(M) \subseteq \mathfrak{a}M$. Thus, ϕ satisfies and equation of the form

$$\phi^r + a_{r-1}\phi^{r-1} + \cdots + a_0\mathbf{id} = 0$$

whre $a_i \in \mathfrak{a}$. Thus, x is integral over $\mathfrak{a}$. ■

Proposition 5.19. *Let $A \subseteq B$ be integral domains with A integrally closed. Let $\alpha \in B$ be integral over an ideal $\mathfrak{a}$ of A. Then α, viewed as an element of $L := Q(B) \supseteq Q(A) =: K$ is algebraic over the field of fractions K of A. Further, if the minimal polynomial of α over K is given by $x^n + a_{n-1}x^{n-1} + \cdots + a_0$, then each a_i is an element of $\sqrt{\mathfrak{a}}$.*

Proof. Let $\alpha_1, \ldots, \alpha_k$ be the distinct conjugates of α in $\overline{K}$, an algebraic closure of K containing L. Then, each α_i is integral over $\mathfrak{a}$. The irreducible polynomial of α over K is given by

$$\prod_{i=1}^{k} (x - \alpha_i)^e$$

for some exponent e. In particular, the coefficients of the non-leading terms are polynomials in th α_i's whence are integral over $\mathfrak{a}$ and also lie in A, whence are elements of $\sqrt{\mathfrak{a}}$. This completes the proof. ■

Theorem 5.20 (Going Down Theorem). *Let $A \subseteq B$ be an integral extension of integral domains with A integrally closed. Suppose $\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$ are prime ideals in A and correspondingly $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$ are prime ideals in B with $m < n$ and $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $1 \leq i \leq m$, then there are prime ideals $\mathfrak{q}_{m+1} \supseteq \mathfrak{q}_n$ with $\mathfrak{q}_m \supseteq \mathfrak{q}_{m+1}$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $m < i \leq n$.*

Proof. We shall prove this in the case $m = 1$ and $n = 2$. This obviously suffices to prove the theorem in its full generality. Consider the composition of maps

$$A \longrightarrow B \longrightarrow B_{\mathfrak{q}_1}$$

where the composition shall be denoted by $f : A \to B_{\mathfrak{q}_1}$. It suffices to show that there is a prime in $B_{\mathfrak{q}_1}$ contracting to $\mathfrak{p}_2$. Due to Theorem 3.23, it suffices to show that $\mathfrak{p}^{ec} = \mathfrak{p}$ where the extension and contraction is taken with respect to f.

Let $x \in \mathfrak{p}_2 B_{\mathfrak{q}_1}$. Then, $x = y/s$ for some $y \in B\mathfrak{p}_2$ and $s \in S$. Note that s is integral over the ideal (1) in A and thus its minimal polynomial over K is of the form

$$t^r + a_{r-1}t^{r-1} + \cdots + a_0$$

where $a_i \in A$.

Now, $y \in B$ and lies in $\mathfrak{p}_2 B \subseteq \sqrt{\mathfrak{p}_2 B}$ whence is integral over $\mathfrak{p}_2$ and hence its minimal polynomial over K is of the form

$$t^{r'} + b_{r'-1}t^{r'-1} + \cdots + b_0$$

with $b_i \in \sqrt{\mathfrak{p}_2} = \mathfrak{p}_2$. Since $s = y/x$ in $Q(B)$, the minimal polynomials of s and y over K must have the same degree, that is, $r = r'$ and $b_i = x^{r-i}a_i$ for $0 \le i \le r-1$. If $x \notin \mathfrak{p}_2$, then $a_i \in \mathfrak{p}_2$ for $0 \le i \le r-1$, which would imply $s^r \in \mathfrak{p}_2 B \subseteq \mathfrak{p}_1 B \subseteq \mathfrak{q}_1$, i.e. $s \in \mathfrak{q}_1$, which is absurd. Thus, $x \in \mathfrak{p}_2$ whence $\mathfrak{p}_2^{ec} \subseteq \mathfrak{p}_2$, which completes the proof. ∎

5.1.3 Another Proof of the Going Down Theorem

Lemma 5.21. *Let $A \subseteq B$ be an integral extension of integral domains. If $S = A \backslash \{0\}$, then $S^{-1}B = Q(B)$, the field of fractions of B and the extension $Q(B)/Q(A)$ is algebraic.*

Proof. Note that $Q(A) \subseteq S^{-1}B$ is an integral extension of integral domains and hence, $S^{-1}B$ is a field that is contained in $Q(B)$, whence, is equal to $Q(B)$. The assertion about algebraic extensions follows from the integrality of the extension. ∎

Lemma 5.22. *Let L/K be a normal extension of fields with $G = \mathrm{Aut}(L/K)$. Let A be an integrally closed subring of $K = Q(A)$, B the integral closure of A in L. Then, for any prime $\mathfrak{p} \in \mathrm{Spec}(A)$, G acts transitively on the fiber of $\mathfrak{p}$ in $\mathrm{Spec}(B)$.*

That G acts on each fiber is trivial to see. Only the transitivity of the action must be demonstrated.

Proof. First, suppose L/K is a Galois extension. That the statement is true for finite Galois extensions is common knowledge. We know that

$$\mathrm{Gal}(L/K) = \varprojlim_{E} \mathrm{Gal}(E/K)$$

where E ranges over all finite Galois extensions of K. Let $\mathfrak{q}, \mathfrak{q}'$ be primes lying over $\mathfrak{p}$. For every finite Galois subextension E of L/K, let C_E denote the integral closure of A in E and $\mathfrak{p}_E, \mathfrak{p}'_E$ the respective contractions of $\mathfrak{q}, \mathfrak{q}'$. We know that there is a collection $\{\sigma_E\} \in \mathrm{Gal}(E/K)$ such that $\sigma_E(\mathfrak{p}_E) = \mathfrak{p}'_E$. Note that the inverse image of this set in $\mathrm{Gal}(L/K)$ is a closed (and hence compact) set, which we shall denote by S_E.

If $E_1, \ldots, E_n$ are finite Galois subextensions of L, then their compositum $F = E_1 \cdots E_n$ is a finite Galois subextension and hence,

$$\varnothing \neq S_F \subseteq \bigcap_{i=1}^{n} S_{E_i},$$

that is, $\{S_E\}$ has the finite intersection property and there is a $\sigma \in \bigcap S_E$, which is the required automorphism taking $\mathfrak{q}$ to $\mathfrak{q}'$.

Now, suppose L/K is normal and $F = L^G$. Then, L/F is Galois and F/K is purely inseparable. Let C denote the integral closure of A in F. We claim that there is precisely one prime in C lying over $\mathfrak{p} \in \operatorname{Spec}(A)$. Indeed, consider

$$\mathfrak{q} = \{x \in C \mid \exists\, n > 0,\ x^{p^n} \in \mathfrak{p}\}.$$

It is not hard to show that $\mathfrak{q}$ is a prime ideal in C and lies over $\mathfrak{p}$. Further, any prime ideal $\mathfrak{q}'$ lying over $\mathfrak{p}$ must contain $\mathfrak{q}$, consequently, must be equal to $\mathfrak{q}$. ■

Theorem 5.23 (Going Down Theorem). *Let $A \subseteq B$ be an integral extension of integral domains with A integrally closed. Suppose $\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$ are prime ideals in A and correspondingly $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$ are prime ideals in B with $m < n$ and $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $1 \le i \le m$, then there are prime ideals $\mathfrak{q}_{m+1} \supseteq \mathfrak{q}_n$ with $\mathfrak{q}_m \supseteq \mathfrak{q}_{m+1}$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $m < i \le n$.*

Proof. We shall prove this in the case $m = 1$ and $n = 2$, which obviously suffices to prove the theorem in its full generality. Let K denote the fraction field of A and L that of B. Let L' denote the normal closure of L in $\overline{L}$, the algebraic closure containing L and C the integral closure of A in L'. Let $\mathfrak{P}_1$ denote a prime in C lying over $\mathfrak{q}_1$ (hence, over $\mathfrak{p}_1$) and $\mathfrak{P}$ a prime in C lying over $\mathfrak{p}_2$. Due to the Going Up Theorem, there is a prime $\mathfrak{P}' \supseteq \mathfrak{P}$ in C lying over $\mathfrak{p}_1$. Since $\operatorname{Aut}(L'/K)$ acts transitively on the fiber of any prime, there is an automorphism $\sigma \in \operatorname{Aut}(L'/K)$ such that $\sigma(\mathfrak{P}') = \mathfrak{P}_1$. Then, $\mathfrak{P}_2 = \sigma(\mathfrak{P})$ is a prime in C lying over $\mathfrak{p}_2$ that is contained in $\mathfrak{P}_1$.

Let $\mathfrak{q}_2 = \mathfrak{P}_2 \cap B$. Then, $\mathfrak{q}_2$ is a prime in B lying over $\mathfrak{p}_2$ that is contained in $\mathfrak{q}_1$. This completes the proof. ■

Corollary 5.24. Let $A \subseteq B$ be an integral extension of integral domains with A integrally closed. If $\mathfrak{q} \in B$ is a prime and $\mathfrak{p} = \mathfrak{q} \cap B$, then $\operatorname{ht}(\mathfrak{q}) = \operatorname{ht}(\mathfrak{p})$.

5.2 Field Theory Arguments

Definition 5.25. Let V be a finite dimensional vector space over a field k. A *bilinear form* on V is a k-bilinear map $\psi : V \times V \to k$. The form ψ is said to be *non-degenerate* if the *left kernel*,

$$\{v \in V \mid \psi(v, x) = 0 \text{ for all } x \in V\} = 0.$$

Lemma 5.26. *If $e_1, \ldots, e_n$ is a basis for V and ψ a non-degenerate bilinear form, then there is a basis $f_1, \ldots, f_n$ of V such that $\psi(f_i, e_j) = \delta_{ij}$. We shall call this the dual basis of $\{e_i\}$ with respect to ψ.*

Proof. Consider the map $\Phi : V \to V^\vee$ given by

$$\Phi(v) = \psi(v, \cdot).$$

This is an injective map since ψ is non-degenerate and thus, an isomorphism. Let $\phi_i : V \to k$ be the map defined on basis elements by $\phi_i(e_j) = \delta_{ij}$. Due to surjectivity, there is some $f_i \in V$ such that $\Phi(f_i) = \phi_i$. The f_i's must be linearly independent since the ϕ_i's are linearly independent as elements of $V^\vee$. This completes the proof. ■

Theorem 5.27. *Let A be an integrally closed integral domain with field of fractions K, L/K a separable extension of degree m and B the integral closure of A in L Then, there are free A-submodules M and M' of L such that*

$$M \subseteq B \subseteq M'.$$

Proof. It is quite obvious that there is an integral basis for L over K, i.e. a K-basis $\{\beta_1, \ldots, \beta_m\}$ with $\beta_i \in B$ for $1 \leq i \leq m$. Let $M = A\beta_1 + \cdots + A\beta_m \subseteq B$. Consider the bilinear form $\langle \cdot, \cdot \rangle : L \times L \to K$ given by

$$\langle x, y \rangle = \mathrm{Tr}_K^L(xy),$$

which is a non-degenerate bilinear form and thus admits a dual basis of $\{\beta_i\}$ with respect to $\langle \cdot, \cdot \rangle$, say $\{\beta_i'\}$. Let $M' = A\beta_1' + \cdots + A\beta_m'$. We shall show that $B \subseteq M'$. For any $b \in B$, there are b_i's such that

$$b = b_1\beta_1' + \cdots + b_m\beta_m'. \tag{5.1}$$

Then,

$$b_i = \langle b, \beta_i \rangle = \mathrm{Tr}_K^L(b\beta_i) \in A,$$

since $b\beta_i$ is integral over A and A is integrally closed. This completes the proof. ∎

Corollary 5.28. With the above setup, if A is noetherian, then so is B. On the other hand, if A is a PID, then B is a free A-module.

Theorem 5.29 (Extension Lemma for Rings). *Let Ω be an algebraically closed field and B/A an integral extension of rings. If $\sigma : A \to \Omega$ is a ring homomorphism, then it can be extended to $\widetilde{\sigma} : B \to \Omega$.*

Proof. Let $\mathfrak{p} = \ker \sigma$, which is a prime ideal and let $\mathfrak{q}$ be a prime ideal in B lying over $\mathfrak{p}$. Due to the First Isomorphism Theorem, there is an induced map $\phi : A/\mathfrak{p} \to \Omega$. Using the universal property of the fraction field, there is an induced map $\psi : Q(A/\mathfrak{p}) \to \Omega$. Note that $A/\mathfrak{p} \subseteq B/\mathfrak{q}$ and thus $Q(A/\mathfrak{p}) \subseteq Q(B/\mathfrak{q})$. Now, using the extension lemma for fields, there is an induced map $\widetilde{\psi} : Q(B/\mathfrak{q}) \to \Omega$ extending ψ. Composing this map with the inclusion $B/\mathfrak{q} \hookrightarrow Q(B/\mathfrak{q})$, we obtain a map $\widetilde{\phi} : B/\mathfrak{q} \to \Omega$ extending ϕ. Finally, composing this map with the surjection $B \twoheadrightarrow B/\mathfrak{q}$, we obtain a map $\widetilde{\sigma} : B \to \Omega$ extending σ. This completes the proof. ∎

Lemma 5.30. *Let A be a subring of a field K and $x \in K^\times$. Let $\varphi : A \to \Omega$ be a ring homomorphism into an algebraically closed field Ω. Then φ has an extension to a homomorphism of either $A[x]$ or $A[x^{-1}]$ into Ω.*

Proof. First, let $\mathfrak{p} = \ker \varphi$. As we have seen earlier, we may extend φ to a ring homomorphism $\varphi : A_\mathfrak{p} \to \Omega$. Hence, we may suppose that A is local with maximal ideal $\mathfrak{m}$.

Suppose first that ∎

proof in lang seems fishy

5.3 Noether's Normalization Lemma

Lemma 5.31. *Let k be a field and $F \in k[X_1, \ldots, X_n]$ a non-constant polynomial. Then there is a k-algebra automorphism*

$$\varphi : k[X_1, \ldots, X_n] \to k[X_1, \ldots, X_n]$$

such that $\varphi(X_n) = X_n$ and

$$\varphi(F) = aX_n^d + f_{d-1}X_n^{d-1} + \cdots + f_1X_n + f_0$$

where $f_i \in k[X_1, \ldots, X_{n-1}]$ for $1 \leq i \leq d-1$.

Proof. We shall pick an automorphism of the form $\varphi(X_i) = X_i + X_n^{t_i}$ for some positive integer t_i for each $1 \leq i \leq n-1$. We shall choose these t_i's at the end of the proof.

First, note that for $1 \leq i \leq n-1$, $\varphi(X_i - X_n^{t_i}) = X_i$ whence φ is a surjection. Since $k[X_1, \ldots, X_n]$ is a noethering, φ is an isomorphism.

Let $\Lambda \subseteq \mathbb{N}^n$ be a finite subset such that

$$F = \sum_{\alpha \in \Lambda} a_\alpha X^\alpha$$

where $a_\alpha \in k^\times$ for each $\alpha \in \Lambda$. For each $\alpha \in \Lambda$, define $\omega(\alpha) = t_1\alpha_1 + \cdots + t_{n-1}\alpha_{n-1} + \alpha_n$.

Choose a positive integer N greater than

$$\max_{\alpha \in \Lambda} \max_{1 \leq i \leq n} \alpha_i$$

and set $t_i = N^i$ for $1 \leq i \leq n-1$. It is not hard to see that all the $\omega(\alpha)$'s are distinct.

We have

$$\varphi(F) = \sum_{\alpha \in \Lambda} \left(a_\alpha \prod_{i=1}^{n-1} (X_i + X_n^{t_i})^{\alpha_i} \right) X_n^{\alpha_n}$$

and since the $\omega(\alpha)$'s are distinct, there is a unique term in the above expansion that contributes to the term with maximum exponent of X_n whence the coefficient of this term is a constant in $K^\times$. This completes the proof. ■

Theorem 5.32 (Noether Normalization). *Let k be a field and A a finitely generated k-algebra. Then, there are $z_1, \ldots, z_m \in A$ such that*

(a) $z_1, \ldots, z_m$ are algebraically independent over k[a]. That is, the evaluation map

$$\mathbf{ev} : k[X_1, \ldots, X_m] \twoheadrightarrow k[z_1, \ldots, z_m]$$

from the ring of polynomials in m variables over k is an isomorphism.

(b) A is integral over $k[z_1, \ldots, z_m]$.

[a] $m = 0$ is permitted

Proof. We shall prove this statement by induction on the cardinality n of the smallest generating set of A as a k-algebra. The base case with $n = 0$ is trivial. Since A is a finitely generated k-algebra, there is a surjective ring homomomrphism

$$\pi : k[X_1, \ldots, X_n] \twoheadrightarrow A.$$

Choose a non-constant polynomial $G \in \ker \pi$. Due to Lemma 5.31, there is an automorphism φ of $k[X_1, \ldots, X_n]$ which sends G to a polynomial F of the form

$$aX_n^d + f_{d-1}X_n^{d-1} + \cdots + f_1 X_n + f_0$$

where $a \in k^\times$. We now have the following sequence of ring homomorphisms

$$k[X_1, \ldots, X_n] \xrightarrow{\varphi^{-1}} k[X_1, \ldots, X_n] \xrightarrow{\pi} A$$

with $F \in \ker(\pi \circ \varphi^{-1})$. Let $x_i = (\pi \circ \varphi^{-1})(X_i)$, then, $F(x_1, \ldots, x_n) = 0$. That is,

$$x_n^d + a^{-1} f_{d-1}(x_1, \ldots, x_{n-1}) x_n^{d-1} + \cdots + a^{-1} f_0(x_0, \ldots, x_{n-1}) = 0,$$

and thus, x_n is algebraic over $B = k[x_1, \ldots, x_{n-1}]$. Due to the induction hypothesis, there are algebraically independent $z_1, \ldots, z_m \in B$ such that B is integral over $k[z_1, \ldots, z_m]$.

We have shown that x_n is integral over B and thus $B \subseteq A$ is an integral extension whence $k[z_1, \ldots, z_m] \subseteq A$ is an integral extension. This completes the proof. ■

5.3.1 Stronger NNL

Theorem 5.33. *Let A be a finitely generated k-algebra and let $\mathfrak{a}_1 \subseteq \cdots \subseteq \mathfrak{a}_p$ be an increasing chain of ideals in A, with $\mathfrak{a}_p \neq (1)$. Then, there is an integer $n > 0$ and algebraically independent $x_1, \ldots, x_n \in A$, such that*

(a) A is integral over $B = k[x_1, \ldots, x_n]$

(b) for each $1 \leq i \leq p$, there is an integer $h(i) \geq 0$ such that $\mathfrak{a}_i \cap B$ is generated by $(x_1, \ldots, x_{h(i)})$.

Proof. Note that it suffices to prove the theorem when A is a polynomial algebra $A' = k[Y_1, \ldots, Y_m]$, for we can write A as a quotient of such a polynomial algebra and replace each $\mathfrak{a}_i$ by its preimage in A', say $\mathfrak{a}_i'$. If $\{x_1', \ldots, x_n'\}$ are in A' satisfying the statement of the theorem, then the images $\{x_1, \ldots, x_n\}$ in A satisfy the statement of the theorem for A. Henceforth, we suppose that $A = k[Y_1, \ldots, Y_m]$ and argue by induction on p.

Suppose $p = 1$. ■

complete NNL

5.3.2 Various Forms of the Nullstellensatz

Lemma 5.34 (Zariski's Lemma). *Let K/k be an extension of fields such that K is a finitely generated k-algebra. Then, K/k is a finite extension.*

Proof. According to Theorem 5.32, there are $z_1, \ldots, z_m \in K$ such that K is integral over $k[z_1, \ldots, z_m]$, which is an integral domain whence a field due to Proposition 5.10. We note that m may not be positive since a polynomial ring can never be a field. Hence, K/k is algebraic and since K is a finitely generated k-algebra, the extension K/k must be finite. ■

Theorem 5.35 (Hilbert's Nullstellensatz, Weak Form 1). *Let k be an algebraically closed field. Then, any maximal ideal in $k[x_1, \ldots, x_n]$ is of the form $(x_1 - a_1, \ldots, x_n - a_n)$.*

Proof. It suffices to show the converse. Let $\mathfrak{m}$ be a maximal ideal in $k[x_1, \ldots, x_n]$. We now have a commutative diagram

$$\begin{array}{ccc} k & \xhookrightarrow{\iota} & k[x_1, \ldots, x_n] \\ & \underset{\varphi}{\searrow} & \downarrow \pi \\ & & k[x_1, \ldots, x_n]/\mathfrak{m} = K \end{array}$$

where $\varphi := \pi \circ \iota$.

The map φ gives K the structure of a finitely generated k-algebra and thus φ is surjective (since k is algebraically closed). Let $\pi(x_i) = a_i$ for $1 \leq i \leq n$. Due to the surjectivity of φ, for each a_i, there is some $a_i' \in k$ with $\varphi(a_i') = a_i$ whence $\pi(x_i - a_i') = 0$ and

$$(x_1 - a_1', \ldots, x_n - a_n') \subseteq \mathfrak{m}.$$

But since the former is a maximal ideal, we must have equality. ■

Theorem 5.36 (Hilbert's Nullstellensatz, Weak Form 2). *Let k be an algebraically closed field and $S \subseteq k^n$. Then, $I(S) = (1)$ if and only if $S = \varnothing$.*

Proof. ($\Longrightarrow$) If $S \neq \varnothing$, then let $a = (a_1, \ldots, a_n)$ be a point in S. Then, $I(S) \subseteq \mathfrak{m}_a = (x_1 - a_1, \ldots, x_n - a_n)$. ($\Longleftarrow$) If $I(S) \neq (1)$, then it is contained in some maximal ideal $\mathfrak{m} = \mathfrak{m}_a$ for some $a \in k^n$, whence $a \in S$. This completes the proof. ■

Theorem 5.37 (Hilbert's Nullstellensatz, Strong Form). *Let* $\mathfrak{a} \subseteq k[x_1, \ldots, x_n]$ *be an ideal. Then,*

$$I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$$

The following proof is due to Rabinowitsch.

Proof. First, note that the inclusion $\sqrt{\mathfrak{a}} \subseteq I(V(\mathfrak{a}))$ is obvious for if $f \in \sqrt{\mathfrak{a}}$, then there is a positive integer r such that $f^r \in \mathfrak{a}$ whence f^r vanishes at all points in $V(\mathfrak{a})$ and thus $f^r \in I(V(\mathfrak{a}))$.

We shall now prove the other inclusion. Since $\mathfrak{a}$ is finitely generated, let $f_1, \ldots, f_m$ be a set of generators for $\mathfrak{a}$ and let $f \in I(V(\mathfrak{a}))$. Consider now the ring $B = k[x_0, x_1, \ldots, x_n]$ which contains $A = k[x_1, \ldots, x_n]$ as a subring and treat all polynomials as elements of B. The polynomials

$$f_1, \ldots, f_m, 1 - x_0 f$$

do not have any common zeros. Let $\mathfrak{b} \subseteq B$ denote the ideal generated by these polynomials. Due to Theorem 5.36 and the fact that the polynomials have no common zeros, we must have $\mathfrak{b} = B$. Consequently, there are polynomials $g_0, \ldots, g_n \in k[x_1, \ldots, x_n]$ such that

$$1 = g_0(1 - x_0 f) + g_1 f_1 + \cdots + g_m f_m.$$

Consider now the evaluation map $\mathbf{ev} : B \to k(x_1, \ldots, x_n)$ which maps $x_0 \mapsto 1/f$ and $x_i \mapsto x_i$ for $1 \le i \le n$. It is not hard to see that this is a ring homomorphism. Under this map, the above equality transforms to

$$1 = g_1(1/f, x_1, \ldots, x_n) f_1(x_1, \ldots, x_n) + \cdots + g_m(1/f, x_1, \ldots, x_n) f_m(x_1, \ldots, x_m).$$

Since all the g_i's and f_i's are polynomials, we may clear out the denominators by multiplying with a suitable power of f, say f^N. Then, we have

$$f^N = h_1(x_1, \ldots, x_n) f_1 + \cdots + h_m(x_1, \ldots, x_n) f_m$$

whereby $f^N \in \mathfrak{a}$ for some positive integer N and equivalently, $f \in \sqrt{\mathfrak{a}}$. This completes the proof. ■

Lemma 5.38. *Let* $A \subseteq C \subseteq B$ *be an extension of rings such that* C *is the integral closure of* A *in* B. *Suppose* $f, g \in B[x]$ *such that* $fg \in C[x]$. *Then,* $f, g \in C[x]$.

Proof. We first begin with an auxiliary result.
Claim. There is a ring D containing B in which $f(x)$ splits into linear factors.
Proof. It suffices to show that there is a ring D in which $f(x)$ has a root. Let R denote the ring $B[T]/(f(T))$. This comes equipped with a natural injection $B \hookrightarrow R$ and hence, we may suppose that $B \subseteq R$. Note that $\overline{T} \in R$ is a root of $f(x)$ which proves the claim. □

Using the above claim, let D be a ring containing B in which both f and g split. Let

$$f(x) = \prod (x - \alpha_i) \qquad g(x) = \prod (x - \beta_j).$$

Then, each α_i, β_j is a root of $fg \in C[x]$, whence is integral over C. Since integral elements form a ring, the coefficients of f and g, being polynomials in the α_i's and β_j's respectively, are integral over C and lie in B, hence, they lie in C. This completes the proof. ■

Theorem 5.39. *Let* $A \subseteq C \subseteq B$ *be an extension of rings such that* C *is the integral closure of* A *in* B. *Then,* $C[x]$ *is the integral closure of* $A[x]$ *in* $B[x]$.

Proof. First, we shall show that the integral closure of $A[x]$ in $B[x]$ is contained in $C[x]$. Suppose $f(x) \in B[x]$ is integral over $A[x]$. Then,

$$f^m + g_{m-1}f^{m-1} + \cdots + g_0 = 0$$

for some $g_i \in A[x]$. Let r be a positive integer greater than the degree of each g_i and f. Let $f_1(x) = f(x) - x^r \in A[x]$. Then,

$$(f_1 + x^r)^m + g_{m-1}(f + x^r)^{m-1} + \cdots + g_0 = 0,$$

which is a monic polynomial in x. Expanding it out, we have an equation of the form

$$f_1^m + h_{m-1}f_1^{m-1} + \cdots + h_0 = 0,$$

for some $h_i \in A[x]$. Note that f_1 is a monic polynomial and thus, so is

$$f_1^{m-1} + h_{m-1}f_1^{m-2} + \cdots + h_1.$$

Using the preceeding lemma, we see that $f_1 \in C[x]$, whence $f \in C[x]$.

We must now show the converse. Let $f(x) \in C[x]$ where $f(x) = c_m x^m + \cdots + c_0$. Then, $f(x) \subseteq A[x][c_0, \ldots, c_m]$, which is a finitely generated $A[x]$-module (since $A[c_0, \ldots, c_m]$ is a finitely generated A-module), whence $f(x)$ is integral over $A[x]$. This completes the proof. ■

5.4 Jacobson Rings

Theorem 5.40. *The following are equivalent:*

(a) Every prime ideal in A is an intersection of maximal ideals.

(b) In every homomorphic image of A, the nilradical is equal to the Jacobson radical.

(c) Every prime ideal in A which is not maximal is equal to the intersection of the prime ideals strictly containing it.

Proof. $(a) \implies (b)$ Any homomorphic image of A can be treated as $A/\mathfrak{a}$ where $\mathfrak{a}$ is an ideal in A. If $\mathfrak{a} = A$, then there is nothing to prove. Suppose now that $\mathfrak{a}$ is a proper ideal. Note that $\mathfrak{R}(A/\mathfrak{a})$ is the intersection of all maximal ideals in $A/\mathfrak{a}$, which is the image of the intersection of all maximal ideals containing $\mathfrak{a}$ in A, due to the ideal correspondence. But the intersection of all maximal ideals containing $\mathfrak{a}$ is the same as the intersection of all prime ideals containing $\mathfrak{a}$ which is the contraction of the nilradical of $A/\mathfrak{a}$. Thus, $\mathfrak{N}(A/\mathfrak{a}) = \mathfrak{R}(A/\mathfrak{a})$.

$(b) \implies (c)$ Let $\mathfrak{p}$ be a prime ideal in A. Then, $\sqrt{\mathfrak{p}}$ is the intersection of all maximal ideals containing it whence $\mathfrak{p}$ is the intersection of all prime ideals strictly containing it.

$(c) \implies (a)$ Suppose there is a prime ideal $\mathfrak{p}$ in A which is not an intersection of maximal ideals. Consider some

$$f \in \mathfrak{p} \setminus \bigcap_{\mathfrak{m} \supseteq \mathfrak{p}} \mathfrak{m}.$$

The poset $\Sigma = \{\mathfrak{a} \trianglelefteq A \mid f \notin \mathfrak{a}\}$ is nonempty (since it contains $\mathfrak{p}$) and has a maximal element, say $\mathfrak{q}$, which is also prime. Due to maximality, any prime containing $\mathfrak{q}$ must contain f and hence, $\mathfrak{q}$ cannot be the intersection of the primes strictly containing it. ■

Definition 5.41 (Jacobson Ring). The ring A is said to be *Jacobson* if it satisfies the equivalent conditions of Theorem 5.40.

Chapter 6

Noetherian and Artinian Rings and Modules

6.1 Chain Conditions

A totally ordered sequence $\{x_n\}_{n=1}^{\infty}$ in the poset $(\Sigma, \leqq)$ is said to be *stationary* if there is an index n such that $x_n = x_{n+1} = \cdots$.

Definition 6.1. An A-module M is said to be *noetherian* or equivalently said to satisfy the *ascending chain condition* if every chain in the poset of submodules of M ordered by $\subseteq$ is stationary.

Similarly, M is said to be *artinian* equivalently said to satisfy the *descending chain condition* if every chain in the poset of submodules of M ordered by $\supseteq$ is stationary.

A ring A is said to be noetherian (resp. artinian) if it is noetherian (resp. artinian) as an A-module.

Proposition 6.2. *Let $(\Sigma, \leqq)$ be a poset. Then, the following are equivalent:*

(a) Every chain in Σ is stationary.

(b) Every subset of Σ has a maximal element.

The proof is omitted owing to its triviality.

Lemma 6.3. *An A-module M is noetherian if and only if every submodule is finitely generated.*

Proof. ■

Corollary 6.4. A ring A is noetherian if and only if every ideal is finitely generated.

Corollary 6.5. Every submoule of a noetherian A-module is noetherian.

Proposition 6.6. *M is a noetherian (resp. artinian) A-module if and only if it is a noetherian (resp. artinian) $A/\operatorname{Ann}_A(M)$-module.*

Proof. Since the poset of $A/\operatorname{Ann}_A(M)$-submodules of M is the same as the poset of A-submodules of M, the conclusion follows. ■

Lemma 6.7 (2/3-lemma). *Consider the short exact sequence $0 \to M' \to M \to M'' \to 0$. Then M is noetherian (resp. artinian) if and only if both M' and M'' are noetherian (resp. artinian).*

Proof. ■

Corollary 6.8. Let $\{M_i\}_{i=1}^n$ be A-modules. Then, $\bigoplus_{i=1}^{n} M_i$ is noetherian (resp. artinian) if and only if each M_i is noetherian (resp. artinian).

Proof. The forward direction is obvious. For the converse, induct on n using the short exact sequence:

$$0 \longrightarrow M_n \longrightarrow \bigoplus_{i=1}^{n} M_i \longrightarrow \bigoplus_{i=1}^{n-1} M_i \longrightarrow 0$$

■

Proposition 6.9. *If A is a noethering (resp. artinian ring), then so is $A/\mathfrak{a}$ for any ideal $\mathfrak{a}$ in A.*

Proof. $A/\mathfrak{a}$ is a noetherian (resp. artinian) A-module and thus a noetherian (resp. artinian) $A/\mathfrak{a}$-module. ■

Proposition 6.10. *Let A be a noetherian (resp. artinian) ring and M a finitely generated A-module. Then, M is noetherian (resp. artinian).*

Proof. Let $\{m_1, \ldots, m_n\}$ be a set of generators of M. Then, there is a surjection $A^n \twoheadrightarrow M$ given by

$$(a_1, \ldots, a_n) \mapsto a_1 m_1 + \cdots + a_n m_n.$$

Since A^n is a noetherian (resp. artinian) A-module, so is M. ■

Proposition 6.11. *Let M be an A-module and $\phi \in \operatorname{End}_A(M)$.*

(a) If M is noetherian and ϕ is surjective, then ϕ is injective.

(b) If M is artinian and ϕ is injective, then ϕ is surjective.

Proof. (a) Consider the ascending chain of submodules

$$\ker \phi \subseteq \ker \phi^2 \subseteq \cdots$$

Since M is noetherian, there is an index n such that $\ker \phi^n = \ker \phi^{n+1}$. Let $x \in \ker \phi^n$. Due to the surjectivity of ϕ, there is $y \in M$ such that $\phi(y) = x$, whence $\phi^{n+1}(y) = 0$ and $y \in \ker \phi^{n+1} = \ker \phi^n$. Therefore, $\ker \phi^n = 0$ and ϕ is injective.

(b) Consider the descending chain of submodules

$$\operatorname{im}\phi \supseteq \operatorname{im}\phi^2 \supseteq \cdots$$

Since M is artinian, there is an index n such that $\operatorname{im}\phi^n = \operatorname{im}\phi^{n+1}$. Then, for every $x \in M$, there is $y \in M$ such that $\phi^n(x) = \phi^{n+1}(y)$, whence $x = \phi(y)$, this establishes surjectivity. ∎

Lemma 6.12. *"Noetherian-ness" is not a local property.*

Proof. Let $A = \mathbb{F}_2 \times \mathbb{F}_2 \times \cdots$ and $\mathfrak{p} \in \operatorname{Spec}(A)$. Note that every element in A is an idempotent. Therefore, every element in $A_\mathfrak{p}$ is also an idempotent. Consequently, for all $x \in A_\mathfrak{p}$, $x(1-x) = 0$. Note that either x or $1-x$ must be a unit lest $1 = x + (1-x)$ be a non-unit. Thus, either $x = 0$ or $1 - x = 0$, equivalently, $x = 1$. Thus, $A_\mathfrak{p} \cong \mathbb{F}_2$. ∎

Remark 6.1.1. *Instead of choosing $A = \mathbb{F}_2 \times \mathbb{F}_2 \times \cdots$, any product of fields works but the proof in the general case requires a bit more machinery. Indeed, if A is an infinite product of fields, then A is absolutely flat, consequently, every localization of A at a prime ideal is a local absolutely flat ring, whence a field, which is noetherian.*

6.2 Length of Modules

Lemma 6.13. *Supose there is a sequence of maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ in A such that $(0) = \mathfrak{m}_1 \cdots \mathfrak{m}_n$. Then, A is a noethering if and only if it is artinian.*

Proof. Suppose A is noetherian. We have the chain of ideals

$$A \supseteq \mathfrak{m}_1 \supseteq \cdots \supseteq \mathfrak{m}_1 \cdots \mathfrak{m}_n = 0$$

Note that each factor $\mathfrak{m}_1 \cdots \mathfrak{m}_{i-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_i$ is a noetherian A-module and thus a noetherian $k_i = A/\mathfrak{m}_i$-module and thus a k_i-vector space satisfying a.c.c whence it satisfies d.c.c and is an artinian $A/\mathfrak{m}_i$-module whence an artinian A-module. We now have a short exact sequence

$$0 \longrightarrow \mathfrak{m}_1 \cdots \mathfrak{m}_{i+1} \longrightarrow \mathfrak{m}_1 \cdots \mathfrak{m}_i \longrightarrow \mathfrak{m}_1 \cdots \mathfrak{m}_{i+1}/\mathfrak{m}_1 \cdots \mathfrak{m}_i \longrightarrow 0$$

Inducting downwards from $\mathfrak{m}_1 \cdots \mathfrak{m}_n = (0)$ (which is clearly artinian) with the repeated usage of Lemma 6.7, we are done. ∎

Lemma 6.14 (Fitting). *Let R be any ring and M a finite-length module. If $f \in \operatorname{End}_R(M)$, then for any sufficiently large n, $M \cong \operatorname{im}(f^n) \oplus \ker(f^n)$.*

Proof. We have the sequences

$$\operatorname{im}(f) \supseteq \operatorname{im}(f^2) \supseteq \cdots \qquad \ker(f) \subseteq \ker(f^2) \subseteq \cdots.$$

Hence, for sufficiently large n, $\ker(f^n) = \ker(f^{n+1}) = \cdots$ and $\operatorname{im}(f^n) = \operatorname{im}(f^{n+1}) = \cdots$. Choose any $x \in M$. Then, there is some $y \in M$ such that $f^n(x) = f^{2n}(y)$, consequently, $x - f^n(y) \in \ker(f^n)$, whence $M = \ker(f^n) + \operatorname{im}(f^n)$.

On the other hand, if $x \in \ker(f^n) \cap \operatorname{im}(f^n)$, then there is some $y \in M$ such that $f^n(y) = x$. Consequently, $f^{2n}(y) = 0$, whence $y \in \ker(f^{2n}) = \ker(f^n)$, thus, $x = f^n(y) = 0$. This shows that $M \cong \ker(f^n) \oplus \operatorname{im}(f^n)$. ∎

6.3 Noetherian Rings

Recall that A is a noetherian ring if it is a noetherian A-module. One must take note that a noethering need not have finite Krull dimension[1] on the other hand, it is not even true that local rings with dimension zero are noetherian. In particular, consider the ring $R = k[x_1, x_2, \dots]/(x_1, x_2^2, \dots)$. Obviously A is not noetherian, owing to the strictly increasing sequence of ideals $(\overline{x_1}) \subsetneq (\overline{x_1}, \overline{x_2}) \subsetneq \cdots$. Now, let $\overline{\mathfrak{p}}$ be a prime ideal in R. Then, the preimage of $\overline{\mathfrak{p}}$ under the natural projection, say $\mathfrak{p}$ is a prime ideal containing $(x_1, x_2^2, \dots)$ and thus contains its radical, $(x_1, x_2, \dots)$. Since the latter is a maximal ideal, so is $\mathfrak{p}$ and hence so is $\overline{\mathfrak{p}}$. This establishes that $\dim A = 0$. Finally, to see that this ring is local, use a similar argument as before to conclude that the preimage of any maximal ideal is the ideal $(x_1, x_2, \dots)$.

Lemma 6.15. *If A is Noetherian and $\phi : A \to B$ is a surjective ring homomorphism, then B is also Noetherian.*

Proof. Since $B \cong A/\ker\phi$, the conclusion follows. ■

Proposition 6.16. *If A is a noethering and $S \subseteq A$ is a multiplicative subset, then $S^{-1}A$ is a noethering.*

Proof. Recall that every ideal in $S^{-1}A$ is finitely generated. Let $I \subseteq S^{-1}A$ be an ideal then there is $\mathfrak{a} \subseteq A$ an ideal such that $S^{-1}\mathfrak{a} = I$. Since A is noetherian, $\mathfrak{a}$ is generated by a finite set $\{x_1, \dots, x_n\}$, whereby I is generated by the set $\{x_1/1, \dots, x_n/1\}$. This completes the proof. ■

But recall, as we have seen earlier, that being a noethering is not a local property, a counterexample to which is an infinite product of fields.

Lemma 6.17. *if A is a noethering and $\mathfrak{a} \subseteq A$ is an ideal, then there is a positive integer n such that $(\sqrt{\mathfrak{a}})^n \subseteq \mathfrak{a}$.*

Proof. Let $\sqrt{\mathfrak{a}} = \{x_1, \dots, x_n\}$. Then, for each index $1 \le i \le n$, there is a positive integer m_i such that $x_i^{m_i} \in \mathfrak{a}$. Let $N = \sum_{i=1}^n n_i$. Then,

$$(\sqrt{\mathfrak{a}})^N = \left(\sum_{i=1}^n (x_i)\right)^N$$

since multiplication of ideal distributes over multiplication, every element in the above expansion would be of the form $(x_1)^{r_1} \cdots (x_n)^{r_n}$ with $\sum_{i=1}^n r_i = N$. But since $(x_i)^{m_i} \in \mathfrak{a}$, we have the desired conclusion. ■

Theorem 6.18 (Hilbert Basis Theorem). *If A is Noetherian, then so is $A[x]$.*

Note that the converse is also true since $A \cong A[x]/(x)$. The following proof is due to Sarges.

Proof. We shall show that every ideal in $A[x]$ is finitely generated. Suppose not and let $I \subseteq A[x]$ be an ideal that is not finitely generated. Choose $f_1 \in I$ with minimum degree. Now, inductively, choose $f_{k+1} \in I \backslash (f_1, \dots, f_k)$ with the minimum degree. Obviously, this process goes on indefinitely, since we have assumed I to not be finitely generated. We now have

$$\begin{aligned} f_1 &= a_1 x^{d_1} + \text{lower degree terms} \\ f_2 &= a_2 x^{d_2} + \text{lower degree terms} \\ &\vdots \\ f_n &= a_n x^{d_n} + \text{lower degree terms} \\ &\vdots \end{aligned}$$

[1] Nagata is to blame for this monster

with $d_1 \le d_2 \le \cdots$. We also have the following ascending chain of ideals in A,

$$(a_1) \subseteq (a_1, a_2) \subseteq \cdots$$

Therefore, there is $n \in \mathbb{N}$ such that $(a_1, \dots, a_n) = (a_1, \dots, a_n, a_{n+1})$. Consequently, we may write a_{n+1} as a linear combination of $a_1, \dots, a_n$, say

$$a_{n+1} = b_1 a_1 + \cdots + b_n a_n$$

for some $b_1, \dots, b_n \in A$. Let

$$g = f_{n+1} - (b_1 x^{d_{n+1} - d_1} f_1 + \cdots + b_n x^{d_{n+1} - d_n} f_n)$$

It is not hard to argue that $g \in I \backslash (f_1, \dots, f_n)$, but $\deg g \le \deg f_{n+1}$, a contradiction. This completes the proof. ■

An analogous theorem, with an analogous proof is true wherein $A[x]$ is replaced by $A[\![x]\!]$.

Corollary 6.19. For a field k, the polynomial ring $k[x_1, \dots, x_n]$ in finitely many indeterminates is noetherian.

Corollary 6.20. If A is a noethering, then every A-algebra of finite type is a noethering.

If $A \subseteq B$ is a ring extension with both A and B noetherian, it is not necessary that B is an A-algebra of finite type. Indeed, consider $\overline{\mathbb{Q}}/\mathbb{Q}$ an extension of fields.

On the other hand, even if B is an A-algebra of finite type and noetherian, it is not necessary for A to be noetherian. Indeed, consider the ring inclusion

$$k[xy, xy^2, \dots] \subsetneq k[x, y]$$

The former is not noetherian owing to the chain of ideals

$$(xy) \subsetneq (xy, xy^2) \subsetneq \cdots$$

while the latter obviously is noetherian.

Proposition 6.21. *Let A be a noethering. Every finitely generated A-module is noetherian.*

Proof. Let M be generated by $\{x_1, \dots, x_n\} \subseteq M$. Since A is a noetherian A-module, so is $A^{\oplus n}$. There is a surjection $\varphi : A^{\oplus n} \twoheadrightarrow M$ which maps the i-th basis element to x_i. Thus, M is noetherian. ■

Proposition 6.22. *Let M be a noetherian A-module. Then, $A/\operatorname{Ann}_A(M)$ is a noethering.*

Proof. Since M is noetherian, it is finitely generated. Let $\{m_1, \dots, m_n\}$ be a set of generators. Then, $\operatorname{Ann}_A(M) = \bigcap_{i=1}^{n} \operatorname{Ann}_M(m_i)$. Consider the map $\phi : A \to M^n$ given by $\phi(a) = (am_1, \dots, am_n)$. Note that $\ker \phi = \operatorname{Ann}_A(M)$. Thus, we have a short exact sequence

$$0 \longrightarrow A/\operatorname{Ann}_A(M) \longrightarrow A \longrightarrow \phi(A) \longrightarrow 0.$$

Consequently, $A/\operatorname{Ann}_A(M)$ is a noetherian A-module and thus a noetherian $A/\operatorname{Ann}_A(M)$-module, whence a noethering. ■

An analogous result does **not** hold for Artinian modules (rings). Consider the module $M = \mu[p^\infty]$ for some prime p as an abelian group. This is an artinian module but not noetherian as we have seen earlier. It is not hard to see that $\operatorname{Ann}_{\mathbb{Z}}(M) = (0)$ whence $\mathbb{Z}/\operatorname{Ann}_{\mathbb{Z}}(M) = \mathbb{Z}$ which is not artinian, as we have seen earlier.

Lemma 6.23 (Artin-Tate Lemma). *Let $A \subseteq B \subseteq C$ be rings with A noetherian, and C an A-algebra of finite type. If either*

(a) C is a finite B-algebra[a]*, or*

(b) C is integral over B,

then B is an A-algebra of finite type.

[a] Recall that this is the same as being finitely generated as a B-module

Proof. Note that $(a) \iff (b)$ due to Theorem 5.2. We shall show that (a) implies the desired conclusion. Since C is an A-algebra of finite type, say it is generated by $\{x_1, \ldots, x_n\}$ as an A-algebra. Similarly, since it is a finite B-algebra, it is finitely generated as a B-module, say by $\{y_1, \ldots, y_m\}$. Therefore, there are coefficients b_{ij} and b_{ijk} in B such that

$$x_i = \sum_{j=1}^{m} b_{ij} y_j$$
$$y_i y_j = \sum_{k=1}^{m} b_{ijk} y_k.$$

Let $B_0 = A[\{b_{ij}\} \cup \{b_{ijk}\}] \subseteq B$. Since A is noetherian, and B_0 is an A-algebra of finite type, it is a noethering.

Now, since C is a finite type A-algebra, every element of C is a polynomial in the x_i's with coefficients in A. Using the first set of relations, it is a polynomial in the y_i's with coefficients in B_0. Using the second set of relations, it is a linear combination of the y_i's with coefficients in B_0, whereby C is a finite B_0-algebra.

Since C is a finitely generated B_0-module it is noetherian and thus B, being a B_0-submodule, is a finitely generated B_0-module and consequently, a B_0-algebra of finite type. Thus, B is an A-algebra of finite type. ∎

Corollary 6.24 (Noether). Let A be a noethering and R an A-algebra (commutative) of finite type and G a finite group of A-algebra automorphisms of R. Let

$$R^G := \{r \in R \mid g \cdot r = r, \forall g \in G\}.$$

Then, R^G is a finitely generated A-algebra, in particular, is a noethering.

Proof. That R^G is indeed an A-algebra is easy to see. Further, it is well known that R/R^G is an integral extension. But since R is integral over R^G and is also a finitely generated R^G-algebra, due to Proposition 5.5, R is a finitely generated R^G-module. Finally from Lemma 6.23, R^G is an A-algebra of finite type. ∎

Lemma 6.25 (Cohen). *A is a noethering if and only if every prime ideal in A is finitely generated.*

Proof. We shall prove the converse. Let Σ be the poset of proper ideals that are not finitely generated, which we suppose is nonempty. If $\mathscr{C}$ is a chain in Σ, then $I = \bigcup_{\mathfrak{a} \in \mathscr{C}} \mathfrak{a}$ may not be finitely generated for if it were, then there is a set of generators $\{r_1, \ldots, r_n\}$ and thus there would exist $\mathfrak{a} \in \mathscr{C}$ containing $\{r_1, \ldots, r_n\}$ whereby equal to I, contradiction. Hence, I is an upper bound for $\mathscr{C}$ and due to Zorn's Lemma, there is a maximal element $\mathfrak{p} \in \Sigma$.

Since $\mathfrak{p}$ may not be prime, there are $x, y \notin \mathfrak{p}$ such that $xy \in \mathfrak{p}$. Consider $\mathfrak{p} + (x)$. This strictly contains $\mathfrak{p}$ and therefore, is finitely generated. The generators of $\mathfrak{p} + (x)$ are of the form $p_i + a_i x$ for $1 \le i \le n$ for some positive integer n.

Consider the ideal $(\mathfrak{p} : x)$. This contains $\mathfrak{p} + (y)$ which strictly contains $\mathfrak{p}$ an thus, is finitely generated. Say $(\mathfrak{p} : x) = (x_1, \ldots, x_m)$ for some positive integer m. Let $\mathfrak{a} = (p_1, \ldots, p_n, xx_1, \ldots, xx_m)$. We contend that $\mathfrak{a} = \mathfrak{p}$.

Obviously, $\mathfrak{a} \subseteq \mathfrak{p}$. On the other hand, for any $p \in \mathfrak{p}$, there is a representation

$$p + x = b_1 p_1 + \cdots + b_n p_n + cx$$

for some $b_1, \ldots, b_n, c \in A$, consequently, $p \in \mathfrak{a}$. Thus, $\mathfrak{a} = \mathfrak{p}$, which is a contradiction to the choice of $\mathfrak{p}$. Hence, Σ is empty and A is a noethering. ■

Proposition 6.26. *A nonzero ideal in a noethering contains a product of prime ideals.*

Proof. Suppose not. Let Σ be the set of all ideals which do not contain a product of prime ideals. According to our assumption, Σ is non-empty and thus contains a maximal element[2], say $\mathfrak{a}$. Since $\mathfrak{a} \in \Sigma$, it cannot be prime, thus, there are $x, y \notin \mathfrak{a}$ with $xy \in \mathfrak{a}$. Since $\mathfrak{a} + (x)$ and $\mathfrak{a} + (y)$ strictly contain $\mathfrak{a}$, they are not in Σ whence there are prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ such that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq \mathfrak{a} + (x) \qquad \mathfrak{q}_1 \cdots \mathfrak{q}_m \subseteq \mathfrak{a} + (y)$$

and thus

$$\mathfrak{p}_1 \cdots \mathfrak{p}_n \mathfrak{q}_1 \cdots \mathfrak{q}_m \subseteq (\mathfrak{a} + (x))(\mathfrak{a} + (y)) = \mathfrak{a}^2 + \mathfrak{a}((x) + (y)) + (xy) \subseteq \mathfrak{a}$$

a contradiction. ■

Lemma 6.27. *Let A be a noethering and $\mathfrak{a} \subseteq A$ an ideal. Suppose $b \in \bigcap_{n=1}^{\infty} \mathfrak{a}^n$. Then $\mathfrak{a} = b\mathfrak{a}$.*

Proof. Let $\mathfrak{a}$ be generated by $a_1, \ldots, a_k$. Let n be a positive integer. Since $b \in \mathfrak{a}^n$, there is a homogeneous polynomial $P_n(x_1, \ldots, x_k) \in A[x_1, \ldots, x_k]$ of degree n such that $P_n(a_1, \ldots, a_k) = b$. Consider now the chain of ideals

$$(P_1) \subseteq (P_1, P_2) \subseteq \cdots$$

Then there is a positive integer N such that $(P_1, \ldots, P_N) = (P_1, \ldots, P_{N+1})$. Consequently, there are polynomials $Q_1, \ldots, Q_N$ in $A[x_1, \ldots, x_k]$ such that

$$P_{N+1} = Q_1 P_1 + \cdots + Q_N P_N$$

Since P_{N+1} is a homogeneous polynomial of degree $N+1$, we may choose each Q_i to be homogeneous of degree $N + 1 - i > 0$ (one can do this by just dropping all the terms which are not of degree $N + 1 - i$). Consequently, for each $1 \leq i \leq N$, $Q_i(a_1, \ldots, a_k) \in \mathfrak{a}$ whence

$$b = P_{N+1}(a_1, \ldots, a_k) = b \sum_{i=1}^{n} Q_i(a_1, \ldots, a_k) \in b\mathfrak{a}$$

This completes the proof. ■

Corollary 6.28. Let A be a noethering and $\mathfrak{a} \subseteq A$ an ideal. Then $\bigcap_{n=1}^{\infty} \mathfrak{a}^n = 0$ if

(a) $\mathfrak{a} \subseteq \mathfrak{R}(A)$, the Jacobson radical.[a]

(b) A is a domain and $\mathfrak{a}$ is a proper ideal.

[a] When A is a local noethering and $\mathfrak{a} = \mathfrak{m}$, this result is known as Krull's Intersection Theorem.

[2] This does not require Zorn, since we are in a noethering

Proof. (a) Let $b \in \bigcap_{n=1}^{\infty} \mathfrak{a}^n$. Then, $b\mathfrak{a} = (b)$ whence there is some $x \in \mathfrak{a}$ such that $bx = b$ or equivalently, $b(1-x) = 0$. Since $x \in \mathfrak{R}(A)$, $1-x$ is invertible and $b = 0$.

(b) Using a similar argument as above, if $bx = b$ then either $b = 0$ or $x = 1$. Since $\mathfrak{a}$ is a proper ideal, we must have $b = 0$.

∎

6.3.1 Primary Decomposition

Definition 6.29 (Irreducible). An ideal $\mathfrak{a} \subseteq A$ is said to be *irreducible* if for all ideals $\mathfrak{b}, \mathfrak{c} \subseteq A$,

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c} \implies \mathfrak{a} = \mathfrak{b} \text{ or } \mathfrak{a} = \mathfrak{c}$$

Lemma 6.30. *In a noethering, every ideal can be expressed as a finite intersection of irreducible ideals.*

Proof. Let Σ be the poset of ideals that cannot be expressed as a finite intersection of irreducible ideals in A. Suppose Σ is nonempty, then every chain in Σ is finite (owing to noetherian-ness) whence has an upper bound, thus Σ has a maximal element (Zorn's Lemma), say $\mathfrak{a}$. Note that $\mathfrak{a}$ cannot be irreducible, therefore, there are ideals $\mathfrak{b}, \mathfrak{c}$ properly containing $\mathfrak{a}$ such that $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$. Due to the maximality of $\mathfrak{a}$, both $\mathfrak{b}$ and $\mathfrak{c}$ can be expressed as a finite intersection of irreducible ideals in A, as a result, so can $\mathfrak{a}$, a contradiction. Thus Σ must be empty and the proof is complete. ∎

Lemma 6.31. *Every irreducible ideal in a noethering is primary.*

Proof. Let $\mathfrak{q} \subseteq A$ be an irreducible ideal. We shall show that (0) is primary in $A/\mathfrak{q}$, which is equivalent to $\mathfrak{q}$ being primary. Let $x, y \in A/\mathfrak{q}$ such that $xy = 0$. If $x \neq 0$, then consider the chain

$$\text{Ann}(y) \subseteq \text{Ann}(y^2) \subseteq \cdots$$

Since $A/\mathfrak{q}$ is a noethering, there is a positive integer n such that $\text{Ann}(y^n) = \text{Ann}(y^{n+1})$. We contend that $(x) \cap (y^n) = 0$. Indeed, if $z \in (x) \cap (y^n)$, then there are $u, v \in A/\mathfrak{q}$ such that $z = ux = vy^n$. Then,

$$vy^{n+1} = zy = uxy = 0$$

whence $v \in \text{Ann}(y^{n+1}) = \text{Ann}(y^n)$, whereby $z = 0$. But since (0) is irreducible and $x \neq 0$, we must have $y^n = 0$ and (0) is primary. This completes the proof. ∎

Corollary 6.32. A noethering has finitely many minimal prime ideals.

Proof. Since A is noetherian, the ideal (0) has a primary decomposition and the minimal primes belonging to (0) are precisely the minimal primes in A and thus are finite. ∎

Alternate Proof to Proposition 6.26. Let $\mathfrak{a} \subseteq A$ be a nonzero ideal. Then, it has a primary decomposition, whereby $\sqrt{\mathfrak{a}}$ can be written as an intersection of prime ideals, say $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$. We have $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$ since the product of ideals is contained in their intersection. Finally, since every ideal in a noethering contains a power of its radical, there is a positive integer m such that

$$(\mathfrak{p}_1 \cdots \mathfrak{p}_n)^m \subseteq \sqrt{\mathfrak{a}}^m \subseteq \mathfrak{a}$$

This completes the proof. ∎

Lemma 6.33. *Let A be a noetherian domain with $\dim A = 1$. Then every nonzero ideal in A can be uniquely expressed as a product of primary ideals whose radicals are distinct.*

Proof. Let $\mathfrak{a} \subsetneq A$ be a nonzero ideal. This has a primary decomposition with the associated primes being maximal and thus comaximal. Thus, the primary ideals in the decomposition are also comaximal. From Theorem 1.3, we have that $\mathfrak{a}$ is in fact the product of the aforementioned primary ideals.

On the other hand, suppose $\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_n$ where $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ are distinct. Since $\dim A = 1$, the ideals $\mathfrak{p}_i$ are maximal whence $\mathfrak{q}_i$ are comaximal. Invoking Theorem 1.3, we see that $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ is a primary decomposition. Further, since $\mathfrak{p}_i$ are also the minimal primes associated with $\mathfrak{a}$, due to Theorem 4.12, the $\mathfrak{q}_i$'s are unique. ∎

Theorem 6.34 (Krull's Intersection Theorem). *Let A be a noetherian ring and $\mathfrak{a} \trianglelefteq A$ an ideal. Set*

$$\mathfrak{b} = \bigcap_{n=1}^{\infty} \mathfrak{a}^n.$$

Then, $\mathfrak{a}\mathfrak{b} = \mathfrak{b}$.

Proof. Since $\mathfrak{a}$ is a proper ideal, so is $\mathfrak{b}$ and $\mathfrak{a}\mathfrak{b}$. Hence, it admits a primary decomposition

$$\mathfrak{a}\mathfrak{b} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n.$$

We contend that $\mathfrak{b} \subseteq \mathfrak{q}_i$ for every $1 \le i \le n$. Suppose not, then there is some index i and $b_i \in \mathfrak{b} \backslash \mathfrak{q}_i$. Note that $b_i\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{q}_i$ and hence, $\mathfrak{a} \subseteq \mathfrak{p}_i$. Now, there is a positive integer $r > 0$ such that $\mathfrak{p}_i^r \subseteq \mathfrak{q}_i$ whence, $\mathfrak{a}^r \subseteq \mathfrak{q}_i$, consequently, $\mathfrak{b} \subseteq \mathfrak{q}_i$, a contradiction. This completes the proof. ∎

There's an analogue of the above theorem for modules as well.

Theorem 6.35 (Krull's Intersection Theorem). *Let A be a noethering, M a finitely generated A-module and $\mathfrak{a} \trianglelefteq A$ an ideal. Set*

$$N = \bigcap_{n=1}^{\infty} \mathfrak{a}^n M.$$

Then, $\mathfrak{a}N = N$.

Proof. If $\mathfrak{a} = (1)$ or $N = M$, there is nothing to prove. Now suppose $N \subsetneq M$, then, it admits a primary decomposition

$$N = Q_1 \cap \cdots \cap Q_n$$

where each Q_i is $\mathfrak{p}_i$-primary and hence, $\mathfrak{p}_i = \sqrt{\operatorname{Ann}_A(M/Q_i)}$. We contend that N is contained in every Q_i. Suppose not, then there is an index i and $x \in N \backslash Q_i$. Notet hat $\mathfrak{a}x$ is a submodule of $\mathfrak{a}N$ which is contained in Q_i. But since x is not contained in Q_i, we must have $\mathfrak{a} \subseteq \mathfrak{p}_i$. As a result, there is a positive integer $r > 0$ such that $\mathfrak{a}^r \subseteq \operatorname{Ann}_A(M/Q_i)$. Hence, $N \subseteq \mathfrak{Q}_i$, a contradiction. This completes the proof. ∎

Corollary 6.36. With the notation of the above result,

$$N = \{x \in M \mid \exists a \in \mathfrak{a},\ (1+a)x = 0\}.$$

6.3.2 Nagata's Monster

Lemma 6.37. *Let A be a ring such that*

(a) for each maximal ideal $\mathfrak{m}$, $A_{\mathfrak{m}}$ is noetherian.

(b) every $x \in A \backslash \{0\}$ has finitely many maximal ideals containing it.

Then, A is noetherian.

Proof. Let $(0) \neq \mathfrak{a} \trianglelefteq A$ be a proper ideal. We shall show that $\mathfrak{a}$ is a finitely generated ideal. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ be the maximal ideals containing $\mathfrak{a}$, which are finite in number since $\mathfrak{a}$ is nonzero. Pick some nonzero $x_0 \in \mathfrak{a}$ and let $\mathfrak{m}_1, \ldots, \mathfrak{m}_r, \ldots, \mathfrak{m}_{r+s}$ be the maximal ideals containing x_0.

For each $1 \leq j \leq s$, there is $x_j \in \mathfrak{a} \backslash \mathfrak{m}_{r+j}$. Now, for each $1 \leq i \leq r$, $\mathfrak{a}A_{\mathfrak{m}_i}$ is a finitely generated ideal and is generated by the images of some $x_1^{(i)}, \ldots, x_{n_i}^{(i)}$.

Let $\mathfrak{a}_0 \subseteq \mathfrak{a}$ denote the ideal in A generated by

$$\{x_0\} \cup \{x_1, \ldots, x_s\} \cup \bigcup_{i=1}^{r} \{x_1^{(i)}, \ldots, x_{n_i}^{(i)}\}.$$

Let $\mathfrak{m}$ be a maximal ideal in A. If $x_0 \in \mathfrak{m}$, then the extensions of both $\mathfrak{a}_0$ and $\mathfrak{a}$ are equal to $A_{\mathfrak{m}}$. Now suppose $x_0 \in \mathfrak{m}$. Thus, $\mathfrak{m} \in \{\mathfrak{m}_1, \ldots, \mathfrak{m}_{r+s}\}$. If $\mathfrak{m} = \mathfrak{m}_{r+j}$ for some j, then $x_j \notin \mathfrak{m}$ but $x_j \in \mathfrak{a}_0$ whence the extensions of both $\mathfrak{a}_0$ and $\mathfrak{a}$ are $A_{\mathfrak{m}}$. Finally, if $\mathfrak{m} = \mathfrak{m}_i$ for some $1 \leq i \leq r$, then both $\mathfrak{a}_0$ and $\mathfrak{a}$ extend to $\mathfrak{a}A_{\mathfrak{m}}$, since the former contains $x_1^{(i)}, \ldots, x_{n_i}^{(i)}$. Thus, the inclusion $\mathfrak{a}_0 \hookrightarrow \mathfrak{a}$ is a surjection, due to Proposition 3.13. This completes the proof. ∎

Theorem 6.38. *Let k be a field and $A = k[x_1, x_2, \ldots]$, the polynomial ring over k in countably many indeterminates. Let $\{m_i\}_{i=1}^{\infty}$ denote an increasing sequence such that $m_{i+1} - m_i > m_i - m_{i-1}$ for all $i > 1$. Finally, let $\mathfrak{p}_i = (x_{m_i+1}, \ldots, x_{m_{i+1}})$ and S denote $A \backslash \bigcup_{i=1}^{\infty} \mathfrak{p}_i$. Then, $R = S^{-1}A$ is a noethering with infinite Krull dimension.*

The proof of the above theorem relies on the following claims.
Claim 1 (Prime Avoidance). If $\mathfrak{a} \trianglelefteq A$ is contained in $\bigcup_{i=1}^{\infty} \mathfrak{p}_i$, then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some i.

Proof. For each $f \in A$, let

$$S(f) := \{i \in \mathbb{N} \mid f \in \mathfrak{p}_i\},$$

which is finite. Pick some $f \in \mathfrak{a}$. If there is no $g \in \mathfrak{a}$ with $S(f) \cap S(g) = \varnothing$, then, $\mathfrak{a}$ is contained in $\bigcup_{i \in S(f)} \mathfrak{p}_i$, and we are done due to Proposition 1.9.

On the other hand, suppose there is some $g \in \mathfrak{a}$ such that $S(f) \cap S(g) = \varnothing$. Obviously, neither $S(f)$ or $S(g)$ can be empty. Choose some $r \in S(g)$ and let $d = \deg f$. We shall show that $S(f + x_{m_r+1}^{d+1} g) = \varnothing$.

First, note that $S(g) = S(x_{m_r+1}^{d+1} g)$. Further, a polynomial in A is contained in $\mathfrak{p}_i$ if and only if each monomial in the aforementioned polynomial is contained in $\mathfrak{p}_i$. Next, suppose $h = f + x_{m_r+1}^{d+1} g \in \mathfrak{p}_l$. Then, we must have all the monomials in h to lie in $\mathfrak{p}_l$, consequently, both f and $x_{m_r+1}^{d+1} g$ must lie in $\mathfrak{p}_l$. That is, $l \in S(f) \cap S(x_{m_r+1}^{d+1} g) = \varnothing$, a contradiction.

Hence, it can never be the case that $S(f) \cap S(g) = \varnothing$. This completes the proof. ∎

Claim 2. The primes in R are precisely the $S^{-1}\mathfrak{p}_i$'s.

Proof. Let $f/s \in R \backslash S^{-1}\mathfrak{p}_i$. We shall show that its image in $R/S^{-1}\mathfrak{p}_i$ is a unit. First, note that it suffices to show that the image of f in $R/S^{-1}\mathfrak{p}_i$ is a unit. Since $f \notin S^{-1}\mathfrak{p}_i$, it has at least one monomial not in $\mathfrak{p}_i$. We may suppose that all the monomials in f are not in $\mathfrak{p}_i$. Consider $f + x_{m_i+1}$, whose image in $R/S^{-1}\mathfrak{p}_i$ is the same that of f. But $f + x_{m_i+1} \in S$ and thus is a unit. This proves the claim. ∎

Proof of Theorem 6.38. Note that $R_{S^{-1}\mathfrak{p}_i} \cong A_{\mathfrak{p}_i}$, which is noetherian, further, every element in $S^{-1}A$ is contained in finitely many of the $S^{-1}\mathfrak{p}_i$'s whence, due to Lemma 6.37, R is noetherian. Finally, note that the height of $S^{-1}\mathfrak{p}_i$ is at least $m_{i+1} - m_i$, consequently, $\dim R = \infty$. This completes the proof. ■

6.3.3 Eakin-Nagata Theorem

Lemma 6.39 (Formanek). *Let M be a finitely generated faithful A-module such that the poset*

$$\{\mathfrak{a}M \mid \mathfrak{a} \text{ is an ideal in } A\}$$

has the ascending chain condition. Then, A is a noethering.

Proof. Suppose not. Consider the poset

$$\Sigma = \{\mathfrak{a} \trianglelefteq A \mid M/\mathfrak{a}M \text{ is not a noetherian } A\text{-module}\}.$$

This is non-empty and hence, contains a maximal element, say $\mathfrak{a}_0$. Let $M' = M/\mathfrak{a}_0 M$ and $A' = A/\operatorname{Ann}_A(M')$. Then, M' is a non-noetherian faithful A'-module. Further, if $\mathfrak{b} \trianglelefteq A'$ is a non-zero ideal, then $M'/\mathfrak{b}M'$ is isomorphic to $M/\mathfrak{a}'M$ where $\mathfrak{a}'$ strictly contains $\mathfrak{a}_0$ and hence, is a noetherian A-module, consequently, a noetherian A'-module.

Consider the poset

$$\Gamma = \{N \leq M' \mid M'/N \text{ is a faithful } A'\text{-module}\}.$$

Note that $N \in \Gamma$ if and only if for all $a \in A' \backslash \{0\}$, $aM' \not\subseteq N$. It is now easy to see that every chain in Γ admits an upper bound in Γ and hence, Γ contains a maximal element, say $N_0 \leq M'$. Let $M'' = M'/N_0$.

First, note that M'' cannot be noetherian since this would force A' to be a noethering, which, in turn would force A to be a noethering. Hence, there is a (non-zero) submodule N of M'' that is not finitely generated as an A'-module. The module M''/N is isomorphic to M'/N' where N' is a submodule of M' that strictly contains N_0 and hence, M'/N' is not a faithful A'-module. That is, there is an $a \in A' \backslash \{0\}$ such that $aM'' \subseteq N$. Note that M''/aM'' is isomorphic to M'/aM', which must be a noetherian A'-module due to our construction of M'.

Hence, N/aM'', being a submodule of M''/aM'' is a noetherian A'-module, in particular, it is finitely generated. Finally, since aM'' is a finitely generated A'-module, we must have that N is a finitely generated A'-module, a contradiction. ■

Theorem 6.40 (Eakin-Nagata). *Let $A \subseteq B$ be an extension of rings such that B is a noethering and a finitely generated A-module. Then, A is a noethering.*

Proof. Follows from Lemma 6.39 by taking $M = B$. ■

6.4 Artinian Rings

Recall that A is artinian if it is an artinian module over itself.

Proposition 6.41. *Let A be an artinian ring. Then A has finitely many maximal ideals.*

Proof. Suppose not. Then, we have a sequence $\{\mathfrak{m}_i\}_{i=1}^{\infty}$ of pairwise distinct maximal ideals. Consider the sequence of ideals $\{\mathfrak{m}_1 \cdots \mathfrak{m}_n\}_{n=1}^{\infty}$. We contend that the inclusion $\mathfrak{m}_1 \cdots \mathfrak{m}_{n-1} \supseteq \mathfrak{m}_1 \cdots \mathfrak{m}_n$ is strict. Indeed, for all $1 \leq i \leq n-1$, pick $x_i \in \mathfrak{m}_i \backslash \mathfrak{m}_n$. Then, $x_1 \cdots x_{n-1} \notin \mathfrak{m}_n$, since $A \backslash \mathfrak{m}_n$ is a multiplicatively closed subset. Thus, $x_1 \cdots x_{n-1} \in \mathfrak{m}_1 \cdots \mathfrak{m}_{n-1} \backslash \mathfrak{m}_1 \cdots \mathfrak{m}_n$. This is a contradiction to A being artinian. ■

Proposition 6.42. *Let A be an artinian ring. Then every prime ideal in A is maximal.*

Proof. Let $\mathfrak{p}$ be a prime ideal in A. Then $A' = A/\mathfrak{p}$ is an Artinian integral domain. We shall show that this is a field, for which it suffices to show that every element is invertible. Choose $x' \in A'$ and let $\phi : A' \to A'$ be the A'-module homomorphism that maps $a \mapsto x'a$. Since A' is an integral domain, this map is injective and since A' is artinian, it is also an isomorphism. Consequently, there is some $y' \in A'$ such that $x'y' = 1$ and the conclusion follows. ■

Corollary 6.43. Let A be an artinian ring. Then $\mathfrak{N}(A) = \mathfrak{R}(A)$.

Lemma 6.44. *Let A be an artinian ring. Then $\mathfrak{N}(A)$ is nilpotent.*

Proof. We shall denote $\mathfrak{N}(A)$ by $\mathfrak{N}$ for the sake of brevity. Consider the decreasing chain

$$\mathfrak{N} \supseteq \mathfrak{N}^2 \supseteq \cdots$$

Then there is an index n such that $\mathfrak{a} = \mathfrak{N}^n = \mathfrak{N}^{n+1} = \cdots$. Suppose for the sake of contradiction that $\mathfrak{a} \neq 0$. Let Σ be the set of ideals $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} \neq 0$. Obviously Σ is empty since it contains $\mathfrak{a}$. Since A is artinian, Σ has a minimal element $\mathfrak{c}$[3].

We contend that $\mathfrak{c}$ is principal. Indeed, there is an element $x \in \mathfrak{c}$ such that $x\mathfrak{a} \neq 0$. Thus, $(x)\mathfrak{a} \neq 0$. Owing to the minimality of $\mathfrak{c}$, we must have $\mathfrak{c} = (x)$.

Consider now the ideal $(x)\mathfrak{a}$. This is a subset of (x) and

$$((x)\mathfrak{a})\mathfrak{a}^k = (x)\mathfrak{a}^{k+1} = (x)\mathfrak{a} \neq 0$$

whence $(x)\mathfrak{a} \in \Sigma$ and again, owing to the minimality of $(x) = \mathfrak{c}$, we have $(x)\mathfrak{a} = (x)$. Hence, there is some $y \in \mathfrak{a}$ such that $xy = x$. We now have

$$x = xy = xy^2 = \cdots$$

Since $y \in \mathfrak{a} \subseteq \mathfrak{N}$, it is nilpotent, whence $x = 0$, a contradiction. Thus $\mathfrak{a} = 0$ and this completes the proof. ■

Theorem 6.45. *A is artinian if and only if it is a noethering with krull dimension zero.*

Proof. ($\Longrightarrow$). Obviously $\dim A = 0$. We know that A has finitely many maximal ideals $\mathfrak{m}_1, \cdots \mathfrak{m}_n$ the intersection of which is the Jacobson radical, which, in this case, is equal to the nilradical. Further, since the maximal ideals are comaximal, we have

$$\mathfrak{N}(A) = \mathfrak{m}_1 \cdots \mathfrak{m}_n$$

But since $\mathfrak{N}(A)$ is nilpotent, there is a positive integer k such that $\mathfrak{m}_1^k \cdots \mathfrak{m}_n^k = 0$, thus due to Lemma 6.13, A is noetherian.

($\Longleftarrow$). Since A is a noethering, the (0) ideal has a primary decomposition, whence $(0) = \bigcap_{i=1}^n \mathfrak{q}_i$ whereby $\mathfrak{N}(A) = \bigcap_{i=1}^n \mathfrak{p}_i$ where each prime $\mathfrak{p}_i$ is maximal owing to the krull dimension. Thus, $\mathfrak{N}(A) = \mathfrak{p}_1 \cdots \mathfrak{p}_n$. Since in a noetherian ring, the nilradical is nilpotent, there is a positive integer k such that

$$(0) = \mathfrak{N}(A)^k = \mathfrak{p}_1^k \cdots \mathfrak{p}_n^k.$$

We are now done due to Lemma 6.13. ■

[3]We have not invoked Zorn to conclude this.

Theorem 6.46 (Structure Theorem of Artinian Rings). *Let A be an artinian ring. Then, there are artinian local rings $A_1, \ldots, A_n$ such that $A \cong A_1 \oplus \cdots \oplus A_n$. Further, the A_i's are unique up to isomorphism.*

Proof. ■

Lemma 6.47.

Chapter 7

DVRs and Dedekind Domains

7.1 General Valuations and Valuation Rings

Definition 7.1 (Valuation). A *valuation* on a field K is a map $v : K \to \Gamma \cup \{\infty\}$ where Γ is an ordered abelian group such that for all $x, y \in K$,

1. $v(xy) = v(x) + v(y)$, that is, the restriction $v : K^\times \to \Gamma$ is a group homomorphism,
2. $v(x + y) \geq \min\{v(x), v(y)\}$.

The set

$$A = \{x \in K^\times \mid v(x) \geq 0\}$$

is called the *valuation ring* of K with respect to the valuation v. Simply stating "A is a valuation ring" means A is a valuation ring of $K = Q(A)$.

That the set A forms a ring follows from the fact that it is closed under addition, multiplication and subtraction.

Proposition 7.2. *Let A be an integral domain and $K = Q(A)$, its field of fractions. Then, A is a* valuation ring *of K iff for every $x \in K\backslash\{0\}$, we have $x \in A$ or $x^{-1} \in A$.*

Proof. The forward direction from the fact that $0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1})$. Conversely, let $\Gamma = K^\times / A^\times$ and $\pi : K^\times \twoheadrightarrow \Gamma$ the natural projection. Define an order on Γ as follows

- Every element in G is of the form $\pi(x)$ for $x \in K^\times$. According to the given hypothesis, $x \in A$ or $x^{-1} \in A$. In the former case, let $\pi(x) \geq 1_\Gamma$ and in the latter, $\pi(x) < 1_\Gamma$.
- To see that this is well defined, suppose $x, y \in K$ with $x/y \in A^\times$, then if $x \in A$ then $y = xu \in A$ where $u \in A^\times$, on the other hand, if $x^{-1} \in A$, then $y^{-1} = ux^{-1} \in A$ where $u \in A^\times$.
- This extends to a total order on Γ by $\pi(x) \geq \pi(y)$ if and only if $\pi(xy^{-1}) \geq 1_\Gamma$, that is, $xy^{-1} \in A$.

We now contend that π is a valuation with valuation ring A. Since π is a homomorphism, it suffices to check $\pi(x + y) \geq \min\{\pi(x), \pi(y)\}$. Indeed, suppose $\pi(x) \geq \pi(y)$, which is equivalent to stating $x/y \in A$. Then, $1 + x/y \in A$, consequently

$$\pi(x + y) = \pi(y(1 + x/y)) = \pi(y)\pi(1 + x/y) \geq \pi(y).$$

This completes the proof. ∎

Proposition 7.3. *Let A be a valuation ring. Then*

(a) A is a local ring.

(b) A is normal.

Proof. (a) We shall show that the nonunits in A form an ideal. Let $\mathfrak{m}$ be the set of nonunits in A and choose $x \in \mathfrak{m}\backslash\{0\}$, $b \in A$. Then, $bx \neq 0$ since x is not a zero divisor. We contend that bx is a nonunit. For if not, then $b(bx)^{-1}$ would be an inverse of x.

Next, let $x, y \in \mathfrak{m}\backslash\{0\}$. According to the given condition, either x/y or y/x are in A. Without loss of generality, suppose $x/y \in A$. Then $x + y = y(1 + x/y) \in \mathfrak{m}$ from the conclusion of the previous paragraph. Thus $\mathfrak{m}$ is an ideal and A is local.

(b) Indeed, let $\alpha \in K$ be integral over A. If $\alpha \in A$, there is nothing to prove. If not, then it satisifes an equation of the form

$$\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0$$

Upon multiplying by $\alpha^{-(n-1)}$, we can represent α as a sum of elements in A, consequently, is an element of A, a contradiction. ∎

Proposition 7.4. *Let A be a domain. Then A is a valuation ring if and only if the ideals in A are totally ordered.*

Proof. ($\Longrightarrow$) Suppose not. Then, there are two distinct ideals $\mathfrak{a}, \mathfrak{b}$ with $\mathfrak{a} \not\subseteq \mathfrak{b}$ and $\mathfrak{b} \not\subseteq \mathfrak{a}$ whence we can pick $a \in \mathfrak{a}\backslash\mathfrak{b}$ and $b \in \mathfrak{b}\backslash\mathfrak{a}$. Since either $a/b \in A$ or $b/a \in A$, we must have $a|b$ or $b|a$. Without loss of generality, suppose $b|a$. Then, $a \in (b) \subseteq \mathfrak{b}$, a contradiction.

($\Longleftarrow$) Let $x = a/b \in K$. Consider the ideals (a) and (b) in A. Since the ideals of A are totally ordered, either $(a) \subseteq (b)$ or $(b) \subseteq (a)$, and thus, either $x \in A$ or $x^{-1} \in A$. This completes the proof. ∎

Definition 7.5 (Bézout Ring). A ring is said to be a *Bézout ring* if every finitely generated ideal is principal.

Proposition 7.6. *A ring is a valuation ring if and only if it is a local Bézout domain.*

Proof. Let A be a valuation ring and $\mathfrak{a} = (a_1, \ldots, a_n) = (a_1) + \cdots + (a_n)$. Since ideals in a valuation ring are totally ordered, there is an index i such that $(a_j) \subseteq (a_i)$ for $1 \leq j \leq n$, consequently, $\mathfrak{a} = (a_i)$.

Conversely, let A be a local Bézout Domain and $x = a/b \in K = Q(A)$. If either a or b is a unit, then either x or $x^{-1} \in A$. Then, there is $c \in A$ such that $(c) = (a, b)$ whence there are $a', b' \in A$ such that $a = ca'$ and $b = cb'$. Let $u \in A$ be such that $(u) = (a', b')$. Then, $(cu') = (c)$ whence u is a unit. If neither a' or b' is a unit, then $(1) = (a', b') = (a') + (b') \subseteq \mathfrak{m}$, a contradiction. Thus, either $a|b$ or $b|a$ which completes the proof. ∎

7.2 Discrete Valuation Rings

Definition 7.7 (Discrete Valuation Ring). A valuation $v : K \to \Gamma \cup \{\infty\}$ is said to be a *discrete valuation* when $\Gamma = \mathbb{Z}$ and v is surjective. An integral domain A is said to be a *discrete valuation ring* if there is a discrete valuation v on the field of fractions of A such that A is the corresponding valuation ring.

First, since A is a valuation ring of its field of fractions, say K, it is local and normal, i.e. integrally closed in K. Further, the maximal ideal $\mathfrak{m}$ in A is the set of all $x \in A$ with positive valuations.

Proposition 7.8. *Let A be a DVR. Then, A is a local PID.*

Proof. Let $\mathfrak{m}_k = \{x \in A \mid v(x) \geq k\}$. We first show that $\mathfrak{m}_k$ is an ideal. Indeed, for all $x, y \in \mathfrak{m}_k$,

$$v(x-y) \geq \min\{v(x), v(-y)\} = \min\{v(x), v(y)\} \geq k$$

and $v(xy) = v(x) + v(y) \geq k$.

Next, we show that every non-zero ideal $\mathfrak{a}$ in A is one of the $\mathfrak{m}_i$'s. Due to the well ordering of the naturals, there is an $x \in \mathfrak{a}$ with $k = v(x) = \min_{a \in \mathfrak{a}} v(a)$. Then, by the choice of k, $\mathfrak{a} \subsetneq \mathfrak{m}_k$. Now, let $y \in \mathfrak{m}_k$. Since v is surjective, there is an element $z \in A$ with $v(z) = v(y) - v(x)$. Whence $xz \in \mathfrak{a}$ and $v(xz) = v(y)$. Since $(xz) = (y)$, we must have $y \in \mathfrak{a}$.

Notice that these ideals form a descending chain

$$\mathfrak{m} = \mathfrak{m}_1 \supsetneq \mathfrak{m}_2 \supsetneq \cdots.$$

Choose some $a \in A$ with $v(a) = 1$, which exists due to the surjectivity of v. Then, $\mathfrak{m} = (a)$ and consequently, $\mathfrak{m}_k = (a^k) = \mathfrak{m}^k$. From this, we may conclude that $\mathfrak{m}$ is the unique non-zero prime ideal in A and every other ideal is a power of $\mathfrak{m}$ and also principal. Thus A is a local PID. ∎

Theorem 7.9. *Let A be a noetherian local domain of Krull dimension 1, $\mathfrak{m}$ its maximal ideal and $k = A/\mathfrak{m}$ its residue field. Then the following are equivalent:*

(a) *A is a discrete valuation ring.*

(b) *A is normal.*

(c) *$\mathfrak{m}$ is principal.*

(d) $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$.

(e) *Every non-zero ideal is a power of $\mathfrak{m}$.*

(f) *There is $x \in A$ such that every nonzero ideal is of the form (x^k) for $k \geq 0$.*

Proof. $(a) \implies (b)$ is obvious.

$(b) \implies (c)$. Let $a \in \mathfrak{m}$. Since the ring is noetherian, (a) has a primary decomposition, but since the Krull dimension is 1, the only non-zero prime ideal is $\mathfrak{m}$, we see that $\sqrt{(a)} = \mathfrak{m}$. Since we are in a noethering, there is a positive integer n such that $\mathfrak{m}^n \subseteq (a)$ but $\mathfrak{m}^{n-1} \subsetneq (a)$. Let $b \in \mathfrak{m}^{n-1} \backslash (a)$ and $x = a/b$, $y = x^{-1} = b/a$ in $K = Q(A)$, the field of fractions.

First, since $b \notin (a)$, $y \notin A$ and therefore, is not integral over A. Since $\mathfrak{m}$ is a finitely generated A-module, it cannot be an $A[y]$-module lest y be integral over A due to Theorem 5.2. Hence, $y\mathfrak{m} \subsetneq \mathfrak{m}$.

Now consider $y\mathfrak{m}$. For any $z \in \mathfrak{m}$, $yz = bz/a \in A$ since $bz \in \mathfrak{m}^n \subseteq (a)$. Thus, $y\mathfrak{m} \subseteq A$. Since this is an ideal and is not contained in $\mathfrak{m}$, we must have $y\mathfrak{m} = A$, whence $\mathfrak{m} = Ax = (x)$ and is principal.

$(c) \implies (d)$. Let $\mathfrak{m} = (a)$ for some $a \in A$. Then, $\mathfrak{m}/\mathfrak{m}^2 = (\bar{a})$ where $\bar{a}$ is the image of a. Thus, $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \leq 1$. Now, note that $\mathfrak{m} \neq \mathfrak{m}^2$, lest due to Lemma 2.17, we have $\mathfrak{m} = 0$. Thus, $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \geq 1$ and the conclusion follows.

$(d) \implies (e)$. Let $\mathfrak{a}$ be a proper non-zero ideal in A. Then, $\sqrt{\mathfrak{a}} = \mathfrak{m}$ as we have argued earlier and thus, there is a least positive integer n such that $\mathfrak{m}^n \subseteq \mathfrak{a}$. Now, $A/\mathfrak{m}^n$ is an artinian local ring with maximal ideal $\bar{\mathfrak{m}} = \mathfrak{m}/\mathfrak{m}^2$. Consequently,

$$\dim_k(\bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2) = \dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$$

whence, due to `<insert reference>`, every ideal in $A/\mathfrak{m}^n$ is principal, in particular, $\bar{\mathfrak{a}}$ is principal.

Complete This Argument

$(e) \implies (f)$. Due to Lemma 2.17, $\mathfrak{m} \supsetneq \mathfrak{m}^2$, hence there is $x \in \mathfrak{m} \backslash \mathfrak{m}^2$. According to our hypothesis, $(x) = \mathfrak{m}^n$ for some positive integer n. Due to our choice of x, we must have $n = 1$, whence $\mathfrak{m} = (x)$. The conclusion now follows.

$(f) \implies (a)$. We shall explicitly create a valuation. First, note that we have $\mathfrak{m} = (x)$ due to maximality and due to Nakayama's Lemma, $\mathfrak{m}^k \neq \mathfrak{m}^{k+1}$ for if not, then $\mathfrak{m}^k = 0$ whereby, $\mathfrak{m} = 0$, upon taking radicals, a contradiction.

For each $a \in A$, $(a) = (x^k)$ for a unique k, since $(x^n) \supsetneq (x^{n+1})$. Define $v(a) = k$ and extend it to $K = Q(A)$ by defining $v(a/b) = v(a) - v(b)$. This is obviously a well defined valuation and $v(a/b) \geq 0$ if and only if $(a) = (x^n)$ and $(b) = (x^m)$ for $n \geq m$, whence $a \in (b)$ and $a/b \in A$. Thus A is the valuation ring of K with respect to v. This completes the proof. ∎

Proposition 7.10. *A is a DVR if and only if A is a local PID which is not a field.*

Proof. If A is a local PID which is not a field, then it is a noetherian local domain of Krull dimension 1 with a principal maximal ideal. From Theorem 7.9, we have that A is a DVR. Putting this together with Proposition 7.8, we have the desired conclusion. ∎

Proposition 7.11. *Let A be a valuation ring that is not a field. Then A is a DVR if and only if A is noetherian.*

Proof. It suffices to show the converse. Since A is noetherian, every ideal is finitely generated and thus principal. Hence, A is a DVR. ∎

7.3 Dedekind Domains

Theorem 7.12. *Let A be a noetherian domain of Krull dimension 1. Then, the following are equivalent*

(a) A is integrally closed.

(b) Every primary ideal in A is a prime power.

(c) Every local ring $A_{\mathfrak{p}}$ is a discrete valuation ring.

Proof. ∎

Definition 7.13. A ring satisfying the equivalent conditions of Theorem 7.12, is said to be a *Dedekind domain*.

Theorem 7.14. *In a Dedekind domain, every non-zero ideal has a unique factorization as a product of prime[a] ideals.*

[a] Which in this case, are maximal.

Proof. From Lemma 6.33, every ideal in a noetherian domain of Krull dimension 1 has a unique factorization as a product of prime ideals. Then, from Theorem 7.12 and Theorem 1.3, the conclusion follows. ∎

Proposition 7.15. *Let A be a Dedekind domain and $\mathfrak{a} \subseteq A$ a nonzero ideal. Then, $A/\mathfrak{a}$ is a principal ring.*

Proof. The ideal $\mathfrak{a}$ has a prime factorization $\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}$ with $A/\mathfrak{a} \cong \bigoplus_{i=1}^{s} A/\mathfrak{p}_i^{n_i}$. We shall show that each factor $A/\mathfrak{p}_i^{n_i}$ is a principal ring, by showing that for every prime ideal $\mathfrak{p}$, the ring $\overline{A} = A/\mathfrak{p}^n$ is principal for every positive integer n.

First, note that $\overline{A}$ must be artinian and local as we have argued in the previous chapters. Hence, due to Lemma 6.47, it suffices to show that the maximal ideal in $\overline{A}$ is principal. Note that the maximal ideal in $\overline{A}$ is given by $p/\mathfrak{p}^n$. If $n = 1$, then $A/\mathfrak{p}^n$ is a field and there is nothing to prove. Now, suppose $n \geq 2$. Let $\overline{p}$ denote the maximal ideal $\mathfrak{p}/\mathfrak{p}^n$ in A. Then, $\overline{\mathfrak{p}}^2 = \mathfrak{p}^2/\mathfrak{p}^n$, which may not be equal to $\overline{\mathfrak{p}}$ due to Lemma 2.17.

Choose some $\overline{a} \in \overline{\mathfrak{p}} \backslash \overline{\mathfrak{p}}^2$. We contend that $\overline{\mathfrak{p}} = (\overline{a})$. Let $a \in A$ be an element mapping to $\overline{a}$ under the projectio $A \twoheadrightarrow A/\mathfrak{p}^n$. Then, $(a) \supseteq \mathfrak{p}^n$, consequently, $\sqrt{(a)} = \mathfrak{p}$ is maximal and thus (a) is $\mathfrak{p}$-primary, whence a power of $\mathfrak{p}$. Since we chose $\overline{a}$ in $\overline{\mathfrak{p}} \backslash \overline{\mathfrak{p}}^2$, we must have $(a) = \mathfrak{p}$ which completes the proof. ∎

Corollary 7.16. Every ideal in a Dedekind domain is generated by at most two elements.

Proof. Let $\mathfrak{a} \trianglelefteq A$ be an ideal and $a \in \mathfrak{a} \backslash \{0\}$. Then, $\mathfrak{a}/(a)$ is a principal ideal. Let $b \in \mathfrak{a}$ map to a generator of $\mathfrak{a}/(a)$. Then, $(a, b) = \mathfrak{a}$. ∎

Proposition 7.17. *Let A be a Dedekind domain and $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \subseteq A$ be ideals. Then,*

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

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

Proof. ∎

Proposition 7.18. *A Dedekind domain is a UFD if and only if it is a PID.*

Proof. We shall show only the forward direction since the converse is trivial. Let $\mathfrak{p}$ be a prime ideal in A and $0 \neq a \in \mathfrak{p}$. Then, a has a factorization, $a = up_1^{e_1} \cdots p_r^{e_r}$ where the p_i's are irreducibles and $e_i > 0$. Since $\mathfrak{p}$ is a prime ideal, there is some $p_i \in \mathfrak{p}$, consequently, $(p_i) \subseteq \mathfrak{p}$. But since (p_i) is a nonzero prime ideal, it must be equal to $\mathfrak{p}$. Thus, every prime ideal in A is principal and thus A is a PID. ∎

Proposition 7.19. *A Dedekind domain with finitely many prime ideals is a PID.*

7.4 Fractional Ideals

Definition 7.20. Let A be an integral domain. A *fractional ideal* of A is a nonzero A-submodule M of $K = Q(A)$, the field of fractions such that there is $d \in A$ with $dM \subseteq A$.

Remark 7.4.1. *If M is an A-fractional ideal, then for any multiplicatively closed subset $S \subseteq A$ not containing 0, we have that $S^{-1}M$ is an $S^{-1}A$ fractional ideal. This observation will be quite useful in the future.*

The ideals contained in A are now called "integral ideals". Obviously, every integral ideal is fractions. Let M and N be A-submodules of K. Define the modified colon operator as

$$\langle M : N \rangle = \{x \in K \mid xN \subseteq M\}.$$

Similarly, one defines the sum and product of A-submodles of K as

$$\sum_{i\in I} M_i = \left\{ \sum_{\text{finite}} m_i \mid m_i \in M_i \right\}$$
$$MN = \left\{ \sum_{\text{finite}} x_i y_i \mid x_i \in M,\ y_i \in N \right\}$$

Proposition 7.21. *Let M, N, P be A-submodule of $K = Q(A)$. Then,*

$$M(N + P) = MN + MP$$

Proposition 7.22. *Let M and N be A-submodules of K and $S \subseteq A$ a multiplicative subset. Then*

(a) $S^{-1}(MN) = (S^{-1}M)(S^{-1}N)$

(b) $S^{-1}\langle M : N\rangle \subseteq \langle S^{-1}M : S^{-1}N\rangle$. *Equality holds when N is finitely generated as an A-module.*

Proof. (a). Let $x = (\sum_i m_i n_i)/s \in S^{-1}(MN)$. Then,

$$x = \sum_i (m_i/s)(n_i/1) \in (S^{-1}M)(S^{-1}N).$$

On the other hand, if $x \in (S^{-1}M)(S^{-1}N)$, then $x = \sum_i (m_i/s_i)(n_i/t_i) = \sum_i (m_i n_i/s_i t_i)$. Let $s = \prod s_i$ and $t = \prod t_i$. Then, it is not hard to see that $x = m'n'/st \in S^{-1}(MN)$ and the conclusion follows.

(b). The inclusion is obvious. To see the inclusion in the other direction, suppose N were generated by $\{n_1, \ldots, n_r\} \subseteq N$. Let $z \in \langle S^{-1}M : S^{-1}N\rangle$ and let $zn_i/1 = m_i/s_i$ with $m_i \in M$ and $s_i \in S$. Set $s = \prod_i s_i$. Then, it is clear that $szn_i \in M$ for each i and thus $sz \in \langle M : N\rangle$ whence $z \in S^{-1}\langle M : N\rangle$. This completes the proof. ■

Proposition 7.23. *Let A be a noetherian domain. Then an A-submodule M of $K = Q(A)$ is a fractional ideal if and only if M is a finitely generated A-module.*

Proof. It is not hard to see that every finitely generated A-submodule M of K is fractional, for if it is generated by $x_1/y_1, \ldots, x_n/y_n$, then choosing $y = \prod_{i=1}^n y_i$, we have $yM \subseteq A$.

On the other hand, if A is noetherian and M a fractional ideal, then there is some $d \in A$ such that $dM \subseteq A$ and is an ideal, say $\mathfrak{a} \subseteq A$. Thus $M = d^{-1}\mathfrak{a}$ and is a finitely generated A-module. ■

Definition 7.24. Let A be an integral domain. An A-submodule M of $K = Q(A)$ is said to be *invertible* if there is an A-submodule N of K with $MN = A$.

Remark 7.4.2. *Each fractional ideal of A is invertible if and only if each integral ideal of A is invertible. Indeed, suppose each integral ideal of A is invertible and M be a fractional ideal of A. Then, there is some $d \in A$ such that dM is an integral ideal whence admits an inverse N. Then, note that dN is an inverse of M.*

For an A-submodule M of K, define

$$\langle A : M\rangle = \{x \in K \mid xM \subseteq A\}.$$

It is not hard to see that $\langle A : M\rangle$ is an A-submodule of K.

Proposition 7.25. *Let A be an integral domain and M an invertible ideal of A. Then, $M^{-1} = \langle A : M \rangle$ and M is finitely generated.*

Proof. Let N denote the inverse of M. Then

$$N \subseteq \langle A : M \rangle = \langle A : M \rangle MN \subseteq AN = N.$$

Since $M\langle A : M \rangle = A$, there exist, for $1 \leq i \leq n$, $x_i \in M$ and $y_i \in \langle A : M \rangle$ such that $\sum_i x_i y_i = 1$. Hence, for any $x \in M$, we have

$$x = \sum_{i=1}^{n} x x_i y_i = \sum_{i=1}^{n} (y_i x) x_i.$$

Since each $y_i \in \langle A : M \rangle$, we have $y_i x \in A$ for $1 \leq i \leq n$, thus M is generated by $x_1, \ldots, x_n$, whence finitely generated. ■

Proposition 7.26. *Let M be a fractional ideal of an integral domain A. Then, the following are equivalent:*

(a) M is invertible.

(b) M is finitely generated and for each $\mathfrak{p} \in \operatorname{Spec} A$, $M_{\mathfrak{p}}$ is invertible.

(c) M is finitely generated and for each $\mathfrak{m} \in \operatorname{MaxSpec} A$, $M_{\mathfrak{m}}$ is invertible.

Proof. $(a) \implies (b)$ First, since M is invertible, it is finitely generated as an A-module. We have

$$A_{\mathfrak{p}} = (M\langle A : M \rangle)_{\mathfrak{p}} = M_{\mathfrak{p}} \langle A_{\mathfrak{p}} : M_{\mathfrak{p}} \rangle$$

whence $M_{\mathfrak{p}}$ is invertible.

$(b) \implies (c)$ Obvious.

$(c) \implies (a)$. Let $\mathfrak{a} = M\langle A : M \rangle$. This is an integral ideal in A. Let $\iota : \mathfrak{a} \hookrightarrow A$ denote the inclusion and let $\mathfrak{m} \subseteq A$ be a maximal ideal. Then,

$$\mathfrak{a}_{\mathfrak{m}} = M_{\mathfrak{m}} \langle A_{\mathfrak{m}} : M_{\mathfrak{m}} \rangle = A_{\mathfrak{m}}.$$

Thus $\iota_{\mathfrak{m}}$ is surjective for all maximal ideals $\mathfrak{m}$ and due to Proposition 3.13, $\mathfrak{a} = A$. ■

Proposition 7.27. *Let A be a local domain. Then A is a DVR iff every non-zero fractional ideal of A is invertible.*

Proof. $(\implies)$ Let M be a fractional ideal of A and $\mathfrak{m} = (x)$. Then, there is $y \in A$ such that $yM \subseteq A$. Let $s > 0$ be chosen such that $(y) = (x^s)$. Then, $x^s M = yM \subseteq A$ is an ordinary ideal and is therefore equal to (x^r) for some non-negative integer r. Then, $M = (x^{r-s})$ is principal and thus invertible.

$(\impliedby)$ First, every integral ideal is fractional and according to the hypothesis, finitely generated. Thus A is noetherian. We shall now show that every nonzero proper integral ideal is a power of $\mathfrak{m}$. Suppose not. Let Σ be the set of all nonzero proper integral ideals in A which are not powers of $\mathfrak{m}$. Let $\mathfrak{a} \in \Sigma$ be a maximal element[1]. Then, $\mathfrak{a} \subsetneq \mathfrak{m}$. But since $\mathfrak{m}$ is invertible, we have

$$\mathfrak{m}^{-1}\mathfrak{a} \subseteq \mathfrak{m}^{-1}\mathfrak{m} = A$$

and thus $\mathfrak{m}^{-1}\mathfrak{a}$ is a proper integral ideal which contains $\mathfrak{a}$, since $1 \in \mathfrak{m}^{-1}$. We contend that this containment is proper. For if not, then

$$\mathfrak{m}^{-1}\mathfrak{a} = \mathfrak{a} \implies \mathfrak{a} = \mathfrak{m}\mathfrak{a}$$

and due to Lemma 2.17, $\mathfrak{a} = 0$. Thus, $\mathfrak{a} \subsetneq \mathfrak{m}^{-1}\mathfrak{a}$ and due to the maximality of $\mathfrak{a}$, there is a positive integer k such that $\mathfrak{m}^{-1}\mathfrak{a} = \mathfrak{m}^k$ whence $\mathfrak{a} = \mathfrak{m}^{k+1}$, a contradiction. This completes the proof. ■

[1] We do not need to invoke Zorn for this since the ring is Noetherian.

Proposition 7.28. *Let A be an integral domain. Then A is a Dedekind domain iff every non-zero fractional ideal of A is invertible.*

Proof. ($\Longrightarrow$) Let M be a fractional ideal in A. Since A is also noetherian, M is finitely generated. Let $\mathfrak{p} \in \operatorname{Spec} A$. Then $M_\mathfrak{p}$ is a fractional ideal in the DVR $A_\mathfrak{p}$ whence invertible. We are done due to Proposition 7.26.

($\Longleftarrow$) We shall show that $A_\mathfrak{p}$ is a DVR for each $\mathfrak{p} \in \operatorname{Spec}(A)$. Due to Remark 7.4.2, it to show that every integral ideal of $A_\mathfrak{p}$ is invertible for each $\mathfrak{p} \in \operatorname{Spec}(A)$. Let $\mathfrak{b}$ be an integral ideal in $A_\mathfrak{p}$, then there is a corresponnding integral ideal $\mathfrak{a}$ in A such that $\mathfrak{b} = \mathfrak{a}_\mathfrak{p}$. According to our assumption, there is a fractional ideal M such that $\mathfrak{a}M = A$ whence $\mathfrak{a}_\mathfrak{p} M_\mathfrak{p} = A_\mathfrak{p}$ and $\mathfrak{b}$ is invertible. This completes the proof. ■

Corollary 7.29. If A is a Dedekind domain, the non-zero fractional ideals of A form a group with respect to multiplication.

7.5 Dedekind Domains and Extensions

Theorem 7.30. *Let A be a Dedekind domain with field of fractions K. If L/K is a separable field extension and B is the integral closure of A in L, then B is a Dedekind domain.*

Proof. Obviously, B is integrally closed. We now show that B has Krull dimension 1. First, note that the only prime ideal in B lying over (0) in A is (0) due to Proposition 5.12. If $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2$ in B, then their contractions $\mathfrak{p}_1^c \subsetneq \mathfrak{p}_2^c$ are prime ideals in A, where the inclusion is strict, again due to Proposition 5.12. Thus, $\mathfrak{p}_1^c = (0)$ and B has dimension 1.

Finally, that B is a noethering follows from Corollary 5.28. This completes the proof. ■

Theorem 7.31. *Let A be a Dedekind domain with field of fractions K. If L/K is a finite purely inseparable extension and B is the integral closure of A in L, then B is a Dedekind domain.*

Proof. We shall show that every ideal of B is invertible. This is equivalent to B being a Dedekind domain. Let $\operatorname{char} A = p > 0$ and $q = p^n$ be the exponent of the purely inseparable extension L/K. Let $\mathfrak{b}$ be an ideal of B and

$$\mathfrak{a} = \{b^q \mid b \in \mathfrak{b}\}A,$$

an ideal of A. Since A is a Dedekind domain, the ideal $\mathfrak{a}$ has an inverse, say $\mathfrak{a}^{-1}$. Let $\mathfrak{a}_B^{-1}$ denote the B-submodule of L generated by $\mathfrak{a}^{-1}$. Since $\mathfrak{a}^{-1}$ was a fractional ideal of A, there is some $d \in A$ such that $d\mathfrak{a}^{-1} \subseteq A$, therefore, $d\mathfrak{a}_B^{-1} \subseteq B$ and $\mathfrak{a}_B^{-1}$ is a fractional ideal of B.

Now, note that $\mathfrak{a} \subseteq \mathfrak{b}^q$ whence

$$1 \in \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{b}^q \mathfrak{a}_B^{-1} \implies B \subseteq \mathfrak{b}^q \mathfrak{a}_B^{-1}.$$

On the other hand, pick some $a \in \mathfrak{a}^{-1}$ and $b_1, \dots, b_q \in \mathfrak{b}$. Then,

$$(b_1 \cdots b_q a)^q = (b_1^q a) \cdots (b_q^q a).$$

Note that $b_i^q \in \mathfrak{a}$ an thus $b_i^q a \in A$. Therefore, $b_1 \cdots b_q a$ is integral over A and thus lies in B. Note that every element of $\mathfrak{b}^q \mathfrak{a}_B^{-1}$ is a B-linear combination of elements of th form $b_1 \cdots b_q a$ and thus lies in B, that is, $\mathfrak{b}^q \mathfrak{a}_B^{-1} \subseteq B$. Hence,

$$\mathfrak{b}^q \mathfrak{a}_B^{-1} = B \implies \mathfrak{b}^{-1} = \mathfrak{b}^{q-1} \mathfrak{a}_B^{-1}.$$

This completes the proof. ■

We immediately obtain the following result.

Corollary 7.32. Let A be a Dedekind domain with field of fractions K. If L/K is a finite extension and B is the integral closure of A in L, then B is a Dedekind domain.

7.5.1 Primes in Extensions

Throughout this section, we consider the following setup:

> A is a Dedekind domain with fraction field K. Let L/K be a finite extension and B the integral closure of A in L.

Definition 7.33. If $\mathfrak{p} \in \operatorname{Spec}(A)$, then $\mathfrak{p}B$ has a prime factorization in B, say

$$\mathfrak{p}B = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}.$$

The number e_i is called the *ramification index*. We say that $\mathfrak{P}$ divides $\mathfrak{p}$ if $\mathfrak{P}$ occurs in the factorization of $\mathfrak{p}$ in B. Further, we write $e(\mathfrak{P}/\mathfrak{p})$ for the ramification index and $f(\mathfrak{P}/\mathfrak{p})$ for the degree of the field extension $[B/\mathfrak{P} : A/\mathfrak{p}]$.

A prime is said to *ramify* if $e_i > 1$ for some i. It is said to *split* if $e_i = f_i = 1$ for all i. It is said to be *inert* if $\mathfrak{p}B$ is a prime ideal in B.

Proposition 7.34. *Let $\mathfrak{p} \in \operatorname{Spec}(A)$. Then, $\mathfrak{P}$ divides $\mathfrak{p}$ if and only if $\mathfrak{P}$ lies over $\mathfrak{p}$.*

Proof. $\implies$ Obviously $\mathfrak{P} \cap A$ contains $\mathfrak{p}$. But since $\mathfrak{p}$ is maximal, and $1 \notin \mathfrak{P}$, we have $\mathfrak{p} = \mathfrak{P} \cap A$.

$\impliedby$ Suppose $\mathfrak{P}$ lies over $\mathfrak{p}$. Then, $\mathfrak{p}B \subseteq \mathfrak{P}$. Consider the prime factorization

$$\prod_{i=1}^{r} \mathfrak{P}^{e_i} = \mathfrak{p}B \subseteq \mathfrak{P} \implies \prod_{i=1}^{r} \mathfrak{P}_i \subseteq \mathfrak{P}$$

and thus $\mathfrak{P}_i \subseteq \mathfrak{P}$ for some i. But since the $\mathfrak{P}_i$'s are maximal, we have $\mathfrak{P}_i = \mathfrak{P}$ for some i. ■

Theorem 7.35 (Ramification Formula). *Suppose L/K is separable with $[L : K] = m$ and $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ be the prime ideals dividing $\mathfrak{p}$. Then,*

$$\sum_{i=1}^{r} e_i f_i = m,$$

where $e_i = e(\mathfrak{P}_i/\mathfrak{p})$ and $f_i = f(\mathfrak{P}_i/\mathfrak{p})$.

Proof. We shall first show that $B/\mathfrak{p}B$ is a vector space of dimension m over $A/\mathfrak{p}$. It obviously is a finite dimensional vector space over $A/\mathfrak{p}$ an thus

$$B/\mathfrak{p}B \cong (A/\mathfrak{p})^s$$

for some positive integer s. Localizing at $\mathfrak{p}$, we have

$$B_{\mathfrak{p}}/(\mathfrak{p}_{\mathfrak{p}}B_{\mathfrak{p}}) \cong (A_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}})^s.$$

Note that $A_{\mathfrak{p}}$ is a DVR, in particular, a PID. Hence, $B_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module since we had already established that B was a finitely generated A-module. Let n be a positive integer such that $B_{\mathfrak{p}} \cong A_{\mathfrak{p}}^n$ as $A_{\mathfrak{p}}$-modules.

Then, upon tensoring with K, have an isomorphism[2] of $A_{\mathfrak{p}}$-modules and thus of K-vector spaces, $K^n \longrightarrow L$ whence $n = m$. On the other hand, upon tensoring with $A_{\mathfrak{p}}/\mathfrak{p}$, we have an isomorphism

$$B_{\mathfrak{p}}/(\mathfrak{p}_{\mathfrak{p}}B_{\mathfrak{p}}) \cong (A_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}})^m,$$

whence $m = s$. This proves our claim.

Now, using the Chinese Remainder Theorem, we have an isomorphism,

$$B/\mathfrak{p}B \cong \prod_{i=1}^{r} B/\mathfrak{P}_i^{e_i}.$$

Note that this is also an isomorphism as $A/\mathfrak{p}$-modules. We shall show, individually, that $[B/\mathfrak{P}_i^{e_i} : A/\mathfrak{p}] = e_i f_i$. First, consider the chain

$$B \supsetneq \mathfrak{P}_i \supsetneq \cdots \supsetneq \mathfrak{P}_i^{e_i}.$$

Since there is no ideal strictly between $\mathfrak{P}_i^j$ and $\mathfrak{P}_i^{j+1}$, each successive quotient above must have dimension 1 as a $B/\mathfrak{P}_i$-vector space. But $B/\mathfrak{P}_i$ itself is a f_i dimensional $A/\mathfrak{p}$-vector space, whence $B/\mathfrak{P}_i^{e_i}$ is $e_i f_i$ dimensional $A/\mathfrak{p}$-vector space. This completes the proof. ■

[2]In general, if $A \subseteq B$ is an integral extension of integral domains, then any element in the localization of B at $A \backslash \{0\}$. Note that any element in the fraction field of B is of the form b/b', which can be written in the form b''/a for some $b'' \in B$ and $a \in A$.

Chapter 8

Completions

8.1 Filtrations of Rings and Modules

Definition 8.1 (Filtered Ring). A *filtered ring* A is a ring A together with a family $(A_n)_{n\geq 0}$ of additive subgroups of A satisfying the conditions:

(a) $A_0 = A$,

(b) $A_{n+1} \subseteq A_n$ for all $n \geq 0$,

(c) $A_m A_n \subseteq A_{m+n}$ for all $m, n \geq 0$.

Substituting $m = 0$ In the last condition, we get $AA_n \subseteq A_n$ for all $n \geq 0$ whence each A_n is in fact an ideal in A.

Example 8.2. (a) Let $\mathfrak{a} \subseteq A$ be an ideal. Then, $A_n = \mathfrak{a}^n$ for $n \geq 0$ gives the $\mathfrak{a}$*-adic filtration* on A.

(b) Let $B \subseteq A$ be a subring. Then, given any filtration $(A_n)_{n\geq 0}$ on A, the sequence $(B \cap A_n)_{n\geq 0}$ is a filtration on B, called the *induced filtration on* B.

Definition 8.3 (Filtered Module). Let A be a filtered ring with filtration $(A_n)_{n\geq 0}$. A *filtered* A*-module* M is an A-module M together with a family $(M_n)_{n\geq 0}$ of additive subgroups of M satisfying:

(a) $M_0 = M$,

(b) $M_{n+1} \subseteq M_n$ for all $n \geq 0$,

(c) $A_m M_n \subseteq M_{m+n}$ for all $m, n \geq 0$.

Substituting $m = 0$ in the last condition, we obtain $AM_n \subseteq M_n$ for all $n \geq 0$ whence each M_n is an A-submodule of M.

Example 8.4. (a) A filtered ring is a filtered module over itself (with the filtration being the same).

(b) Let $\mathfrak{a} \subseteq A$ be an ideal, then the sequence $(\mathfrak{a}^n M)_{n\geq 0}$ of A-submodules of M forms a filtration on M, called the $\mathfrak{a}$*-adic filtration*.

(c) More generally, given a filtration $(A_n)_{n\geq 0}$ on a ring A, define $M_n := A_n M$, which gives M the structure of a filtered A-module.

(d) Let M be a filtered A-module and N an A-submodule of M. Then, we have an *induced filtration* on N and M/N given by

$$(N \cap M_n)_{n \geq 0} \quad \text{and} \quad \left(\frac{N + M_n}{N}\right)_{n \geq 0}$$

respectively.

Definition 8.5. Let M and N be filtered A-modules (over a filtered ring). A *homomorphism of filtered modules* is an A-module homomorphism $f : M \to N$ such that $f(M_n) \subseteq N_n$ for all $n \geq 0$.

Definition 8.6. A filtration $(M_n)_{n \geq 0}$ of an A-module M is said to be an $\mathfrak{a}$-*filtration* if $\mathfrak{a}M_n \subseteq M_{n+1}$ for all $n \geq 0$. And a *stable* $\mathfrak{a}$-*filtration* if there is a positive integer N such that $\mathfrak{a}M_n = M_{n+1}$ for $n \geq N$.

Definition 8.7 (Graded Ring). A *graded ring* is a ring A together with a family $(A_n)_{n \geq 0}$ of additive subgroups such that $A = \bigoplus_{n \geq 0} A_n$ and $A_m A_n \subseteq A_{m+n}$ for all $m, n \geq 0$. A nonzero element of A_n is said to be a *homogeneous element of degree* n.

Proposition 8.8. *Let $A = (A_n)_{n \geq 0}$ be a graded ring with the specified grading. Then,*

(a) A_0 is a subring,

(b) A is an A_0-module,

(c) A_n is an A_0-submodule for all $n \geq 0$.

Proof. (a) Since $A_0 A_0 \subseteq A_0$, it is closed under multiplication and obviously under addition. There is some $n \geq 0$ and $a_0, \ldots, a_n$ such that $1 = a_0 + \cdots + a_n$. Thus, $a_i = a_0 a_i + \cdots + a_n a_i$. Comparing degrees, $a_i = a_0 a_i$ for $0 \leq i \leq n$. Thus,

$$a_0 = a_0 \cdot 1 = a_0(a_0 + \cdots + a_n) = a_0 a_0 + \cdots + a_0 a_n = a_0 + \cdots + a_n = 1.$$

Hence, $1 \in A_0$ and it is a subring.

(b) Trivial.

(c) Trivial. ■

Definition 8.9. Let A be a graded ring. A *graded A-module* is an A-module M together with a family $(M_n)_{n \geq 0}$ of subgroups of M such that $M = \bigoplus_{n \geq 0} M_n$ and $A_m M_n \subseteq M_{m+n}$. A nonzero element of M_n is said to be a *homogeneous element of degree* n.

Definition 8.10. If M and N are graded A-modules, then a *homomorphism of graded A-modules* is an A-module homomorphism $f : M \to N$ such that $f(M_n) \subseteq N_n$ for all $n \geq 0$.

Proposition 8.11. *Let $A = \bigoplus_{n\geq 0} A_n$ be a graded ring. Then, the following are equivalent:*

(a) A is a Noetherian ring.

(b) A_0 is noetherian and A is an A-algebra of finite type.

Proof. $\implies$ Let $A_+ := \bigoplus_{n\geq 1} A_n$. This is obviously an ideal of A and $A/A_+ \cong A_0$ and thus is noetherian. Since A is noetherian, A_+ is a finitey generated ideal. Suppose it is generated by $x_1, \ldots, x_s$, where we may suppose that the x_i's are homogeneous with degrees $1, \ldots, s$ respectively for $s > 0$. Let A' denote the subring $A[x_1, \ldots, x_s]$ of A.

We shall inductively show that $A_n \subseteq A'$ for $n \geq 0$. The base case with $n = 0$ is trivial to prove. Let $y \in A_n$ for $n > 0$. Then, thre is a linear combination

$$y = \sum_{i=1}^{s} a_i x_i$$

where $a_i \in A$. Comparing degrees, we see that $a_i \in A_{n-i}$ with the convention that $A_k = 0$ for $k < 0$. Due to the induction hypothesis, for each i, there is a polynomial f_i with coefficients in A_0 such that $a_i = f_i(x_1, \ldots, x_s)$. Let $g = a_1 f_1 + \cdots + a_s f_s$. Then, $y = g(x_1, \ldots, x_s)$, whence, $y \in A'$. Thus, $A_n \subseteq A'$ for $n \geq 0$, consequently, $A = A'$.

$\impliedby$ Follows from Theorem 6.18. ∎

Definition 8.12 (Rees Algebra). Let $\mathfrak{a} \subseteq A$ be an ideal. Define the *Rees algebra* to be

$$A^* := \bigoplus_{n\geq 0} \mathfrak{a}^n$$

where element multiplication is the analogue of polynomial multiplication. That is, represent every element of A^* as a polynomial

$$a_0 + a_1 T + \cdots + a_n T^n$$

in some indeterminate T, where $a_i \in \mathfrak{a}^i$. It is now easy to see how multiplication is defined. The identity element is simply given by $(1, 0, \ldots)$ or in the polynomial notation, simply the monomial 1. This gives A^* the structure of a commutative ring.

Definition 8.13. Let M be a filtered A-module with filtration $(M_n)_{n\geq 0}$ over A with the $\mathfrak{a}$-adic filtration for some ideal $\mathfrak{a} \subseteq A$. Define

$$M^* := \bigoplus_{n\geq 0} M_n.$$

As in the definition of the Rees algebra, we view elements of M^* as formal polynomials

$$m_0 + m_1 T + \cdots + m_n T^n$$

in some indeterminate T, where $m_i \in M_i$. This has a natural action of the Rees algebra, A^*, by polynomial multiplication, which is well defined, since $\mathfrak{a}^i M_j \subseteq M_{i+j}$ due to the filtered structure of M. This structure also shows that M^* is a graded A^*-module with the above grading.

Proposition 8.14. *A is a noethering if and only if A^* is a noethering.*

Proof. The converse is obvious since A can be realized as a quotient of A^*. Suppose A is a noethering. Then, $\mathfrak{a}$ is finitely generated, say $\mathfrak{a} = (a_1, \dots, a_n)$. Consider the map $\varphi : A[x_1, \dots, x_n] \to A[T]$ mapping $x_i \mapsto x_i T$ (this map exists due to the universal property of the polynomial ring). It is not hard to see that $\operatorname{im} \varphi = A^* \subseteq A[T]$, whence we are done due to Theorem 6.18. ■

Proposition 8.15. *Let A be a noethering, M a finitely generated A-module and $(M_n)_{n \geq 0}$ an $\mathfrak{a}$-filtration of M. Then, the following are equivalent:*

(a) M^* is a finitely generated A^*-module.

(b) The filtration $(M_n)_{n \geq 0}$ is $\mathfrak{a}$-stable.

Proof. Since M is a finitely generated module over a noethering, it is a noetherian A-module whence each M_n is finitely generated. Let

$$Q_n := \bigoplus_{k=1}^{n} M_k T^k$$

be an A-module and M_n^* be the A^*-module generated by it. Note that M_n^* is finitely generated since each M_k is finitely generated. Further, these form an ascending chain

$$\left(M_0^* \subseteq M_1^* \subseteq \cdots \right) \subseteq M^* \tag{†}$$

Recall that A^* is noetherian. Thus, M^* is finitely generated if and only if M^* is noetherian if and only if (†) stabilizes if and only if $M^* = M_{n_0}^*$ for some $n_0 \in \mathbb{N}$. Now, let $n \geq n_0$. Let $m_{n+1} \in M_{n+1}$. Then, $m_{n+1} T^{n+1} \in M_{n+1}^* = M_n^*$ and thus

$$m_{n+1} T^{n+1} = \sum_{k=1}^{r} P_k^A(T) P_k^M(T)$$

where each P_k^A is a polynomial in A^* while P_k^M is a polynomial in Q_n. Looking at the coefficient of T^{n+1}, we see that $m_{n+1} \in \mathfrak{a} M_n$ whence $M_{n+1} = \mathfrak{a} M_n$ whereby the filtration $(M_n)_{n \geq 0}$ is stable. The converse is obvious and thus this is an equivalence thereby completing the proof. ■

Lemma 8.16 (Artin-Rees Lemma). *Let A be a noethering, $\mathfrak{a} \subseteq A$ an ideal, M a finitely-gennerated A-module, $(M_n)_{n \geq 0}$ a stable $\mathfrak{a}$-filtration of M. If M' is an A-submodule of M, then $(M' \cap M_n)_{n \geq 0}$, the induced filtration on M' is a stable $\mathfrak{a}$-filtration of M'.*

Proof. We have

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

whence the induced filtration $(M' \cap M_n)_{n \geq 0}$ is an $\mathfrak{a}$-filtration. Consider M'^* induced by this filtration. This is an A^*-submodule of M^*. Due to Proposition 8.15, M^* is a finitely generated A^*-module whence is noetherian and thus M'^* is a finitely generated A^*-module. Again, Proposition 8.15, the filtration $(M' \cap M_n)_{n \geq 0}$ is $\mathfrak{a}$-stable. This completes the proof. ■

Corollary 8.17 (Krull's Intersection Theorem). Let A be a noethering and $\mathfrak{a} \subseteq \mathfrak{R}(A)$ a proper ideal. Let M be a finitely generated A-module. Then $\bigcap_{n \geq 0} \mathfrak{a}^n M = 0$.

Proof. Let $N := \bigcap_{n \geq 0} \mathfrak{a}^n M$. Then, $\mathfrak{a}^n M \cap N = N$ for all $n \in \mathbb{N}$. The filtration $\mathfrak{a}^n M$ is $\mathfrak{a}$-stable and thus, so is the induced filtration on N. But this means $(N)_{n \geq 0}$ is a stable $\mathfrak{a}$-filtration, implying that $\mathfrak{a} N = N$ and thus $N = 0$ from Lemma 2.17. ■

Definition 8.18 (Equivalent Filtrations). Let M be a filtered A-module. Two filtrations $(M_n)_{n\geq 0}$ and $(M'_n)_{n\geq 0}$ are said to be *equivalent* if there is a positive integer k such that

$$M_{n+k} \subseteq M'_n \qquad \text{and} \qquad M'_{n+k} \subseteq M_n$$

for all $n \geq 0$.

8.2 Completion

Definition 8.19. An *inverse system* of A-modules is a collection of A-modules $(M_n)_{n\geq 0}$ and homomorphisms $(\theta_n)_{n\geq 1}$ where $\theta_n : M_n \to M_{n-1}$. If θ_n is surjective for all n, then the system is said to be a *surjective system*.

The *inverse limit* of this system is the *categorical limit* over the diagram

$$M_0 \xleftarrow{\theta_1} M_1 \xleftarrow{\theta_2} M_2 \xleftarrow{\theta_3} \cdots$$

in $A-\textbf{Mod}$.

Example 8.20. Suppose we have a filtration $M = M_0 \supseteq M_1 \supseteq \cdots$, then we have an inverse system $(M/M_n)_{n\geq 0}$ with

$$\theta_{n+1} : M/M_{n+1} \twoheadrightarrow M/M_n$$

being the natural map $x + M_{n+1} \mapsto x + M_n$. Moreover, this is a *surjective system*.

Proposition 8.21. *The inverse limit of an inverse system $((M_n)_{n\geq 0}, (\theta_n)_{n\geq 1})$ exists and is unique upto unique isomorphism.*

Proof. It suffices to show existence since the "unique upto unique isomorphism" simply follows from the fact that the inverse limit is a "universal object".

Let $N := \prod_{i\geq 0} M_i$ and $\pi_i : N \to M_i$ denote the projection. Let

$$M := \{(x_i)_{i\geq 0} \in N \mid \theta_{i+1}(x_{i+1}) = x_i \text{ for all } i \geq 0\}.$$

That this is a submodule is easy to verify. This is called the submodule of *coherent sequences*. Next, define $f_i : M \to N_i$ by the restriction $f_i = \pi_i|_M$. We contend that

$$M = \varprojlim_n M_n.$$

Indeed, let P be another A-module with maps $g_i : P \to M_i$ such that $\theta_{i+1} \circ g_{i+1} = g_i$ for all $i \geq 0$. Define the map $h : P \to M$ by $h(p) = (g_0(p), g_1(p), \ldots)$. Since this sequence is coherent, it is a valid map into M. Morover, for any $a \in A$, and $p, p' \in P$,

$$h(p + ap') = (g_i(p) + ag_i(p')) = (g_i(p)) + a(g_i(p')) = h(p) + ah(p')$$

and thus, h is an A-module homomorphism. Finally,

$$f_i \circ h(p) = f_i((g_j(p))_{i\geq 0}) = g_i(p)$$

as desired. ∎

Topological Interlude

Definition 8.22. Let G be a topological abelian group. A *fundamental system* of neighborhoods of $\{0\}$ is a descending chain of subgroups
$$G = G_0 \supseteq G_1 \supseteq \cdots .$$
such that $U \subseteq G$ is a neighborhood of 0 if and only if it contains some G_n.

Proposition 8.23. *Let G be an abelian group and $G = G_0 \supseteq G_1 \supseteq \cdots$ be a descending chain of subgroups of G. The collection*
$$\mathscr{B} := \{g + G_i \mid g \in G\}$$
forms a basis for a topology on G. Under this topology, G is a topological group.

Proof. Let $i < j$ and $h \in (g + G_i) \cap (g' + G_j)$. Then, $g - h \in G_i$ and $g' - h \in G_j \subseteq G_i$ therefore, $g - g' \in G_i$. Consequently,
$$h + G_j = g' + G_j \subseteq g' + G_i = g + G_i$$
whence $h + G_j \subseteq (g + G_i) \cap (g' + G_j)$. This shows that $\mathscr{B}$ indeed forms a basis for some topology on G.

Let $\varphi : G \times G \to G$ given by $\varphi(x, y) = x - y$. Suppose $(x, y) \in \varphi^{-1}(g + G_n)$. Then,
$$(x + G_n) \times (y + G_n) \subseteq \varphi^{-1}(g + G_n)$$
whence $\varphi^{-1}(g + G_n)$ is open. This completes the proof. ■

Definition 8.24. A sequence (x_n) in a topological abelian group G is said to be *Cauchy* if for every open neighborhood U of 0, there is a positive integer N such that $x_n - x_m \in U$ for all $m, n \geq N$.

We shall now construct the completion of a group using Cauchy sequences.

- Define a relation on the set of all Cauchy sequences in G by $(x_n) \sim (y_n)$ if and only if $x_n - y_n \to 0$ as $n \to \infty$.
- That this is an equivalence relation is easy to see, for if $(x_n) \sim (y_n)$ and $(y_n) \sim (z_n)$, then
$$\lim_{n\to\infty} (x_n - z_n) = \lim_{n\to\infty} \big((x_n - y_n) + (y_n - z_n)\big) = \lim_{n\to\infty} (x_n - y_n) + \lim_{n\to\infty} (y_n - z_n) = 0.$$
- Let $\widehat{G}$ denote the equivalence classes under the above relation. Define the operation $[(x_n)] + [(y_n)] = [(x_n + y_n)]$. It is not hard to verify that this is well defined and endows $\widehat{G}$ with the structure of an abelian group.

Proposition 8.25. *Let $\varphi : G \to \widehat{G}$ denote the map $g \mapsto [(g)]$, the equivalence class of the constant sequence. This is a homomorphism of groups and* $\ker \varphi = \bigcap U$ *where the intersection ranges over all neighborhoods of* 0.

Proof. ■

Back to Completions

Let M be a filtered module with filtration $(M_n)_{n\geq 0}$ over a filtered ring A with filtration $(A_n)_{n\geq 0}$. In accordance with Proposition 8.23, both M and A have the structure of abelian topological groups.

Proposition 8.26. *Under the aforementioned induced topology, A is a topological ring and M is a topological module. This topology is called the* ***topology induced by the filtration****.*

Proof. We have seen already that A forms a topological group under addition. It remains to show that multiplication is continuous. Let $\varphi : A \times A \to A$ be the multiplication map and $(a, b) \mapsto x \in A$. Let A_n be a neighborhood x. Then, $(a + A_n) \times (b + A_n)$ maps into $x + A_n$ under φ (this is where we use properties of the filtration) whence $\varphi^{-1}(x + A_n)$ is open in $A \times A$.

A similar proof works for the module case. ■

Proposition 8.27. *Equivalent filtrations induce the same topology on M.*

Proof. Trivial. ■

We now have a topology on the module M whence, we can form its completion, $\widehat{M}$, as outlined in the previous (sub)section.

- Let (x_n) be Cauchy in M and $a \in A$, in particular, let $a \in A_{m_0}$. Let U be a neighborhood of 0, which contains M_{n_0} for some positive integer n_0. Then, there is a positive integer n_1 such that for all $m, n \geq n_1$, $x_m - x_n \in M_{n_0}$, whereby $a(x_m - x_n) \in A_{m_0}M_{n_0} \subseteq M_{n_0} \subseteq U$.
- Further, if $(x_n) \sim (y_n)$ and $a \in A$, we must have $(ax_n) \sim (ay_n)$ using a similar argument as above.

Thus $\widehat{M}$ is also an A-module.

Proposition 8.28. $\widehat{M} \cong \varprojlim_n M/M_n$ *as A-modules.*

Proof. We shall define a map $\alpha : \widetilde{M} := \varprojlim_n M/M_n \to \widehat{M}$. Let $(y_n) \in \widetilde{M}$ be a coherent sequence. For each $n \geq 0$, pick any $x_n \in M_n$ such that $\pi_n(x_n) = y_n$ where $\pi_n : M \to M/M_n$ is the natural projection. First, note that ■

complete this

Now, let A be a filtered ring, which can be regarded as a filtered module over itself. Then, $\widehat{A}$ is an A-module. There is a natural product on this module, which can be seen easily using coherent sequences. That is,

$$[(x_n)_{n\geq 0}] \cdot [(y_n)_{n\geq 0}] = [(x_n y_n)_{n\geq 0}].$$

Thus, $\widehat{A}$ is an A-algebra, in particular, a ring in its own right.

Definition 8.29. Given inverse systems (M_n, θ_n) and (M'_n, θ'_n), a *morphism of inverse systems* $f : (M'_n)_n \to (M_n)_n$ is a family of maps $f_n : M'_n \to M_n$ for $n \geq 0$ such that the diagram

$$\begin{array}{ccc} M'_n & \xleftarrow{\theta'_{n+1}} & M'_{n+1} \\ {\scriptstyle f_n}\downarrow & & \downarrow{\scriptstyle f_{n+1}} \\ M_n & \xleftarrow{\theta_{n+1}} & M_{n+1} \end{array}$$

commutes for all $n \geq 0$. Exactness of such a sequence has the obvious definition.

A morphism as above induces a map $f_* : \varprojlim_n M'_n \to \varprojlim_n M_n$ given by $(x_n) \mapsto (f_n(x_n))$. The commutativity of the diagram ensures that the sequence on the right is coherent.

Proposition 8.30. *Let* $0 \to \{A_n\} \to \{B_n\} \to \{C_n\} \to 0$ *be an exact sequence of inverse systems. Then*

$$0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n$$

is exact. Further, if $\{A_n\}$ *is a surjective system, then*

$$0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n \to 0$$

is exact.

Proof. Define the map $d^A : \prod_n A_n \to \prod_n A_n$ as

$$d^A((a_n)) = (a_n - \theta_{n+1}(a_{n+1})).$$

Similarly, define d^B and d^C. These obviously are morphisms and fit into the following commutative diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \prod_n A_n & \longrightarrow & \prod_n B_n & \longrightarrow & \prod_n C_n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d^A} & & \downarrow{\scriptstyle d^B} & & \downarrow{\scriptstyle d^C} & & \\ 0 & \longrightarrow & \prod_n A_n & \longrightarrow & \prod_n B_n & \longrightarrow & \prod_n C_n & \longrightarrow & 0 \end{array}$$

From the Snake Lemma, we have an exact sequence

$$0 \longrightarrow \ker d^A \longrightarrow \ker d^B \longrightarrow \ker d^C \longrightarrow \operatorname{coker} d^A.$$

It remains to show that d^A is surjective when $\{A_n\}$ is a surjective system. Indeed, let $(a_n) \in \prod_n A_n$. Choose any $x_0 \in A_0$ and inductively choose x_{n+1} such that $\theta_{n+1}(x_{n+1}) = x_n - a_n$. Then, $d^A((x_n)) = (a_n)$. This completes the proof. ∎

Corollary 8.31. Let

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

be an exact sequence and $(M_n)_{n\geq 0}$ a filtration of M with induced filtrations on M' and M''. If completions are taken with respect to these filtrations, the sequence

$$0 \longrightarrow \widehat{M'} \longrightarrow \widehat{M} \longrightarrow \widehat{M''} \longrightarrow 0$$

is exact.

Corollary 8.32. Let M be an A-module with filtration $(M_n)_{n\geq 0}$ and completion $\widehat{M}$. Then, the completion $\widehat{M}_n$ of M_n with respect to the induced filtration is a submodule of $\widehat{M}$ and $\widehat{M}/\widehat{M}_n \cong M/M_n$ for all $n \geq 0$.

Proof. The first assertion follows from the exactness of completion. As for the second assertion, again, using the exactness of completion, we have

$$\frac{\widehat{M}}{\widehat{M}_n} \cong \widehat{\left(\frac{M}{M_n}\right)}.$$

Note that the induced topology on M/M_n is the discrete topology whence

$$\widehat{\left(\frac{M}{M_n}\right)} \cong \frac{M}{M_n}.$$ ∎

Corollary 8.33. Let M be an A-module with filtration $(M_n)_{n\geq 0}$. This induces a filtration $(\widehat{M}_n)_{n\geq 0}$ on $\widehat{M}$ and $\widehat{\widehat{M}} \cong \widehat{M}$.

Proof. Note that the isomorphism $M/M_n \cong \widehat{M/M_n}$. Now, consider the following commutative diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_{n+1} & \longrightarrow & M & \longrightarrow & M/M_{n+1} & \longrightarrow & 0 \\ & & \downarrow & & \| & & \downarrow & & \\ 0 & \longrightarrow & M_n & \longrightarrow & M & \longrightarrow & M/M_n & \longrightarrow & 0 \end{array}$$

Taking completions, we obtain another commutative diagram

$$\begin{array}{ccccc} \frac{M}{M_{n+1}} & \longrightarrow & \widehat{\frac{M}{M_{n+1}}} & \longrightarrow & \frac{\widehat{M}}{\widehat{M}_{n+1}} \\ \downarrow & & \downarrow & & \downarrow \\ \frac{M}{M_n} & \longrightarrow & \widehat{\frac{M}{M_n}} & \longrightarrow & \frac{\widehat{M}}{\widehat{M}_n} \end{array}$$

where all the horizontal arrows are isomorphisms. Thus,

$$\varprojlim M/M_n \cong \varprojlim \widehat{M}/\widehat{M}_n. \qquad \blacksquare$$

Let M be an A-module. There is a canonical map $M \to \widehat{M}$ given by $m \mapsto (m)_{n\geq 0}$. Upon tensoring with $\widehat{A}$, we have a map $\widehat{A} \otimes_A M \to \widehat{A} \otimes_A \widehat{M}$ which, on elementary tensors is given by

$$(a_n)_{n\geq 0} \otimes_A m \mapsto (a_n) \otimes_A (m)_{n\geq 0},$$

where we are denoting the elements of $\widehat{A}$ by Cauchy sequences.

Now, consider the map $\widehat{A} \otimes_A \widehat{M} \to \widehat{M}$ given by

$$(a_n)_{n\geq 0} \otimes_A (m_n)_{n\geq 0} \mapsto (a_n m_n)_{n\geq 0}.$$

Composing this with the previous maps, we obtain a map $\phi_M : \widehat{A} \otimes_A M \to \widehat{M}$ given by

$$(a_n)_{n\geq 0} \otimes_A m \mapsto (a_n m)_{n\geq 0}.$$

It is not hard to verify that this map is indeed $\widehat{A}$-linear between $\widehat{A}$-modules. Note that this map is valid for all filtered modules M over a filtered ring A. So is the following theorem.

Theorem 8.34. *If M is finitely generated, then ϕ_M is surjective. Further, if A is noetherian, then ϕ_M is an isomorphism.*

Proof. If M and N are two A-modules, then it is not hard to verify that the following diagram commutes:

$$\begin{array}{ccc} (\widehat{A} \otimes_A M) \oplus (\widehat{A} \otimes_A N) & \xrightarrow{\sim} & \widehat{A} \otimes_A (M \oplus N) \\ \downarrow{\scriptstyle \phi_M \oplus \phi_N} & & \downarrow{\scriptstyle \phi_{M\oplus N}} \\ \widehat{M} \oplus \widehat{N} & \xrightarrow[\sim]{} & \widehat{M \oplus N} \end{array}$$

where the horizontal map on the bottom is given by $(m_i)_{i\geq 0} \oplus (n_i)_{i\geq 0} \mapsto (m_i \oplus n_i)_{i\geq 0}$. Now, note that $\phi_A : \widehat{A} \otimes_A A \to \widehat{A}$ is obviously an isomorphism. Thus, inductively, ϕ_F is an isomorphism whenever F is a finite dimensional free A-module.

Now, if M is finitely generated, then, there is a finite dimensional free module F and an exact sequence $N \to F \to M \to 0$. This fits into a commutative diagram,

$$\begin{array}{ccccccc} N & \longrightarrow & F & \longrightarrow & M & \longrightarrow & 0 \\ \phi_N \big\downarrow & & \phi_F \big\downarrow \wr & & \phi_M \big\downarrow & & \big\| \\ \widehat{N} & \longrightarrow & \widehat{F} & \longrightarrow & \widehat{M} & \longrightarrow & 0 \end{array}$$

with exact rows. Thus, ϕ_M is a surjection. Now, if A is noetherian, then N is finitely generated, since it is a submodule of F, which is a noetherian A-module. Due to the Four Lemma, ϕ_M must be an injection whence an isomorphism. This completes the proof. ■

8.3 $\mathfrak{a}$-adic filtration

Let A be a fitered ring with filtration $(A_n)_{n\geq 0}$ and M a filtered A-module with filtration $(M_n)_{n\geq 0}$. We shall show that $\widehat{M}$ has the structure of a $\widehat{A}$-module. Indeed, for $(x_n)_{n\geq 0} \in \widehat{M}$ and $(a_n)_{n\geq 0} \in \widehat{A}$, define

$$(a_n)_{n\geq 0} \cdot (x_n)_{n\geq 0} = (a_n x_n)_{n\geq 0}.$$

To see that this is well defined, suppose $(a_n)_{n\geq 0} \sim (a'_n)_{n\geq 0}$ and $(x_n)_{n\geq 0} \sim (x'_n)_{n\geq 0}$. Then,

$$a_n x_n - a'_n x'_n = a_n(x_n - x'_n) + (a_n - a'_n)x'_n.$$

Consider a basic open set A_m containing 0. For sufficiently large n, $x_n - x'_n \in M_m$ and $a_n - a'_n \in A_m$. The conlusion now follows.

Next, we examine the functoriality of completion. If $f : M \to N$ is a homomorphism of filtered A-modules, then there is an induced map $\widehat{f} : \widehat{M} \to \widehat{N}$ of filtered $\widehat{A}$-modules given by

$$f((x_n)_{n\geq 0}) = (f(x_n))_{n\geq 0}.$$

This map is obviously $\widehat{A}$-linear. It is also not hard to see that

$$\widehat{g \circ f} = \widehat{g} \circ \widehat{f} \qquad \text{and} \qquad \widehat{\mathbf{id}_M} = \mathbf{id}_{\widehat{M}}$$

whence completion is a functor from the category of filtered A-modules to the category of $\widehat{A}$-modules.

Proposition 8.35. *Let A be a noetherian ring and $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ be a short exact sequence of finitely generated A-modules. Then,*

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

is a short exact sequence of $\widehat{A}$-modules where the completions are $\mathfrak{a}$-adic for some ideal $\mathfrak{a} \trianglelefteq A$.

Proof. We may treat M' as a submodule of M. The induced filtration is just $(M' \cap \mathfrak{a}^n M)_{n\geq 0}$. Due to Lemma 8.16, this is a stable $\mathfrak{a}$-filtration of M' whence, is equivalent to the filtration $(\mathfrak{a}^n M')_{n\geq 0}$. Thus, the completions are also isomorphic. Next, the induced filtration on M'' is obviously $(\mathfrak{a}^n M'')_{n\geq 0}$. The conclusion now follows from the exactness of completion. ■

Corollary 8.36. In particular, $\widehat{A}$ is a flat A-module when A is noetherian.

Proposition 8.37. *Let A be a noethering, $\mathfrak{b} \trianglelefteq A$ an ideal in A, and $\widehat{A}$ the $\mathfrak{a}$-adic completion for an ideal $\mathfrak{a} \trianglelefteq A$. Then,*

(a) $\widehat{\mathfrak{b}} = \mathfrak{b}\widehat{A}$.

(b) $\widehat{\mathfrak{b}^n} = \widehat{\mathfrak{b}}^n$.

(c) $\mathfrak{b}^n/\mathfrak{b}^{n+1} \cong \widehat{\mathfrak{b}}^n/\widehat{\mathfrak{b}}^{n+1}$ *for all* $n \geq 0$.

(d) $\widehat{\mathfrak{b}}$ *is contained in the Jacobson radical of* $\widehat{A}$.

Proof. (a) Consider the injection $\mathfrak{b} \hookrightarrow A$. Upon tensoring with $\widehat{A}$, we obtain an injection $\mathfrak{b} \otimes_A \widehat{A} \hookrightarrow \widehat{A}$. The image of $\mathfrak{b} \otimes_A \widehat{A}$ under this map is given by $\mathfrak{b}\widehat{A}$, which is also the extension of the ideal $\mathfrak{b}$ under canonical map $A \to \widehat{A}$.

(b) Follows (a), since

$$\widehat{\mathfrak{b}^n} = \underbrace{\mathfrak{b}^n\widehat{A} = (\mathfrak{b}\widehat{A})^n}_{\text{since we are extending an ideal}} = (\widehat{b})^n.$$

(c) Recall that $A/\mathfrak{b}^n \cong \widehat{A}/\widehat{\mathfrak{b}^n}$. Now, apply the third isomorphism theorem.

(d) For any $a \in \widehat{\mathfrak{a}}$, note that $1 - a$ is a unit since it has an inverse $1 + a + a^2 + \cdots$. This converges since $a^n \in \mathfrak{a}^n$ and the topology on $\widehat{A}$ is given by the fundamental system $\widehat{A} \supseteq \widehat{\mathfrak{a}} \supseteq \widehat{\mathfrak{a}}^2 \supseteq \cdots$. Ths conclusion now follows. ■

Corollary 8.38. If $(A, \mathfrak{m}, k)$ is a noetherian local ring, then $\widehat{R}$ is a local ring with unique maximal ideal, $\widehat{\mathfrak{m}}$.

Theorem 8.39 (Krull's Intersection Theorem). *Let A be a noethering, M a finitely generated A-module and $\mathfrak{a} \trianglelefteq A$ an ideal. Let $\widehat{M}$ be the $\mathfrak{a}$-adic completion of M. Then, the kernel of the canonical map $M \to \widehat{M}$ consists of precisely those elements of M that are annihilated by some element of $1 + \mathfrak{a}$. That is,*

$$\bigcap_{n=0}^{\infty} \mathfrak{a}^n M = \left\{ x \in M \mid \exists a \in \mathfrak{a},\ (1+a)x = 0 \right\}.$$

Proof. Note that the kernel of the map is precisely equal to $\bigcap_{n=0}^{\infty} \mathfrak{a}^n M$. First, if $x \in M$ is annihilated by $1 + a$ for some $a \in \mathfrak{a}$, then

$$x = -ax = a^2x = -a^3x = \cdots \in \bigcap_{n=0}^{\infty} \mathfrak{a}^n M.$$

Conversely, let $N = \bigcap_{n=0}^{\infty} \mathfrak{a}^n M$. Then, due to Lemma 8.16, there is a positive integer n such that

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

for all $k \geq 0$. Choosing $k = 1$ and applying Corollary 2.16, the desired conclusion follows. ■

Corollary 8.40. If A is a noetherian domain and $\mathfrak{a} \triangleleft A$ is a proper ideal, then $\bigcap_{n=0}^{\infty} \mathfrak{a}^n = (0)$.

Proof. Every element of $1 + \mathfrak{a}$ is nonzero and thus cannot annihilate any other nonzero element. ■

8.3.1 Associated Graded Stuff

Definition 8.41 (Associated Graded Ring). Let A be a filtered ring with filtration $(A_n)_{n\geq 0}$. Define

$$G_n(A) := A_n/A_{n+1} \quad \text{and} \quad G(A) := \bigoplus_{n\geq 0} G_n(A).$$

This has a natural multiplication structure given by $(a+A_{n+1})(b+A_{m+1}) = ab + A_{m+n+1}$, where $a \in A_n$ and $b \in A_m$. This gives $G(A)$ the structure of a graded ring and is known as the *associated graded ring* of A.

To see that the multiplication is well defined, suppose $a' \in A_n$ and $b' \in A_m$ such that $a + A_{n+1} = a' + A_{n+1}$ and $b + A_{m+1} = b' + A_{m+1}$. Then,

$$ab - a'b' = (a-a')b + a'(b-b') \in A_{m+n+1}.$$

Remark 8.3.1. *If A has the $\mathfrak{a}$-adic filtration for an ideal $\mathfrak{a} \trianglelefteq A$, then we denote $G(A)$ by $G_{\mathfrak{a}}(A)$ to be explicit.*

Definition 8.42 (Associated Graded Module). Let A be a filtered ring with filtration $(A_n)_{n\geq 0}$ and M a filtered A-module with filtration $(M_n)_{n\geq 0}$. Define

$$G_n(M) := M_n/M_{n+1} \quad \text{and} \quad G(M) := \bigoplus_{n\geq 0} G_n(M).$$

This has a natural $G(A)$-module structure given by

$$(a + A_{m+1})(x + M_{n+1}) = ax + M_{m+n+1}$$

for $a \in A_m$ and $x \in M_n$. This is called the *associated graded module* of M.

To see that the multiplication is well defined, suppose $a' \in A_m$ and $x' \in M_n$ such that $a + A_{m+1} = a' + A_{m+1}$ and $x + M_{n+1} = x' + M_{n+1}$. Then,

$$ax - a'x' = (a-a')x + (x-x')a' \in M_{m+n+1}.$$

Definition 8.43 (Functoriality of G). Let A be a filtered ring with filtration $(A_n)_{n\geq 0}$ and M, N filtered A-modules with filtrations $(M_n)_{n\geq 0}$ and $(N_n)_{n\geq 0}$ respectively. Let $f : M \to N$ be a homomorphism of filtered A-modules.

Define $G(f) : G(M) \to G(N)$ on homogeneous elements by

$$G(f)(x + M_{n+1}) = f(x) + N_{n+1}.$$

This is a homomorphism of graded $G(A)$-modules. Further, it is functorial, which is not hard to verify.

Theorem 8.44. *Let A be a noethering and $\mathfrak{a} \trianglelefteq A$. Then,*

(a) $G_{\mathfrak{a}}(A)$ is a noethering.

(b) $G_{\mathfrak{a}}(A)$ and $G_{\widehat{\mathfrak{a}}}(\widehat{A})$ are isomorphic as graded rings.

(c) if M is a finitely generated A-module, and $(M_n)_{n\geq 0}$ is a stable $\mathfrak{a}$-filtration of M, then $G(M)$ is a finitely

generated $G_{\mathfrak{a}}(A)$-module.

Proof. (a) Let $\mathfrak{a} = (x_1, \ldots, x_s)$ as an A-module and let $\overline{x}_i$ denote the image of x_i under the projection $A \twoheadrightarrow A/\mathfrak{a}$. It is obvious that $G_{\mathfrak{a}}(A) \cong A/\mathfrak{a}[\overline{x}_1, \ldots, \overline{x}_s]$. Therefore, $G_{\mathfrak{a}}(A)$ is a nothering.

(b) Follows from Proposition 8.37.

(c) There is an $n_0 \geq 0$ such that $M_{n_0+r} = \mathfrak{a}^r M_{n_0}$ for all $r \geq 0$. We contend that $G(M)$ is generated by $\bigoplus_{n=0}^{n_0} G_n(M)$ as a $G_{\mathfrak{a}}(A)$-module. Indeed, consider some homogeneous element $\overline{x} \in M_{n_0+r}/M_{n_0+r+1}$, and $x \in M_{n_0+r}$ such that $\overline{x} = x + M_{n_0+r+1}$. Then, there is some $y \in M_{n_0}$ and $a \in \mathfrak{a}^r$ such that $ay = x$. It now follows that $\overline{ay} = \overline{x}$ where $\overline{y} \in G_{n_0}(M)$ and $\overline{a}$ is the image of a in $\mathfrak{a}^r/\mathfrak{a}^{r+1}$.

Finally, note that each $G_n(M)$ is a finitely generated $A/\mathfrak{a}$-module for $n \leq n_0$. Whence, $G(M)$ is a finitely generated $G_{\mathfrak{a}}(A)$-module. ■

Lemma 8.45. *Let A be a filtered ring and M, N filtered A-modules. Let $\widehat{\phi}$ and $G(\phi)$ denote the induced maps between the associated graded modules and completed modules respectively. Then,*

(a) if $G(\phi)$ is injective, then $\widehat{\phi}$ is injective.

(b) if $G(\phi)$ is surjective, then $\widehat{\phi}$ is surjective.

Proof. The map ϕ induces maps $\alpha_n : M/M_n \to N/N_n$, which is not hard to see from the universal property of the quotient. This gives us a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_n/M_{n+1} & \longrightarrow & M/M_{n+1} & \longrightarrow & M/M_n & \longrightarrow & 0\ . \\ & & \downarrow{\scriptstyle G_n(\phi)} & & \downarrow{\scriptstyle \alpha_{n+1}} & & \downarrow{\scriptstyle \alpha_n} & & \\ 0 & \longrightarrow & N_n/N_{n+1} & \longrightarrow & N/N_{n+1} & \longrightarrow & N/N_n & \longrightarrow & 0 \end{array}$$

Due to the Snake Lemma, we have the following exact seqence

$$0 \to \ker G_n(\phi) \to \ker \alpha_{n+1} \to \ker \alpha_n \to \operatorname{coker} G_n(\phi) \to \operatorname{coker} \alpha_{n+1} \to \operatorname{coker} \alpha_n \to 0.$$

Suppose $G(\phi)$ is injective. Then, each $G_n(\phi)$ is injective, whence we can inductively argue that $\ker \alpha_n = 0$ for every $n \geq 0$ since the base case $\ker \alpha_0 = 0$ is trivial.

Consequently, $\alpha : \{M/M_n\} \to \{N/N_n\}$ is an injective map of surjective systems. Consequently, under the inverse limit, it induces an injective map $\widehat{\phi} : \widehat{M} \to \widehat{N}$. Similarly, one can handle the case when $G(\phi)$ is surjective. This completes the proof. ■

Lemma 8.46. *Let $\mathfrak{a} \trianglelefteq A$ such that A is complete in the $\mathfrak{a}$-topology and M an A-module with $(M_n)_{n \geq 0}$ an $\mathfrak{a}$-filtration of M in which M is Hausdorff. If $G(M)$ is a finitely generated $G(A)$-module, then M is a finitely generated A-module.*

Proof. Suppose $G(M)$ is generated by the homogeneous elements y_i for $1 \leq i \leq s$ with homogeneous degree of y_i being $n(i) \geq 0$. There is a corresponding $x_i \in M_{n(i)}$ whose image in $G_{n(i)}(M)$ is y_i. Let $F^{(i)}$ denote the A-module A with $\mathfrak{a}$-filtration given by $F_k^{(i)} = \mathfrak{a}^{n(i)+k}$. Finally, let $F = \bigoplus_{i=1}^{s} F^{(i)}$. Let $\phi^{(i)} : F^{(i)} \to M$ denote the map sending $1 \in F^{(i)}$ to $x_i \in M$. This induces a homomorphism of filtered A-modules $\phi : F \to M$. This map in turn, induces a $G(A)$-module homomorphism $G(\phi) : G(F) \to G(M)$.

According to the way we had chosen the x_i's, the map $G(\phi)$ is surjective and thus, $\widehat{\phi} : \widehat{F} \to \widehat{M}$ is surjective. Let $\alpha : F \to \widehat{F}$ and $\beta : M \to \widehat{M}$ denote the canonical maps. The following diagram commutes.

$$\begin{array}{ccc} F & \xrightarrow{\phi} & M \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ \widehat{F} & \xrightarrow[\widehat{\phi}]{} & \widehat{M} \end{array}$$

Since A is complete in the $\mathfrak{a}$-adic topology we see that $A \cong \widehat{A}$ and since F is a free A-module, the map α must be an isomorphism. Further, since M is Hausdorff in its chosen filtration, the map β is an injection. Since the map $\widehat{\phi} \circ \alpha$ is a surjection, it must be the case that ϕ is a surjection, consequently, M is finitely generated. ■

Corollary 8.47. With the hypotheses of Lemma 8.46, if $G(M)$ is a noetherian $G(A)$-module, then M is a noetherian A-module.

Proof. Let $M' \subseteq M$ be a submodule. We shall show that M' is finitely generated. If $(M_n)_{n \geq 0}$ is the filtration of M, then the induced filtration $(M' \cap M_n)_{n \geq 0}$ is also an $\mathfrak{a}$-filtration, which we denote by $(M'_n)_{n \geq 0}$. Note that the inclusion $M'_n \hookrightarrow M_n$ induces an injective homomorphism $M'_n/M'_{n+1} \hookrightarrow M_n/M_{n+1}$. Thus, the inclusion map $M' \hookrightarrow M$ which is also a map of filtered modules, induces an injective map $G(M') \hookrightarrow G(M)$. Since $G(M)$ is noetherian, $G(M')$ must be a finitely generated $G_{\mathfrak{a}}(A)$-module. Finally, we also have

$$\{0\} \subseteq \bigcap_{n=0}^{\infty} M'_n \subseteq \bigcap_{n=0}^{\infty} M_n = \{0\}.$$

Now, we can complete using Lemma 8.46. ■

Theorem 8.48. *If A is a noethering and $\mathfrak{a} \trianglelefteq A$, then the $\mathfrak{a}$-adic completion $\widehat{A}$ of A is a noethering.*

Proof. Due to Theorem 8.44, $G_{\mathfrak{a}}(A) \cong G_{\widehat{\mathfrak{a}}}(\widehat{A})$ and $G_{\mathfrak{a}}(A)$ is a noethering. Apply Corollary 8.47 to the complete ring $\widehat{A}$ and take $M = \widehat{A}$ with the filtration $(\widehat{\mathfrak{a}}^n)_{n \geq 0}$. Note that this filtration induces a Hausdorff topology since $\widehat{a}$ is contained in the Jacobson radical of $\widehat{A}$. This completes the proof. ■

Theorem 8.49. *Let $(A, \mathfrak{m}, k)$ be a noetherian local ring and M, N be finitely generated A-modules. Let $\widehat{(\cdot)}$ denote the $\mathfrak{m}$-adic completion. If $\widehat{M} \cong \widehat{N}$, then $M \cong N$.*

Proof. ■

Chapter 9

Dimension Theory

9.1 Hilbert Polynomial

Throughout this section, let $A = \bigoplus_{n=0}^{\infty} A_n$ be a noetherian graded ring and λ a $\mathbb{Z}$-valued additive function on the category of A-modules.

Definition 9.1 (Euler-Poincaré Series). Associate with each A-module M, the *Euler-Poincaré* series,

$$P_\lambda(M,t) = \sum_{n=0}^{\infty} \lambda(M_n)t^n \in \mathbb{Z}[\![t]\!].$$

We often write $P(M,t)$ for $P_\lambda(M,t)$ when the additive function is clear.

Theorem 9.2 (Hilbert-Serre). *$P(M,t)$ is a rational function in t of the form*

$$P(M,t) = \frac{f(t)}{\prod_{i=1}^{n}(1-t^{n_i})}$$

where $f(t) \in \mathbb{Z}[t]$.

Proof. Suppose A is generated over A_0 by s homomgeneous elements, $x_1, \ldots, x_s$. We shall induct on s. Let k_s denote the degree of x_s. Then, for all $n \geq 0$, we have an exact sequence

$$0 \to K_n \to M_n \xrightarrow{x_s} M_{n+k_s} \to L_{n+k_s} \to 0.$$

Thus,

$$\lambda(K_n) - \lambda(M_n) + \lambda(M_{n+k_s}) - \lambda(L_{n+k_s}).$$

Multiplying by t^{n+k_s} and adding, we obtain

$$\begin{aligned} 0 &= t^{k_s}\sum_{n=0}^{\infty}\lambda(K_n)t^n - t^{k_s}\sum_{n=0}^{\infty}\lambda(M_n)t^n + \sum_{n=0}^{\infty}\lambda(M_{n+k_s})t^{n+k_s} - \sum_{n=0}^{\infty}\lambda(L_{n+k_s})t^{n+k_s} \\ &= t^{k_s}P(K_n,t) - t^{k_s}P(M,t) + P(M,t) - P(L,t) + g(t) \end{aligned}$$

where $g(t) \in \mathbb{Z}[t]$. Note that $K = \bigoplus_{n=0}^{\infty} K_n$ and $L = \bigoplus_{n=0}^{\infty} L_n$ is a graded $A' = A_0[x_1, \ldots, x_{s-1}]$. Invoking the induction hypothesis, we are done. ■

Proposition 9.3. *Let $(A, \mathfrak{m})$ be a noetherian local ring with $\mathfrak{q}$ an $\mathfrak{m}$-primary ideal, M a finitely generated A-module and $(M_n)_{n\geq 0}$ a $\mathfrak{q}$-stable filtration. Then,*

(a) M/M_n is of finite length for every $n \geq 0$.

(b) for all sufficiently large n, this length is a polynomial $g(n)$ of degree $\leq s$ where s is the least number of generators of $\mathfrak{q}$.

(c) the degree and leading coefficient of $g(n)$ is independent of the chosen filtration.

Proof. (a) Note that M_i/M_{i+1} is naturally an $A/\mathfrak{q}$-module, which has finite length, since $A/\mathfrak{q}$ is Artin local. Using the additivity of length, we have

$$l(M/M_n) = \sum_{i=1}^{n}(M_{i-1}/M_i),$$

which is finite.

(b)

(c) Let $(\widetilde{M}_n)_{n\geq 0}$ be another $\mathfrak{q}$-stable filtration of M. Then, these two are equivalent filtrations, that is, there is $n_0 > 0$ such that $M_{n+n_0} \subseteq \widetilde{M}_n$ and $\widetilde{M}_{n+n_0} \subseteq M_n$ for all $n \geq 0$. Thus, $\widetilde{g}(n+n_0) \geq g(n)$ and $g(n+n_0) \geq \widetilde{g}(n)$. Consequently, $\lim_{n\to\infty} g(n)/\widetilde{g}(n) = 1$. This completes the proof. ■

Definition 9.4 (Hilbert-Samuel Polynomial). With the notation of Proposition 9.3, the polynomial $g(n)$ corresponding to the filtration $(\mathfrak{q}^n)_{n\geq 0}$ is denoted by $\chi_{\mathfrak{q}}^M(n)$ and is called the *Hilbert-Samuel polynomial*. For sufficiently large n, we have

$$\chi_{\mathfrak{q}}^M(n) = l(M/\mathfrak{q}^n M).$$

If $M = A$, we write $\chi_{\mathfrak{q}}(n)$ for $\chi_{\mathfrak{q}}^A(n)$ and call it the *characteristic polynomial* of the $\mathfrak{m}$-primary ideal $\mathfrak{q}$.

Corollary 9.5. Let $(A, \mathfrak{m})$ be a noetherian local ring and $\mathfrak{q}$ an $\mathfrak{m}$-primary ideal in A. Then, the length $l(A/\mathfrak{q}^n)$ is a polynomial $\chi_{\mathfrak{q}}(n)$ of degree $\leq s$ for sufficiently large n, where s is the least number of generators of $\mathfrak{q}$.

Proposition 9.6. *Let $(A, \mathfrak{m})$ be a noetherian local ring and $\mathfrak{q}$ an $\mathfrak{m}$-primary ideal in A. Then,*

$$\deg \chi_{\mathfrak{q}}(n) = \deg \chi_{\mathfrak{m}}(n).$$

Proof. There is a positive integer $r > 0$ such that $\mathfrak{m}^r \subseteq \mathfrak{q} \subseteq \mathfrak{m}$. Then, for sufficiently large n, we have

$$\chi_{\mathfrak{m}}(n) \leq \chi_{\mathfrak{q}}(n) \leq \chi_{\mathfrak{m}}(rn).$$

Since the $\chi_{\mathfrak{m}}$ and $\chi_{\mathfrak{q}}$ are polynomials for sufficiently large n, it must be th case that $\deg \chi_{\mathfrak{m}} = \deg \chi_{\mathfrak{q}}$. This completes the proof. ■

Definition 9.7. With the notation of Proposition 9.6, let $d(A)$ denote the degree of $\chi_{\mathfrak{m}}$.

9.2 Noetherian Local Rings

Throughout this section, let $(A, \mathfrak{m})$ be a noetherian local ring with maximal ideal $\mathfrak{m}$. Denote by $\delta(A)$, the least number of generators of an $\mathfrak{m}$-primary ideal of A. From the last section, we already know that $\delta(A) \geq d(A)$.

Lemma 9.8. *Let M be a finitely-generated A-module, $x \in A$ not a zero-divisor in M, and $M' = M/xM$. Then,*

$$\deg \chi_{\mathfrak{q}}^{M'} \leq \chi_{\mathfrak{q}}^{M} - 1.$$

Proof. Let $N = xM$, and $N_n = N \cap \mathfrak{q}^n M$. Then, due to Lemma 8.16, $(N_n)_{n \geq 0}$ is a $\mathfrak{q}$-stable filtration of N. ■

complete this

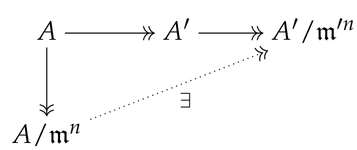
Corollary 9.9. If x is not a zero-divisor in A, then $d(A/(x)) \leq d(A) - 1$.

Proposition 9.10. $d(A) \geq \dim A$.

Proof. We shall induct on $d(A)$. If $d(A) = 0$, then $l(A/\mathfrak{m}^n)$ is eventually constant. Therefore, $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ for sufficiently large n, whence $\mathfrak{m} = 0$, i.e. A is artinian and $\dim A = 0$.

Suppose now that $d = 0$ and let $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ be any chain of prime ideals in A. If $r = 0$, then there is nothing more to prove. If $r > 0$, then let $x \in \mathfrak{p}_1 \backslash \mathfrak{p}_0$ and let $A' = A/\mathfrak{p}_0$ with x' denoting the image of x in A'.

Let $\mathfrak{m}'$ denote the image of $\mathfrak{m}$ under the surjection $A \twoheadrightarrow A'$. Then, $(A', \mathfrak{m}')$ is a local ring with an induced surjection $A/\mathfrak{m}^n \twoheadrightarrow A'/\mathfrak{m}'^n$ through the following commutative diagram.



Consequently, $l(A/\mathfrak{m}^n) \geq l(A'/\mathfrak{m}'^n)$. Therefore, $d(A) \geq d(A')$, due to the standard polynomial argument.

Now, $d(A'/(x')) \leq d(A') - 1 \leq d(A) - 1$ and hence, the induction hypothesis applies to $A'/(x')$, that is, $d(A'/(x')) \geq \dim A'/(x')$. Note that the image of the strictly ascending chain $\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ in $A'/(x')$ is a strictly ascending chain of prime ideals of length $r - 1$ whence

$$r - 1 \leq \dim A'/(x') \leq d(A'/(x')) \leq d(A) - 1 \implies r \leq d(A)$$

which completes the proof. ■

Corollary 9.11. If A is a noetherian local ring, then $\dim A$ is finite.

Corollary 9.12. A prime ideal in a noethering has finte height. Therefore, the set of primes in a noethering satisfies the descending chain condition.

Proposition 9.13. *Let* $\dim A = d$*. Then, there exists an* $\mathfrak{m}$*-primary ideal in* A *generated by* d *elements. Therefore,* $\dim A \geq \delta(A)$*.*

Proof. We shall inductively construct a sequence $x_1, \ldots, x_d$ of elements in A such that the ideal $(x_1, \ldots, x_i)$ has height at least i. First, if $d = 0$, then A is an artinian local ring and the conclusion follows since $\mathfrak{m}$ is nilpotent.

Suppose now that $d \geq 1$. There are finitely many minimal primes in A. Pick an x_1 that lies in $\mathfrak{m}$ but not in any of the minimal primes. It follows from the choice of x_1 that any prime ideal containing x_1 must have height at least 1. Let the sequence $x_1, \ldots, x_i$ have been constructed. Thus, any prime ideal containing $(x_1, \ldots, x_i)$ has height at least i. Let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ be the set of height i prime ideals containing $(x_1, \ldots, x_i)$. Note that these would be minimal over $x_1, \ldots, x_i$ and hence, are finitely many. Usig prime avoidance, pick an $x_{i+1} \in \mathfrak{m} \backslash \bigcup_{j=1}^r \mathfrak{p}_r$. It is not hard to argue that any prime containing $(x_1, \ldots, x_{i+1})$ must have height at least $i + 1$.

Finally, let $\mathfrak{a} = (x_1, \ldots, x_d)$. Then, any prime containing $\mathfrak{a}$ must have height at least d and hence, must be maximal. As a result, there is a unique minimal prime belonging to $\mathfrak{a}$, namely $\mathfrak{m}$, whence $\mathfrak{a}$ is $\mathfrak{m}$-primary. This completes the proof. ■

Putting everything together, we have the following theorem:

Theorem 9.14 (Dimension Theorem). *For any notherian local ring* A*, the following integers are equal:*

(a) $\dim A$*.*

(b) the degree of the characteristic polynomial $\chi_{\mathfrak{m}}$*.*

(c) the least number of generators of an $\mathfrak{m}$*-primary ideal of* A*.*

Corollary 9.15. $\dim A \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2)$ where $k = A/\mathfrak{m}$ is the residue field.

Proof. There are $x_1, \ldots, x_s \in \mathfrak{m}$ generating it such that their images in $\mathfrak{m}/\mathfrak{m}^2$ form a k-basis. Thus,

$$\dim A = \delta(A) \leq s = \dim_k(\mathfrak{m}/\mathfrak{m}^2).$$ ■

Corollary 9.16 (Krull's Hauptidealsatz). Let A be a noethering and $\mathfrak{p} \trianglelefteq A$ a prime ideal. Then, the following are equivalent:

(a) $\operatorname{ht}(\mathfrak{p}) \leq n$.

(b) There is an ideal $\mathfrak{a} \trianglelefteq A$, generated by n elements, such that $\mathfrak{p}$ is a minimal prime belonging to $\mathfrak{a}$.

Proof. $\Longleftarrow$ Let $\mathfrak{a} = (x_1, \ldots, x_n)$. In $A_\mathfrak{p}$, the ideal $\mathfrak{a}A_\mathfrak{p}$ is $\mathfrak{p}A_\mathfrak{p}$-primary, since its radical is $\mathfrak{p}A_\mathfrak{p}$, which is a maximal ideal.

$\Longrightarrow$ We have $\dim A_\mathfrak{p} \leq n$ and thus, there is a $\mathfrak{p}A_\mathfrak{p}$-primary ideal $\mathfrak{b}$ of $A_\mathfrak{p}$ generated by n elements. Let $\mathfrak{a}$ denote the contraction of $\mathfrak{b}$ in A. Then, $\mathfrak{a}$ is generated by n elements and is contained in $\mathfrak{p}$. Moreover, $\mathfrak{p}$ must be the minimal prime containing $\mathfrak{a}$ due to the order preserving bijection between the primes contained in $\mathfrak{p}$ and $\operatorname{Spec}(A_\mathfrak{p})$. This completes the proof. ■

As an application, we have the following attractive result, taken from Hartshorne's Algebraic Geometry.

Proposition 9.17. *Let A be a noetherian domain. Then, A is a UFD if and only if every height 1 prime in A is principal.*

Proof. The forward direction is trivial and does not require the noetherian hypothesis. Conversely, note that every noetherian domain is a factorization domain and hence, it suffices to show that all irreducibles in A are prime. Let $f \in A$ be an irreducible and $\mathfrak{p} \in \operatorname{Spec}(A)$ be a minimal prime containing f. Due to Corollary 9.16, $\operatorname{ht}(\mathfrak{p}) \leq 1$ and hence, is equal to 1, whence, is principal, say $\mathfrak{p} = (x)$. Then, $f = xy$ for some $y \in A$. Since f is irreducible, we must have $(f) = \mathfrak{p}$, consequently, f is prime. This completes the proof. ■

9.3 Dimension Theory of Polynomial Algebras

This section has been taken from [Ser12].

Lemma 9.18. *Let $B = A[x]$, $\mathfrak{p} \subseteq A$ a prime ideal and $\mathfrak{q} \subseteq \mathfrak{q}'$ two prime ideals in B lying over A such that $\mathfrak{q} \subsetneq \mathfrak{q}'$. Then, $\mathfrak{q} = \mathfrak{p}B$.*

Proof. Note that $B/\mathfrak{p}B \cong (A/\mathfrak{p})[x]$, and both the primes $\mathfrak{q}$ and $\mathfrak{q}'$ must contain $\mathfrak{p}B$. Therefore, upon quotienting out by $\mathfrak{p}B$, we have reduced to the case of A being an integral domain and $\mathfrak{p} = (0)$.

Now, localize at $S = A \backslash \{0\}$ to reduce to the case of A being a field and $\mathfrak{p} = (0)$. Note that $\mathfrak{q}' \cap S = \varnothing$ therefore, they extend to prime ideals in $S^{-1}B \cong (S^{-1}A)[x]$. But this is obvious, since any non-zero prime ideal in $A[x]$ is maximal, owing to it being a PID. This completes the proof. ■

Theorem 9.19. *If $B = A[x]$, then*

$$\dim A + 1 \leq \dim B \leq 2 \dim A + 1.$$

Lemma 9.20. *Let $B = A[x]$ and $\mathfrak{a} \trianglelefteq A$. Let $\mathfrak{p} \trianglelefteq A$ be a minimal prime ideal containing $\mathfrak{a}$. Then, $\mathfrak{p}B$ is a minimal prime ideal containing $\mathfrak{a}B$ in B.*

Proof. Suppose $\mathfrak{p}B$ were not minimal among the primes containing $\mathfrak{a}B$. Then, there is some prime $\mathfrak{q}$ with $\mathfrak{a}B \subseteq \mathfrak{q} \subsetneq \mathfrak{p}B$. Note that $\mathfrak{q} \cap A$ is a prime ideal in A containing $\mathfrak{a}$ and is contained in $\mathfrak{p}$, therefore, $\mathfrak{q} \cap A = \mathfrak{p}$. Consequently, due to Lemma 9.18, $\mathfrak{q} = \mathfrak{p}B$, a contradiction. ■

Proposition 9.21. *Let A be a noethering and $\mathfrak{p} \trianglelefteq A$ a prime ideal. If $B = A[x]$, then $\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\mathfrak{p}B)$.*

Proof. Let $n = \operatorname{ht}(\mathfrak{p})$. Then, there is a strictly ascending chain $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ of prime ideals in A. Then, $\mathfrak{p}_0 B \subseteq \mathfrak{p}_1 B \subsetneq \cdots \subsetneq \mathfrak{p}_n B$ is a strictly ascending chain of prime ideals in B. Hence, $\operatorname{ht}(\mathfrak{p}B) \geq n$.

Conversely, there is an ideal $\mathfrak{a}$ generated by n elements, contained in $\mathfrak{p}$ such that $\mathfrak{p}$ is minimal among the primes containing $\mathfrak{a}$. Then, $\mathfrak{a}B \subseteq \mathfrak{p}B$, $\mathfrak{a}B$ is generated by n elements and due to Lemma 9.20 and Corollary 9.16, $\operatorname{ht}(\mathfrak{p}B) \leq n$. ■

Theorem 9.22. *Let A be a noethering. Then,*

$$\dim(A[x_1, \ldots, x_n]) = \dim A + n.$$

Proof. It suffices to prove the theorem for $n = 1$. Let $B = A[x]$. We know that $\dim(B) \geq \dim A + 1$. We shall show that $\dim(B) \leq \dim A + 1$. Let $\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_r$ be a strictly ascending chain of prime ideals in B. Define $\mathfrak{p}_i = \mathfrak{q}_i \cap A$ for $0 \leq i \leq r$. If all the $\mathfrak{p}_i$'s are distinct, then $r \leq \dim A$.

Suppose now that the $\mathfrak{p}_i$'s are not distinct. Let j be the maximum index such that $\mathfrak{p}_j = \mathfrak{p}_{j+1}$. Then, $\mathfrak{q}_j = \mathfrak{p}_j B$. Due to Proposition 9.21, $\mathrm{ht}(\mathfrak{p}_j) = \mathrm{ht}(\mathfrak{p}_j B) = \mathrm{ht}(\mathfrak{q}_j)$. Now, note that $\mathfrak{p}_{j+1} \subsetneq \cdots \subsetneq \mathfrak{p}_r$. Hence,

$$\dim A \geq r - (j+1) + \mathrm{ht}(\mathfrak{p}_j) = r - (j+1) + \mathrm{ht}(\mathfrak{q}_j) \geq r - 1 \implies r \leq \dim A + 1.$$

This completes the proof. ■

Corollary 9.23. Let k be a field. Then, $\dim(k[x_1, \ldots, x_n]) = n$.

9.4 Dimension of a Variety

9.5 Dimension Theory of Affine k-Algebras

Theorem 9.24. *Let A be an affine k-domain. Then,* $\dim(A) = \mathrm{trdeg}_k(Q(A))$.

Proof. Follows from the Going Up Theorem and Noether's Normalization Lemma. ■

Theorem 9.25. *Let A be an affine k-domain and $\mathfrak{p} \in \mathrm{Spec}(A)$. Then,*

$$\dim(A) = \dim(A/\mathfrak{p}) + \mathrm{ht}(\mathfrak{p})$$

Proof. Using Noether's Normalization Lemma, there is a polynomial algebra $B = k[y_1, \ldots, y_n] \subseteq A$ such that A/B is an integral extension. Hence, $\dim(A) = \dim(B)$. Let $\mathfrak{q} = \mathfrak{p} \cap B$. Due to the Going Down Theorem, $\mathrm{ht}(\mathfrak{q}) = \mathrm{ht}(\mathfrak{p})$. Further, $A/\mathfrak{p}$ is integral over $B/\mathfrak{q}$ whence it suffices to prove the theorem for polynoimal algebras $A = k[x_1, \ldots, x_n]$. We shall do so by induction on $\mathrm{ht}(\mathfrak{p})$.

Claim. If $\mathfrak{p} \subseteq A = k[y_1, \ldots, y_n]$ is a height 1 prime, then $\dim(A/\mathfrak{p}) = \dim(A) - 1$.

Let $a \in \mathfrak{p}$ be a non-zero element. This admits a unique factorization in terms of irreducibles $a = f_1 \cdots f_r$. Hence, there is an $f_i \in \mathfrak{p}$. Since (f_i) is a non-zero prime ideal, we must have $\mathfrak{p} = (f_i)$. Since f_i is non-zero, it contains at least one monomial. Suppose, without loss of generality that y_n occurs in this monomial.

$$f_i(y_1, \ldots, y_n) = \sum_{j=0}^{d} g_j(y_1, \ldots, y_{n-1}) y_n^j$$

where $g_j \in k[y_1, \ldots, y_{n-1}]$ with at least one of the g_j's being non-zero.

Note that $\overline{y}_1, \ldots, \overline{y}_{n-1} \in A/\mathfrak{p}$ are algebraically independent. This is easy to see by examining the degree of y_n. But, we also see that $\overline{y}_n \in Q(A/\mathfrak{p})$ is algebraic over $k[\overline{y}_1, \ldots, \overline{y}_{n-1}]$ and hence, $\mathrm{trdeg}_k(Q(A/\mathfrak{p})) = n - 1$, whence, $\dim(A/\mathfrak{p}) = n - 1 = \dim(A) - 1$. □

From the Claim, we see that the theorem is true for all height 1 primes. We shall now induct on $\mathrm{ht}(p)$. Let $r = \mathrm{ht}(\mathfrak{p})$. Then, there is a chain $(0) \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r = \mathfrak{p}$. Set $B = A/\mathfrak{p}_1$. Then, $\dim(B) = \dim(A) - 1$ and $\mathrm{ht}(\mathfrak{p}/\mathfrak{p}_1) = r - 1$ and the induction hypothesis applies to obtain

$$\dim(A) - 1 = \dim(B) = \dim(A/\mathfrak{p}) + \mathrm{ht}(\mathfrak{p}/\mathfrak{p}_1) = \dim(A/\mathfrak{p}) + \mathrm{ht}(\mathfrak{p}) - 1.$$

This completes the proof. ■

Proposition 9.26. *Let A be an affine k-domain with* $\dim A = d$*. Then, every saturated, maximal chain* $(0) = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ *has length d.*

Proof. We shall prove this by induction on d. The base case with $d = 0$ is trivial. Now, let $B = A/\mathfrak{p}_1$. Then, $\dim B = d - 1$ and $(0) = \bar{\mathfrak{p}}_1 \subsetneq \cdots \subsetneq \bar{\mathfrak{p}}_n$ is a saturated, maximal chain and hence, has length $d - 1$. The conclusion follows. ■

Theorem 9.27. *Let A be an affine k-algebra. Then, given any two prime ideals $\mathfrak{p} \subseteq \mathfrak{q}$ in A, every saturated chain of prime ideals from $\mathfrak{p}$ to $\mathfrak{q}$ has the same length.*

Proof. Let $\mathfrak{p} = \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r = \mathfrak{q}$ be a saturated chain. There are surjections

$$A/\mathfrak{p} = A/\mathfrak{p}_0 \twoheadrightarrow A/\mathfrak{p}_1 \twoheadrightarrow \ldots \twoheadrightarrow A/\mathfrak{p}_r = A/\mathfrak{q}.$$

And, $\dim(A/\mathfrak{p}_{i+1}) = \dim(A/\mathfrak{p}_i) - 1$. Consequently, $\dim(A/\mathfrak{q}) = \dim(A/\mathfrak{p}) - r$. This means

$$r = \dim(A/\mathfrak{p}) - \dim(A/\mathfrak{q}) = \operatorname{ht}(\mathfrak{q}) - \operatorname{ht}(\mathfrak{p}).$$

This completes the proof. ■

Corollary 9.28. Let A be an affine k-domain with $\dim A = d$. Then, $\operatorname{ht}(\mathfrak{m}) = d$ for every maximal ideal $\mathfrak{m} \subsetneq A$.

9.6 Dimension Theory of Power Series Algebras

Lemma 9.29. *A maximal ideal in $A[\![x]\!]$ is of the form $(\mathfrak{m}, x)$ where $\mathfrak{m}$ is a maximal ideal in A.*

Proof. ■

Theorem 9.30. *Let A be a noethering. Then,* $\dim A[\![x]\!] = \dim A + 1$*.*

Proof. Let $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ be a chain of primes in A. Then,

$$\mathfrak{p}_0[\![x]\!] \subsetneq \cdots \subsetneq \mathfrak{p}_n[\![x]\!] \subseteq \mathfrak{p}_n[\![x]\!] + (x)$$

is a chain of prime ideals in $A[\![x]\!]$. Hence, $\dim A[\![x]\!] \geq \dim A + 1$.

Conversely, let $\mathfrak{M}$ be a maximal ideal in $A[\![x]\!]$. Then, $\mathfrak{M} = (\mathfrak{m}, x)$ where $\mathfrak{m}$ is a maximal ideal in A. Let $n = \operatorname{ht}\mathfrak{m}$, then there are elements $a_1, \ldots, a_n \in A$ such that $\mathfrak{m}$ is minimal over $(a_1, \ldots, a_n)$. Consequently, $\mathfrak{m} + (x)$ is minimal over $(a_1, \ldots, a_n, x)$ in $A[\![x]\!]$. Hence, $\operatorname{ht}\mathfrak{M} \leq n + 1 \leq \dim A + 1$. The conclusion follows. ■

Remark 9.6.1. *The above result also follows from the fact that completions preserve dimension but that requires a significant amount of machinery.*

Bibliography

[AM69] Michael Atiyah and Ian MacDonald. *Introduction to Commutative Algebra*. CRC Press, 1969.

[Gop84] N.S. Gopalakrishnan. *Commutative Algebra*. Oxonian Press, 1984.

[Lan02] Serge Lang. *Algebra*. Springer Science & Business Media, 2002.

[Mil20] J. S. Milne. *Algebraic Number Theory*. 2020.

[Ser12] Jean-Pierre Serre. *Local Algebra*. Springer Science & Business Media, 2012.