Commutative Algebra

Swayam Chube

June 24, 2023

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.

Contents

Part I

Theory Building

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 $1 \leq i \leq n$.*

(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. 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 1.15. *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 1.16. 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 1.17. *(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 1.18 (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

$$\text{m-spec}\, A = \{\mathfrak{m} \mid \mathfrak{m} \text{ is a maximal ideal in } A\}$$

For each $E \subseteq A$, define

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

Proposition 1.19. *(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 1.20. *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 1.21. *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 1.22. $\operatorname{spec} A$ *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. If spec A is T_1, then spec A is Hasudorff.

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 $\mu : R \to \mathrm{End}(M)$. Similarly, a right R-module is an abelian group $(M, +)$ along with a ring homomorphism $\mu : R^{\mathrm{op}} \to \mathrm{End}(M)$ 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:

$$\begin{tikzcd}
S \arrow[r, "g"] \arrow[d, "f"'] & M \\
F \arrow[ur, dotted, "\exists! h"'] &
\end{tikzcd}$$

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 $H \le F$ is a submodule, then H is free and* $\dim H \le \dim F$.

Proof. Let $\{e_i\}_{i\in I}$ be a basis for F. Denote the projection map of the i-th coordinate by $p_i : F \to R$. Due to the Well Ordering Theorem, we can impose a well order $(I, \leqq)$ on I. Let F_i be the submodule generated by $\{e_j \mid j \leqq i\}$ and $H_i = H \cap F_i$. Now, $p_i(H_i)$ is an ideal in R, and therefore, is of the form $a_i R$ for some $a_i \in R$. Of course, it is possible that $a_i = 0$. If $a_i \neq 0$, then pick some $h_i \in H_i$ such that $p_i(h_i) = a_i$, on the other hand, if $a_i = 0$, then set $h_i = 0$. It is not hard to see from this definition that $p_i(h_j) = 0$ whenever $j < i$.

We contend that the set $S = \{h_i \neq 0 \mid i \in I\}$ forms a basis for H, this would immediately imply that $\dim H \le \dim F$. First, we shall show that S is linearly independent. We shall do this by transfinite induction. The base case is trivial. Suppose the induction hypothsis holds for $S_i = \{h_j \in S \mid j < i\}$. If a linear combination of the elements of S_{i+1} is zero, then the coefficient of h_i must be nonzero. Therefore, we may write

$$bh_i = \sum_{k=1}^{n} a_{j_k} h_{j_k}$$

For some $a_{j_1}, \ldots, a_{j_n}, b \in R$. Upon projecting using p_i, we obtain $ba_i = 0$, consequently, $b = 0$, and S_{i+1} is linearly independent.

It is not hard to argue that the h_i's span H. Pick some $h \in H$. Note that only finitely many of the $p_i(h)$'s will be nonzero. Let them be $i_1 < \cdots < i_n$. Now work backwards from i_n to determine the coefficients of h_{i_k} for each $1 \le k \le n$. ■

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 $1 \le i \le n$, 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 $(\phi\delta_{ij} - a_{ij})_{1 \le i,j \le n}$. Then, multiplying by $\operatorname{adj}(B)$, we see that $\det(B)(x_j) = 0$ for all $1 \le j \le n$ 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. ■

Lemma 2.16 (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. 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 2.16. ■

Lemma 2.17. *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 $M = N$. ■

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 $\mathrm{Hom}_R(M, N)$. When the choice of the ring R is clear from the context, we shall denote this set by $\mathrm{Hom}(M, N)$.

Proposition 2.18. *Let M, N be A-modules. Then $\mathrm{Hom}(M, N)$ has the structure of an A-module.*

Proof. It is obvious that $\mathrm{Hom}(M, N)$ 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 2.19. *Let $\{M_\lambda\}_{\lambda\in\Lambda}$ be a collection of A-modules. Then, for any A-module N, we have a natural isomorphism*

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

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

Theorem 2.20. *Let $\phi : M \to N$ be an A-module homomorphism. Then, for every R-module P, there is an induced A-module homomorphism $\overline{\phi} : \mathrm{Hom}(N, P) \to \mathrm{Hom}(M, P)$ and an induced A-module homomorphism $\widetilde{\phi} : \mathrm{Hom}(P, M) \to \mathrm{Hom}(P, N)$.*

Equivalently phrased, $\mathrm{Hom}(-, P)$ is a contravariant functor while $\mathrm{Hom}(P, -)$ 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:

$$\begin{tikzcd}
M \arrow[r, "\phi"] \arrow[dr, dotted, "f\circ\phi"'] & N \arrow[d, "f"] \\
 & P
\end{tikzcd}$$

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

Theorem 2.21. *$\mathrm{Hom}(M, -)$ is a left exact functor.*

Proof. Let $0 \to N' \overset{f}{\to} N \overset{g}{\to} N''$ 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 $\mathrm{im}\,\overline{f} = \ker \overline{g}$. 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 2.22. 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 2.23 (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.

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\iota"] \arrow[d, "\mathbf{id}_A"'] & B \arrow[r, "\pi"] \arrow[d, dotted, "\Phi"] & C \arrow[r] \arrow[d, "\mathbf{id}_C"] & 0 \\
0 \arrow[r] & A \arrow[r] & A \oplus C \arrow[r] & C \arrow[r] & 0
\end{tikzcd}$$

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 2.24 (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:

$$\begin{tikzcd}
M \times N \arrow[r, "f"] \arrow[d, "g"'] & P_1 \arrow[dl, dotted, "\phi"] \\
P_2 &
\end{tikzcd}$$

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 2.25 (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:

$$\begin{tikzcd}
M \times N \arrow[r, "T"] \arrow[d, "\varphi"'] & P \\
M \otimes_A N \arrow[ru, dotted, "\exists!\phi"']
\end{tikzcd}$$

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:

$$\begin{tikzcd}
M \times N \arrow[r, "T"] \arrow[d, hook, "\iota"'] & P \\
F \arrow[r, "\pi"'] \arrow[ru, dotted, "\exists!f"] & G \arrow[u, dotted, "\exists!\phi"']
\end{tikzcd}$$

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:

$$\begin{tikzcd}
M_1 \times \cdots \times M_n \arrow[r, "T"] \arrow[d, "\varphi"'] & P \\
M_1 \otimes \cdots \otimes M_n \arrow[ru, dotted, "\exists!\phi"']
\end{tikzcd}$$

Proposition 2.26. *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 2.27. *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:

$$\begin{tikzcd} M \times N \arrow[r, "T"] \arrow[d, "\varphi"'] & N \times M \arrow[d, "\varphi'"] \\ M \otimes N & N \otimes M \end{tikzcd}$$

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:

$$\begin{tikzcd}
A \times M \arrow[r, "T"] \arrow[d, "\varphi"'] & M \\
A \otimes M \arrow[ur, dotted, "f"'] &
\end{tikzcd}$$

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 2.28. 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 2.29. *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 2.30. *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 2.29, 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.

2.8 Flat Modules

Definition 2.31 (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 2.32. *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 2.33. *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. 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. ■

2.9 Projective Modules

Theorem 2.34. *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:

$$\begin{tikzcd}
& P \arrow[dl, "\widetilde{f}"'] \arrow[d, "f"] & \\
M \arrow[r, "g"'] & M'' \arrow[r, two heads] & 0
\end{tikzcd}$$

(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 $\operatorname{Hom}_A(A, M) \xrightarrow{\sim} M$, consequently, there is a natural isomorphism

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

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 2.35 (Projective Module). An A-module P satisfying any one of the four equivalent conditions of Theorem 2.34 is said to be a *projective A-module*.

In particular, from Theorem 2.34(c), we see that every free module is projective.

Lemma 2.36. *A finitely generated projective module P over a local ring $(A, \mathfrak{m})$ is free.*

Proof. Let $\{\overline{x}_1, \ldots, \overline{x}_n\}$ be a basis for $M/\mathfrak{m}M$ as a k-vector space where $k = A/\mathfrak{m}$. As we have seen earlier, $\{x_1, \ldots, x_n\}$ generates M. Let F be the free module with basis $\{e_1, \ldots, e_n\}$ 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 $\{r_1, \ldots, r_n\}$. 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 2.16, we must have that $K = 0$ whence M is free. ■

Proposition 2.37. *Projective modules are flat.*

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

2.10 Injective Modules

Theorem 2.38 (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. $(\implies)$ Trivial.

$(\impliedby)$ 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 $M \leq M' \leq N$ 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 $M \leq M' \leq N$. If $M' \neq N$, 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 2.39. *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 Algebras

Definition 2.40. 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.

$$\begin{tikzcd}
A \arrow[r, "\phi_1"] \arrow[d, "\phi_2"'] & B_2 \\
B_1 \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

This gives rise to a locally small category $A - \mathbf{Alg}$ 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 $A[x_1, \ldots, x_n]$ for some positive integer n.

Proposition 2.41. *If C is a finite B-algebra and B is a finite A-algebra, then C is a finite A-algebra.*

Proposition 2.42. *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. ■

2.11.1 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,

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

2.12 Structure Theorem for Modules over a PID

Throughout this section, let R be a PID.

Lemma 2.43. *A finitely generated torsion free R-module is free.*

Proof. ■

Definition 2.44. Let E be an R-module. For $x \in E$, an element $r \in R$ such that $\mathrm{Ann}_R(x) = (r)$ 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 2.12.1. *In order to show that $x_1, \ldots, x_n$ are independent, it suffices to show that given any linear combination $a_1x_1 + \cdots + a_nx_n = 0$, we must have $a_ix_i = 0$ 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 2.45 (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, $\mathrm{Ann}(\overline{y}) \supseteq \mathrm{Ann}(\overline{E}) \supseteq (p^r)$ whereby, $\mathrm{Ann}(y) = (p^n)$ for some $n \leq r$. Thus, $p^ny \in (x_1)$ whence there is $p^sc \in R$ with $p \nmid c$ such that $p^ny = p^scx_1$. Now, p^scx_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 $z = y - p^{s-n}cx_1$. 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

$$ax_1 + a_1y_1 + \cdots + a_my_m = 0$$

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 $a_iy_i = 0$ and thus $ax_1 = 0$, 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 $\alpha = up_1^{t_1} \cdots p_r^{t_r}$ where $u \in R^\times$.

Lemma 2.46.

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

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 2.45, 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.

2.12.1 The Jordan Canonical Form

Let k be an algebraically closed field

2.13 Finitely Presented Modules

I need to place this section somewhere nice.

Definition 2.47 (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 2.48. *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.

$$\begin{tikzcd}
0 \arrow[r] \arrow[d] & S^{-1}\operatorname{Hom}_A(M,N) \arrow[r] \arrow[d] & S^{-1}\operatorname{Hom}_A(A^n,N) \arrow[r] \arrow[d, "\sim"'] & S^{-1}\operatorname{Hom}_A(A^m,N) \arrow[d, "\sim"'] \\
0 \arrow[r] & \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N) \arrow[r] & \operatorname{Hom}_{S^{-1}A}(S^{-1}A^n, S^{-1}N) \arrow[r] & \operatorname{Hom}_{S^{-1}A}(S^{-1}A^m, S^{-1}N)
\end{tikzcd}$$

■

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 multiplica-*

tively 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 $\phi : \prod_{i\in I}(S_i^{-1}A_i) \to (\prod_{i\in I} S_i)^{-1}(\prod_{i\in I} A_i)$ 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. 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.

$$\begin{tikzcd}
A \arrow[r, "\psi"] \arrow[d, "\phi"'] & C \\
B \arrow[ur, "f"'] &
\end{tikzcd}$$

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 3.4. *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*

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\varphi"'] & B \\
S^{-1}A \arrow[ur, dotted, "\exists! g"'] &
\end{tikzcd}$$

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 3.5. $S^{-1} : A - \mathbf{Mod} \to S^{-1}A - \mathbf{Mod}$ *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, $\operatorname{im}(S^{-1}f) \subseteq \ker(S^{-1}g)$. 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, $\ker(S^{-1}g) \subseteq \operatorname{im}(S^{-1}f)$. This completes the proof. ■

Proposition 3.6. *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 3.5, 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 3.5, 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 3.5, 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 3.7. *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. For every multiplicative subset $S \subseteq A$, $S^{-1}A$ is a flat A-module.

Proposition 3.8. *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. ■

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 3.9. *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* $\mathfrak{m} \in \text{m-spec } A$

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 3.10. *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 3.11. *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* $\mathfrak{p} \in \text{m-spec } A$

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.

$(c) \implies (a)$. ■

Proposition 3.12. *"Being an integral domain" is* <u>*not*</u> *a local property. Similarly, "being noetherian" is* <u>*not*</u> *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.

As for the second assertion, consider the ring $R = k \times k \times \cdots$ where k is a nonzero field. This is obviously not noetherian due to the following ascending chain of ideals:

$$(0) \times (0) \times \cdots \subsetneq k \times (0) \times \cdots \subsetneq \cdots$$

But due to Proposition 3.3, every localization is isomorphic to k, consequently, is noetherian. ■

3.4 Extension and Contraction of Ideals

Definition 3.13. 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 3.14. *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 3.15. *The operation S^{-1} on ideals of A commutes with formation of finite sums, products, intersections and radicals.*

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

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

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

Proposition 3.16. *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

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

■

Chapter 4

Primary Decomposition

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. ■

Lemma 4.4. *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 $1 \le i \le n$ and the conclusion follows. ■

Lemma 4.5. *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 4.6 (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 $1 \le i \le n$, $\sqrt{\mathfrak{q}_i}$ 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 4.4, it is not hard to see that every decomposable ideal has a minimal decomposition.

Theorem 4.7 (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 4.8. *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 4.9. *Let S be a multiiplicatively 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 4.10 (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 4.11 (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 $S = A \setminus \bigcup_{j=1}^{m} \mathfrak{p}_{i_j}$. 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. In particular, the primary ideals which correspond to the minimal primes associated to $\mathfrak{a}$ are uniquely determined.

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. ■

In particular, from Theorem 5.2(c), we note that any element in a finite A-algebra is integral over A.

Proposition 5.3. *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.*

Proof. Denote by A_k the subring $A[x_1, \ldots, x_k]$. We have that A_{k+1} is a finitely generated A_k-algebra, whereby A_n is a finitely generated A-algebra, thereby completing the proof. ■

Corollary. 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 5.4. *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. 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 5.5. *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 5.6. *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. ■

Proposition 5.7. *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 5.5, $B/\mathfrak{q}$ is integral over a copy of $A/\mathfrak{p}$. The conclusion now follows from the above proposition. ■

Proposition 5.8. *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 3.6.

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 5.9. *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 5.10. 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 5.11. *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 5.12. *Let A be an integral domain and $S \subsetneq A$ 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 5.11, we see that $S^{-1}A$ is the integral closure of $S^{-1}A$ in $S^{-1}K = K$. This completes the proof. ■

Proposition 5.13. *Let A be an integral domain. Then, the following are equivalent:*

1. *A is normal*
2. *$A_{\mathfrak{p}}$ is normal for all $\mathfrak{p} \in \operatorname{spec} A$*
3. *$A_{\mathfrak{m}}$ is normal for all $\mathfrak{m} \in \operatorname{m-spec} A$*

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 5.14. *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 $A \hookrightarrow C$.*

Proposition 5.15. *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 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 $\sqrt{\mathfrak{a}}$.*

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. A ring A is noetherian if and only if every ideal is finitely generated.

Corollary. Every submoule of a noetherian A-module is noetherian.

Proposition 6.4. *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 6.5 (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. 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 6.6. *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 6.7. *Let A be a noetherian (resp. artinian) ring and M a finitely generated A-module. Then, M is noetherian (resp. artinian).*

Proof. Let $\{m_1, \dots, m_n\}$ be a set of generators of M. Then, there is a surjection $A^n \twoheadrightarrow M$ given by

$$(a_1, \dots, a_n) \mapsto a_1 m_1 + \cdots + a_n m_n.$$

Since A^n is a noetherian (resp. artinian) A-module, so is M. ■

Proposition 6.8. *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 6.9. *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 6.5, we are done. ■

6.2 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 $R = k[x_1, x_2, \ldots]/(x_1, x_2^2, \ldots)$. 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 $(x_1, x_2^2, \ldots)$ and thus contains its radical, $(x_1, x_2, \ldots)$. 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 $(x_1, x_2, \ldots)$.

Lemma 6.10. *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 6.11. *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 $\{x_1, \ldots, x_n\}$, whereby I is generated by the set $\{x_1/1, \ldots, x_n/1\}$. 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.

[1] Nagata is to blame for this monster

Lemma 6.12. *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 $1 \leq i \leq n$, 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 6.13 (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

$$\begin{aligned} f_1 &= a_1 x^{d_1} + \text{lower degree terms} \\ f_2 &= a_2 x^{d_2} + \text{lower degree terms} \\ &\vdots \\ f_n &= a_n x^{d_n} + \text{lower degree terms} \\ &\vdots \end{aligned}$$

with $d_1 \leq d_2 \leq \cdots$. 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 $\deg g \leq \deg f_{n+1}$, a contradiction. This completes the proof. ∎

An analogous theorem, with an analogous proof is true wherein $A[x]$ is replaced by $A[\![x]\!]$.

Corollary. For a field k, the polynomial ring $k[x_1, \dots, x_n]$ in finitely many indeterminates is noetherian.

Corollary. 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

$$k[xy, xy^2, \ldots] \subsetneq k[x, y]$$

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 6.14. *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 $\{m_1, \ldots, m_n\}$ 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 $\phi(a) = (am_1, \ldots, am_n)$. 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 $M = \boldsymbol{\mu}[p^\infty]$ 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 6.15 (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. ■

Lemma 6.16 (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 $\{r_1, \dots, r_n\}$ and thus there would exist $\mathfrak{a} \in \mathscr{C}$ containing $\{r_1, \dots, r_n\}$ 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 $1 \leq i \leq n$ 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 $(\mathfrak{p} : x) = (x_1, \dots, x_m)$ for some positive integer m. Let $\mathfrak{a} = (p_1, \dots, p_n, xx_1, \dots, xx_m)$. 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 $b_1, \dots, b_n, c \in A$, 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 6.17. *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 $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ and $\mathfrak{q}_1, \dots, \mathfrak{q}_m$ 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. ■

6.2.1 Primary Decomposition

Definition 6.18 (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 6.19. *In a noethering, every ideal can be expressed as a finite intersection of irreducible ideals.*

[2] This does not require Zorn, since we are in a noethering

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 6.20. *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

$$\operatorname{Ann}(y) \subseteq \operatorname{Ann}(y^2) \subseteq \cdots$$

Since $A/\mathfrak{q}$ is a noethering, there is a positive integer n such that $\operatorname{Ann}(y^n) = \operatorname{Ann}(y^{n+1})$. 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 $v \in \operatorname{Ann}(y^{n+1}) = \operatorname{Ann}(y^n)$, 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. 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 6.17. Let $\mathfrak{a} \subsetneq A$ 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 6.21. *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 $\mathfrak{a} \subseteq A$ 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 4.11, the $\mathfrak{q}_i$'s are unique. ■

6.3 Artinian Rings

Recall that A is artinian if it is an artinian module over itself.

Proposition 6.22. *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 6.23. *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. Let A be an artinian ring. Then $\mathfrak{N}(A) = \mathfrak{R}(A)$.

Lemma 6.24. *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 6.25. *A is artinian if and only if it is a noethering with krull dimension zero.*

Proof. ($\implies$). 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

$$\mathfrak{N}(A) = \mathfrak{m}_1 \cdots \mathfrak{m}_n$$

[3] We have not invoked Zorn to conclude this.

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 6.9, 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 6.9. ■

Theorem 6.26 (Structure Theorem of Artinian Rings). *Let A be an artinian ring. Then, there are artinian local rings $A_1, \dots, A_n$ such that $A \cong A_1 \oplus \cdots \oplus A_n$. Further, the A_i's are unique up to isomorphism.*

Proof. ■

Lemma 6.27.

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 valuation ring. Then the ideals in A are totally ordered.*

Proof. 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. 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, $\mathfrak{a} \subseteq \mathfrak{m}_k$. 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

$$\mathfrak{m} = \mathfrak{m}_1 \supseteq \mathfrak{m}_2 \supseteq \cdots .$$

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 2.16, 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 $\overline{\mathfrak{m}} = \mathfrak{m}/\mathfrak{m}^2$. Consequently,

$$\dim_k(\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2) = \dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$$

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 2.16, $\mathfrak{m} \supsetneq \mathfrak{m}^2$, 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 in a unique way.

(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 6.21, 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 6.27, 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 2.16.

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. Every ideal in a Dedekind domain is generated by at most two elements.

Proof. ■

Easy write up. Stop being lazy

Theorem 7.16. *The ring of integers $\mathcal{O}_K$ in an algebraic number field*[a] $K \supseteq \mathbb{Q}$ *is a Dedekind domain.*

[a] An algebraic number field is a finite field extension of $\mathbb{Q}$

Proof. ■

Read the section on valuations and then add this

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. ■

7.4 Fractional Ideals

Definition 7.18. 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 $dM \subseteq A$.

The ideals contained in A are now called "integral ideals". Obviously, every integral ideal is fractions.

- 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 7.19. 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 $MN = A$.

For an A-submodule M of K, recall that we had defined the colon operator as

$$(A : M) = \{x \in K \mid xM \subseteq A\}.$$

It is not hard to see that $(A : M)$ is an A-submodule of K.

Proposition 7.20. *Let A be an integral domain and M an invertible ideal of A. Then, $M^{-1} = (A : M)$.*

Proof. Let N denote the inverse of M. Then

$$N \subseteq (A : M) = (A : M)MN \subseteq AN = N.$$

This completes the proof. ■

Chapter 8

Completions

8.1 Completion Abelian Topological Groups

Throughout this section, let G denote a first countable abelian topological group.

Definition 8.1 (Convergence, Cauchy). A sequence $\{x_n\}_{n=1}^{\infty}$ of elements of G *converges* to $x \in G$ if for any open neighborhood U of x, there is an integer $N \in \mathbb{N}$ such that for all $n \geq N$, $x_n - x \in U$. This is denoted by $x_n \to x$. The sequence is said to be *Cauchy* if for every open neighborhood U of 0, there is an integer $N \in \mathbb{N}$ such that for all $m, n \geq N$, $x_m - x_n \in U$.

Proposition 8.2. *If $\{x_n\}$ and $\{y_n\}$ are Cauchy sequences, then so is $\{x_n + y_n\}$.*

We now define a relation on the set of all Cauchy sequences in G, given by

$$\{x_n\} \sim \{y_n\} \iff x_n - y_n \to 0$$

This relation is obviously reflexive and symmetric. We contend that this is also transitive. This follows from the following proposition.

Proposition 8.3. *If $\{x_n\} \to x$ and $\{y_n\} \to y$ in G, then $\{x_n + y_n\} \to x + y$.*

Proof. In $G \times G$, the sequence $\{(x_n, y_n)\}$ converges to (x, y) and since $\varphi : G \times G \to G$ given by $\varphi(g, h) = g + h$ is continuous, we have that $\{x_n + y_n\}$ converges to $x + y$. ■

We now denote the set of equivalence classes of Cauchy sequences in G by $\widehat{G}$. Endow $\widehat{G}$ with an addition operation given by

$$[\{x_n\}] + [\{y_n\}] = [\{x_n + y_n\}]$$

It is not hard to see that $(\widehat{G}, +)$ is an abelian group.

For each $U \subseteq G$ a neighborhood containing 0, define $\widehat{U}$ to be the set of all equivalence classes $[\{x_n\}]$ such that there is a positive integer N such that $x_n \in U$ for all $n \geq N$. This forms a basis around $[\{0\}]$ because $\widehat{U} \cap \widehat{V} = \widehat{U \cap V}$ and since $\widehat{G}$ is a topological group, it is homogeneous and this determines the topology on $\widehat{G}$.

There is also a natural map $\phi : G \to \widehat{G}$ that maps $g \in G$ to the equivalence class $[\{g\}]$. This is obviously a group homomorphism and $\ker \phi = \bigcap U$ where U ranges over all open neighborhoods of 0 in U. Therefore, ϕ is injective if and only if G is Hausdorff.

Now, suppose $f : G \to H$ is a continuous homomorphism between abelian topological groups. We contend that f maps Cauchy sequences to Cauchy sequences. Indeed, if $\{x_n\}$ is Cauchy in G and V an open neighborhood of H, let $U = f^{-1}(V)$. Then, there is a positive integer N such that for all $n \geq N$, $x_n \in U$, whereby $f(x_n) \in V$.

Therefore, f induces a map $\widehat{f} : \widehat{G} \to \widehat{H}$ given by $f([\{x_n\}]) = [\{f(x_n)\}]$. That $\widehat{f}$ is a homomorphism is obvious. We contend that $\widehat{f}$ is also a continuous map. Indeed, if $\widehat{V}$ is a basis element around 0, then $\widehat{f}^{-1}(\widehat{V}) = \widehat{f^{-1}(V)}$. Since the topology on $\widehat{H}$ is homogeneous, the map $\widehat{f}$ is continuous.

8.1.1 Completion Using Inverse Limits