Commutative Algebra

Swayam Chube

May 21, 2023

Abstract

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 $\dim A$.

1.1 Nilradical and Jacobson radical

Definition 1.2 (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 1.3. *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 1.4. A commutative ring A is said to be local if it has a unique maximal ideal.

Proposition 1.5. *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 1.6. *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 1.7. *(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 1.8. *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 1.9. *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 1.10. *Let A be a UFD. Then A is a PID if and only if* $\dim A \leq 1$.

1.3.1 Radical Ideals

Definition 1.11 (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 1.12. *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) $\sqrt{\mathfrak{a} + \mathfrak{b}} = \sqrt{\sqrt{a} + \sqrt{b}}$

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.

∎

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.

1.4 The Zariski Topology

Definition 1.13 (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 1.14. *(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 1.15. *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 1.16. *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**.

1.4.1 On the Topological Properties

Proposition 1.17. $\operatorname{spec} A$ *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.

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 $\mu : R \to \text{End}(M)$.

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*.

Definition 2.2 (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 2.3 (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 2.4 (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 2.5 (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 2.6 (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

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

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

Proposition 2.7. *If I is an ideal contained in $\mathrm{Ann}_A(M)$, 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. ■

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 2.8 (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 2.9 (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 2.10. *Let F be a free R-module. If $H \leq F$ is a submodule, then H is free and* $\dim H \leq \dim F$.

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 $\dim H \leq \dim F$. 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 $1 \leq k \leq n$. ∎

2.3 Finitely Generated Modules

Definition 2.11 (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 2.12. *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 $(r_1, \ldots, r_n) \mapsto r_1 x_1 + \cdots + r_n x_n$. From the first isomorphism theorem, we have $M \cong R^{\oplus n} / \ker \phi$. ∎

Proposition 2.13. *Let M be a finitely generated A-module and $\mathfrak{a}$ an ideal of A. Let $\phi \in \mathrm{End}(M)$ 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 $\mathrm{End}(M)$*, where a_k is treated as the homomorphism $x \mapsto a_k x$ in* $\mathrm{End}(M)$*.*

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

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

We may rewrite this as

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

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

Lemma 2.14 (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 $\mathrm{End}(M)$. Using Proposition 2.13, 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 2.14. ∎

Lemma 2.15. *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 2.16. *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 2.17. *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 product in $A - \mathbf{Mod}$, the conclusion follows from the universal property. ■

Theorem 2.18. *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. ■

2.5 Exact Sequences

Definition 2.19. 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

2.6 Tensor Product

Definition 2.20 (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 2.21 (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:

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

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:

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

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:

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

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 2.22. *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) Define the map $f : (\bigoplus_{ß \in I} M_i) \times N \to \bigoplus(M_i \otimes_A N)$ 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

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

(c)

(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 1. 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 $M \otimes N$.

2.7 Right Exactness

Proposition 2.23. *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 2.24. *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 2.23, 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 2.25 (Flat Module). An A-module M is sida 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 2.26. *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 2.27. *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 2.28. *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 $\mathrm{Hom}_A(P, -)$ is exact.*

Proof.

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

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

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

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

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

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

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

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

whence it follows that the sequence

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

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

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

■

Definition 2.29 (Projective Module). An A-module P satisfying any one of the four equivalent conditions of Theorem 2.28 is said to be a *projective A-module*.

In particular, from Theorem 2.28(c), we see that every free module is projective.

Lemma 2.30. *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 2.14, we must have that $K = 0$ whence M is free. ■

Proposition 2.31. *Projective modules are flat.*

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

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 1.5. ■

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, $a/s = 0/s$.

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 3.3. *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 3.4. $S^{-1} : A - \mathbf{Mod} \to S^{-1}A - \mathbf{Mod}$ *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, $\mathrm{im}(S^{-1}f) \subseteq \ker(S^{-1}g)$. 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, $\ker(S^{-1}g) \subseteq \mathrm{im}(S^{-1}f)$. This completes the proof. ■

Proposition 3.5. *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) $S^{-1}\left(\sum_{i\in I} M_i\right) = \sum_{i\in I} S^{-1}M_i$

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 3.4, 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 3.4, the sequence $0 \to S^{-1}M_i \to S^{-1}\overline{M}$ is exact. Consequently, $\sum_{i\in I} S^{-1}M_i \subseteq S^{-1}\overline{M}$.

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.

■

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

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

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. ∎

Chapter 5

Noetherian and Artinian Rings and Modules

5.1 Chain Conditions

5.2 Noetherian Rings

Lemma 5.1. *If A is Noetherian and $\phi : A \to B$ is a surjective ring homomorphism, then B is also Noetherian.*

Theorem 5.2 (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 $f_{k+1} \in I \backslash (f_1, \ldots, f_k)$ 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 $(a_1, \ldots, a_n) = (a_1, \ldots, a_n, a_{n+1})$. Consequently, we may write a_{n+1} as a linear combination of $a_1, \ldots, a_n$, say

$$a_{n+1} = b_1 a_1 + \cdots + b_n a_n$$

for some $b_1, \ldots, b_n \in A$. 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 $g \in I \backslash (f_1, \ldots, f_n)$, 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 $A[\![x]\!]$.

5.2.1 Primary Decomposition

Definition 5.3 (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 5.4. *In a noethering, every ideal can be expressed as a finite intersection of irreducible ideals.*

Proof. Let Σ be the poset of ideals that cannot be expressed as a finite intersection of irreducible ideals in A. Suppose Σ is nonempty, then every chain in Σ is finite (owing to noetherian-ness) whence has an upper bound, thus Σ has a maximal element (Zorn's Lemma), say $\mathfrak{a}$. Note that $\mathfrak{a}$ cannot be irreducible, therefore, there are ideals $\mathfrak{b}, \mathfrak{c}$ properly containing $\mathfrak{a}$ such that $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$. Due to the maximality of $\mathfrak{a}$, both $\mathfrak{b}$ and $\mathfrak{c}$ can be expressed as a finite intersection of irreducible ideals in A, as a result, so can $\mathfrak{a}$, a contradiction. Thus Σ must be empty and the proof is complete. ∎

Lemma 5.5. *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

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

Since $A/\mathfrak{q}$ is a noethering, there is a positive integer n such that $\mathrm{Ann}(y^n) = \mathrm{Ann}(y^{n+1})$. 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 $v \in \mathrm{Ann}(y^{n+1}) = \mathrm{Ann}(y^n)$, 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. ∎

5.3 Artinian Rings