Commutative Algebra

Pitchayut Saengrungkongka

Last updated: November 18, 2025

Contents

1 Rings 1

1.1 Rings and Ideals 1

1.1.1 Ring Homomorphisms 1

1.1.2 Ideals 2

1.1.3 Quotient Rings 4

1.2 Properties of Rings 5

1.2.1 Special Elements 5

1.2.2 PID and UFD 6

1.2.3 Chinese Remainder Theorem 7

1.3 Primes and Maximal Ideals 7

1.3.1 Definition and Basic Properties 7

1.3.2 Zorn's Lemma and Krull's Theorem 9

1.4 Radicals 10

1.4.1 Nilradical 10

1.4.2 Radical Ideal 10

1.5 Spectrum and Zariski Topology 11

1.5.1 Varieties 11

1.5.2 Spectrum of a Ring 12

1.5.3 Zariski Topology 12

1.5.4 Contraction and Spec Functor 14

1.5.5 Spec $\mathbb{Z}[x]$ and Spec $\mathbb{C}[x, y]$ 15

1.6 Problems 16

2 Modules 17

2.1 Modules 17

2.1.1 Definition and Basic Properties 17

2.1.2 Constructions of Modules 17

2.1.3 Modules Over PID 19

2.2 Cayley-Hamilton Theorem and Consequences 19

2.2.1 Cayley-Hamilton Theorem 19

2.2.2 Nakayama's Lemma 20

2.3 Exactness 21

2.3.1 Exact Sequences 21

2.3.2 Exact Functor 23

2.4 Colimits . . . 25

2.4.1 Directed System and Colimit . . . 25

2.4.2 Filtered Colimit Preserves Exactness . . . 28

2.5 Tensor Product . . . 30

2.5.1 Definition . . . 30

2.5.2 Properties of Tensor Product . . . 31

2.5.3 Right Exactness of Tensor Product . . . 33

2.5.4 Base Change . . . 35

2.6 Problems . . . 37

3 Localization 39

3.1 Localization of Rings . . . 39

3.1.1 Definition and Explicit Construction . . . 39

3.1.2 Examples . . . 40

3.1.3 Ideals of Localization . . . 41

3.1.4 Localization Commutes with Everything . . . 43

3.2 Localization of Modules . . . 44

3.2.1 Definition and Basic Properties . . . 44

3.2.2 Exactness . . . 44

3.2.3 Localization Commutes with Everything II . . . 45

3.3 Local Properties of a Module . . . 45

3.4 Locally Free Modules . . . 47

3.4.1 Definition and Examples . . . 47

3.4.2 Linear Algebra on Locally Free Modules . . . 48

3.5 Problems . . . 50

4 Integral Extensions 51

4.1 Integral Elements . . . 51

4.2 Integral Extension and Closure . . . 53

4.2.1 Definition . . . 53

4.2.2 Basic Properties . . . 54

4.3 Cohen-Seidenberg Theory . . . 57

4.3.1 Going-up Theorem . . . 57

4.3.2 Going-down Theorem . . . 60

4.4 Noether Normalization and Nullstellensatz . . . 61

4.4.1 Noether Normalization . . . 61

4.4.2 Nullstellensatz . . . 62

4.5 First Steps in Dimension Theory . . . 65

4.6 Problems . . . 67

5 Chain Conditions **69**
5.1 Noetherian and Artinian Modules 69
5.1.1 Definitions and Basic Examples 69
5.1.2 Properties of Noetherian and Artinian Modules 70
5.2 Noetherian Rings 71
5.2.1 Properties of Noetherian Rings 71
5.2.2 Zariski Topology of Noetherian Rings 73
5.2.3 Irreducible Components 73
5.3 Artinian Rings 76
5.3.1 Preliminary: Product Rings 76
5.3.2 Structure Theorem for Artinian Rings 77
5.4 Problems 79

6 Associated Primes and Primary Decomposition **81**
6.1 Associated Primes 81
6.1.1 Definition 81
6.1.2 Basic Properties 82
6.1.3 Local Property and Associated Primes 84
6.2 Primary Decomposition 84
6.2.1 Primary Ideals 84
6.2.2 Primary Decomposition 86
6.2.3 Quasi-uniqueness of Primary Decomposition 88
6.3 Problems 88

7 Discrete Valuation Rings and Dedekind Domains **91**
7.1 Discrete Valuation Ring 91
7.1.1 Definition and Basic Properties 91
7.1.2 Characterization of DVRs 92
7.2 Dedekind Domain 94
7.2.1 Definition and Unique Factorization 94
7.2.2 Key Example: Extensions of Dedekind Domain 95
7.3 Fractional Ideals 97
7.3.1 Fractional Ideals and Invertible Ideals 97
7.3.2 Class Group 98
7.4 Problems 100

8 Completion **101**
8.1 Construction 101
8.1.1 Inverse Limit 101
8.1.2 Completion with respect to Filtration 103
8.2 Hensel's Lemma 104
8.3 Artin-Rees Lemma 106
8.3.1 Statement 106
8.3.2 Proof 106

8.4 Properties of Completion 108
  8.4.1 Exactness 108
  8.4.2 Flatness 108
  8.4.3 Associated Graded Ring and Noetherianess 110
8.5 Problems 112

9 Dimension Theory 115
9.1 Preliminary: Length of a Module 115
9.2 Hilbert's Dimension 117
  9.2.1 Definition 117
  9.2.2 Proof of Polynomiality 118
9.3 Primary Ideal Dimension and Dimension Theorem 120
  9.3.1 Primary Ideal Dimension 120
  9.3.2 The Primary Ideal Dimension is at least the Hilbert Dimension 121
  9.3.3 The Hilbert Dimension is at least the Krull Dimension 121
  9.3.4 The Krull Dimension is at least the Primary Ideal Dimension 122
9.4 Consequences of Dimension Theorem 123
  9.4.1 Dimension of Local Rings 123
  9.4.2 Krull's Principal Ideal Theorem 124
9.5 Regular Local Ring 125
  9.5.1 Definition and Basic Properties 125
  9.5.2 Harder Facts about Regular Local Rings 128
9.6 Problems 128

10 Flatness 131
10.1 Homological Algebra Crash Course 132
  10.1.1 Homology 132
  10.1.2 Free Resolutions 133
10.2 Flatness and Tor 133
  10.2.1 The Tor Functor 133
  10.2.2 Ideal-theoretic Criterion of Flatness 135
  10.2.3 Flatness over Local Rings 137
  10.2.4 (Bonus) Local Criteria of Flatness 137
10.3 Going-Down Theorem, Flat Version 138
  10.3.1 Faithful Flatness 138
  10.3.2 Proof of Going Down 140
10.4 Flatness Implies Constant-Dimension Fibers 141
10.5 Problems 142

A Background 145
A.1 Category and Functors 145
A.2 Universal Properties 146
A.3 Topological Spaces 148

B More About Free Resolutions **151**
B.1 Chain Homotopy 151
B.2 Fundamental Theorem of Homological Algebra 152
B.3 Proof that Tor does not Depend on Free Resolution 153

Index **155**

Notations **159**

Bibliography **161**

Preface

▶ **What is Commutative Algebra?** The origin of commutative algebra comes from the following two fields:

- **algebraic number theory,** which studies prime factorization in number fields (such as $\mathbb{Q}(\sqrt{-5})$) and its ring of integers (such as $\mathbb{Z}$ and $\mathbb{Z}[\sqrt{-5}]$).
- **algebraic geometry,** which studies solutions of systems of algebraic equations (such as $x^2+y^2=1$), which can be turned to study of quotients of polynomial rings (such as $\mathbb{C}[x,y]/(x^2+y^2-1)$).

Throughout time, people have realize that theory from these two subjects can be unified into a single theory of commutative rings. This results in a single, clean theory of commutative algebra that stands on its own, but its true purpose is to be applied in the context of number theory and algebraic geometry

▶ **Prerequisite** We assume that the reader is familiar with rings and modules at an undergraduate level (e.g., as in [Art11]). Basic concepts of rings and modules will be rapidly reviewed in Chapter 1 and Chapter 2. Familiarity with basic category theory and topology is assumed, but we quickly review those in Appendix A. Knowledge of field theory at an undergraduate level is assumed in some places.

▶ **Content** These notes cover standard material typically covered in an introductory graduate course (such as 18.705 at MIT). The goal is to develop basic theory of rings and modules necessary in the study of algebraic number theory and algebraic geometry. Although we do not cover algebraic geometry or algebraic number theory, we try, whenever possible, to point out motivations and connections from these two subjects. The breakdown by chapter is as follows.

- **Chapter 1 (Rings).** We start out by quickly reviewing the notions of rings and ideals, including primary and maximal ideals. The spectrum of a ring, which is a central notion in algebraic geometry, is introduced in Section 1.5.
- **Chapter 2 (Modules).** We quickly review basis notions of modules, then we proceed to discuss properties and constructions related to modules at a significantly greater depth than typically covered in undergraduate algebra. We discuss Cayley-Hamilton theorem from linear algebra and its consequence on modules that we will use multiple times throughout. Then, we discuss important constructions related to modules: exactness, colimits, and tensor products.
- **Chapter 3 (Localization).** Localization is the "art of adding denominators" to rings. This construction has a geometric interpretation of "zooming into" open sets or points and is immensely useful in studying rings.
- **Chapter 4 (Integral Extensions).** Integral extension and integral closure is a fundamental notion that connects to finite maps, smooth curves, and ring of algebraic integers. As a consequence of this theory, we present Noether normalization lemma and use it to prove Hilbert nullstellensatz and study dimension of a variety.
- **Chapter 5 (Chain Conditions).** We discuss Noetherian rings and modules, the fundamental finiteness conditions that has numerous consequences. Artinian rings are also discussed.

- **Chapter 6 (Associated Primes and Primary Decomposition).** In unique factorization domains such as $\mathbb{Z}$, every element can be factored uniquely into products of primes. We discuss a analogue of this in a general ring, which will allow us to decompose an ideal into intersection of primary ideals (which is an analogue of prime power).
- **Chapter 7 (DVR and Dedekind Domains).** Discrete valuation rings (DVR) are the simplest kind of rings after fields. Geometrically, its "valuation" comes naturally from trying to define order of vanishing of functions at a point. A global analogue of DVR is a Dedekind domain, which arise naturally from ring of integers (in number theory) and a smooth curve (in algebraic geometry). We discuss their properties.
- **Chapter 8 (Completion).** As power series is useful in studying functions in real and complex analysis, we develop the notion of power series in commutative algebra, resulting in construction known as completion. We prove several nice properties of completion.
- **Chapter 9 (Dimension Theory).** Although dimension is an intuitive concept in geometry, proving properties about dimension of rings are notoriously difficult. In this chapter, we develop a robust framework to study and compute dimensions. A brief treatment of regular local rings (rings corresponding to smooth varieties) is discussed.
- **Chapter 10 (Flatness).** We study flat modules (defined in Chapter 2 in terms of tensor products) in more detail, discussing various geometric consequence such as going-down property, and constant dimension of fiber.

The text is meant to be read in order, although dependencies between many chapters are weak, and some flexibility is possible.

All contents existed in standard commutative algebra textbooks. The one closest to our notes is [AM69]. Other books that influenced our presentation are [AK13], [Eis95], and [Vak24]. I claim no originality in any of these materials.

▶ **History and Acknowledgements** These notes were based on the notes that I took when taking the Fall 2023 instance of 18.705 (a commutative algebra course) at MIT, taught by Davesh Maulik. Since then, many parts were rewritten, and a new Chapter 10 on flatness was added. Nevertheless, the structure of these notes still largely follows how Maulik taught the class, and his insights and presentation is still imparted throughout these notes. The flatness chapter was based on the Fall 2024 instance of 18.705, taught by Miguel Moreira, which also influences the presentation of various parts of theses notes as well.

We thank Derek Liu for contributing part of Chapter 10. We also thank Srinivas Arun, David Dong, and Linus Tang for useful comments and suggestions.

1 Rings

The origins of commutative algebra goes back to about 150 years ago, when the following subjects are studied.

- **Algebraic Number Theory**, which studies about a specific kind of commutative rings generated from **number fields**. (e.g., $\mathbb{Q}$, $\mathbb{Z}[i]$, $\mathbb{Z}_p$, $\mathbb{Z}/p\mathbb{Z}$, etc.)
- **Algebraic Geometry**, which studies about polynomial rings $k[x]$, $k[x_1, \ldots, x_n]$, and their quotients (where k is a field). The most important casae is when $k = \mathbb{C}$, but modern algebraic geomety have extended to studying polynomial equations over arbitrary field too.

However, people then realize that these two subjects have the same foundation. In particular, theorems about Algebraic Number Theory and theorems in Algebraic Geometry have a lot in common, and the common foundation — properties of commutative rings — establishes **commutative algebra**. The central object of commutative algebra is ring, which we introduce in this chapter.

§1.1 Rings and Ideals

In this section, we set up some basic concepts of rings and ideals.

§1.1.1 Ring Homomorphisms

The most basic object we are going to study is (commutative) rings. A **ring** R has operations addition $+$ and multiplication $\cdot$, which must satisfies the following:

- addition forms an abelian group, i.e., it must be associative, commutative, have identity 0, and each element must have additive inverse;
- multiplication is associative, commutative, and has identity 1 (but each element need not have multiplicative inverse); and
- distributive property holds.

We allow $0 = 1$, in which case $R = \{0\}$.

In these notes, we assume all rings are commutative and contain 1.

Example 1.1.1 (Basic rings).

The most basic example of ring is integers $\mathbb{Z}$. Furthermore, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all rings. Integers modulo n, $\mathbb{Z}/n\mathbb{Z}$, form a ring.

Example 1.1.2 (Constructing new rings)**.**

Here are some ways to construct a new ring.

- Given a ring R, one can adjoin a free element x to get a **polynomial ring** $R[x]$, which is described by

$$R[x] = \{a_0 + a_1 x + \cdots + a_n x^n : a_0, \ldots, a_n \in R\}.$$

  Similarly, one can adjoin arbitrarily many elements to get rings such as $R[x_1, \ldots, x_m]$, which is a ring of polynomials in m variables with coefficients in R.

- Given two rings R and S, one construct the **product ring**

$$R \times S = \{(r, s) : r \in R, s \in S\},$$

  where addition and multiplication are done component-wise.

A **ring morphism** between two rings R and S is a map $\phi : R \to S$, that satisfies $\phi(x+y) = \phi(x)+\phi(y)$, $\phi(xy) = \phi(x)\phi(y)$, and $\phi(1) = 1$ for all $x, y \in R$. In particular,

$$\boxed{\text{We assume that all ring morphisms preserve 1.}}$$

Example 1.1.3 (Ring morphisms)**.**

We have the following examples:

- For any ring R, there exists a unique ring homomorphism $f : \mathbb{Z} \to R$ by

$$f(n) = \underbrace{1 + \cdots + 1}_{n}.$$

- For any ring R, there exists a unique ring morphism $f : R \to \{0\}$.
- If p is a prime, and suppose $\underbrace{1 + \cdots + 1}_{p} = 0$ (i.e., R has characteristic p), then we have the **Frobenius morphism** $F : R \to R$ by $F(a) = a^p$. (Proof: multiplication is obvious. For addition, $(a + b)^p = a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \cdots + b^p = a^p + b^p$.)

§1.1.2 Ideals

Ideals are a subset of ring that has special properties. Most importantly, it forms a quotient ring, which we describe in the next subsection. A subset $I \subseteq R$ is an **ideal** if and only if it

- is closed under addition ($a, b \in I \implies a + b \in I$) and
- absorbs multiplication ($a \in I, r \in R \implies ra \in I$).

Example 1.1.4.

We have the following examples of ideals.

- For any integer n, $(n) = n\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal. Moreover, all ideals of $\mathbb{Z}$ are of this form.
- $\{0\}$ and R itself is an ideal of R. If R is a field, these two are the only ideals of R.
- For each $a \in R$, we have the ideal generated by a defined by $(a) = \{ar : r \in R\}$. These

ideals are called **principal ideals**. For $\mathbb{Z}$, every ideal is principal.

- More generally, given some subset $T \subseteq R$, we can define the ideal generated by T as the smallest ideal containing T, which is

$$(T) = \left\{ \sum_{i=1}^{m} a_i t_i : a_i \in R, t_i \in T \right\}.$$

Ideals generated by $\{x_1, \dots, x_n\}$ is often written as $(x_1, \dots, x_n)$.

Another way to construct ideals is to take the kernel. Given a ring homomorphism $f : R \to S$, then

$$\operatorname{Ker} f = f^{-1}(\{0\}) \subseteq R$$

is always an ideal of R. This is in fact a special case of a more general construction called contraction.

Definition 1.1.5 (Contraction and Extension).

Consider a ring homomorphism $f : R \to S$.

- For each ideal $J \subseteq S$, the **contraction** $f^{-1}(J) \subseteq R$ is automatically an ideal.
- For each ideal $I \subseteq R$, the **extension** IS is the ideal **generated by** the image $f(I)$.

Finally, we have the following operations of ideals.

Definition 1.1.6 (Ideal operations).

Let I, J be an ideal of a ring R. Then,

- $I \cap J$ is an ideal.
- $I + J = \{i + j : i \in I, j \in J\}$ is an ideal.
- IJ is the ideal generated by $\{ij : i \in I, j \in J\}$.

They are analogue of lcm, $\gcd$, and product, respectively. For example, in $\mathbb{Z}$, we have $(4) \cap (6) = (12)$, $(4) + (6) = (2)$, and $(4)(6) = (24)$.

Remark 1.1.7 (Origin of ideals).

The first usage of the word **ideal** is by Dedekind, who is a algebraic number theorist. He coined the word **ideal numbers** to describe the phenomenon of unique factorization in rings of algebraic integers.

To elaborate, people at that time are interested in solving the equation $x^n + y^n = z^n$ (Fermat's last theorem) where $x, y, z \in \mathbb{Z}$. One idea (led by Kummer) to solve this problem is to adjoin $\zeta = e^{2\pi i/n}$, then one can rewrite this equation to

$$(x + y)(x + \zeta y) \dots (x + \zeta^{n-1} y) = z^n.$$

Then, people work with the ring $\mathbb{Z}[\zeta]$ and, assuming that it's UFD (i.e., has unique factorization property), able to deduce that each factor $x + y$, $x + \zeta y$, …, $x + \zeta^{n-1} y$ must be an n-th power (or close to), and then make a contradiction.

However, the ring of algebraic integers is not necessarily a UFD. For example, in the ring $\mathbb{Z}[\sqrt{-5}]$, we have $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, and neither 2, 3, $1 + \sqrt{-5}$, nor $1 - \sqrt{-5}$ can be factored further in $\mathbb{Z}[\sqrt{-5}]$. Thus, $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. In the case of Fermat's last theorem, the smallest n for which unique factorization property fail is $n = 23$.

> In the world of ideals, both 2 and 3 breaks up in $\mathbb{Z}[\sqrt{-5}]$. Indeed, in ideals,
>
> $$(2) = (2, 1+\sqrt{-5})^2, \quad (3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5}),$$
>
> and unique factorization is restored, except that the ideal $(2, 1+\sqrt{-5})$ is no longer principal. In Section 7.2, we will discuss a broad class of ring that unique factorization of ideals hold.

§1.1.3 Quotient Rings

We now describe the most important way to generate new rings, called **quotient ring**. Given a ring R and an ideal $I \subseteq R$, then we define the quotient ring R/I as the ring of cosets

$$\{[a] := a + I : a \in R\}.$$

We define the operations by $[a+b] = [a]+[b]$ and $[ab] = [a][b]$ as expected. This map is well-defined. Indeed, if $a - a' \in I$, then e.g., $ab - a'b \in I$, so $[ab] = [a'b]$.

We then also define the surjective ring homomorphism $\pi : R \to R/I$ by $\pi(a) = [a]$. The kernel of this map is I. This map satisfies the following universal property: suppose S is another ring and a homomorphism $f : R \to S$ such that $f(I) = 0$, then there exists a unique ring homomorphism $\overline{f} : R/I \to S$ such that the following diagram commutes:

$$\begin{tikzcd} R \arrow[rr, "\pi"] \arrow[dr, "f"'] & & R/I \arrow[dl, "\exists! \overline{f}"] \\ & S & \end{tikzcd}$$

(Proof: we are forced to have $\overline{f}([a]) = f(a)$, so f is unique. Moreover, this is well-defined because f sends I to 0.)

By the usual argument (see Appendix A.2), this universal property classify π and R/I up to isomorphism.

Theorem 1.1.8 (Correspondence Theorem)**.**

There is a bijection between

$$\{\text{ideals of } R/I\} \longleftrightarrow \{\text{ideals of } R \text{ containing } I\}.$$

For example, the ideals of $\mathbb{Z}/6\mathbb{Z}$ are 0, $\mathbb{Z}/6\mathbb{Z}$, $2\mathbb{Z}/6\mathbb{Z}$, and $3\mathbb{Z}/6\mathbb{Z}$, while the ideals of $\mathbb{Z}$ that contains $6\mathbb{Z}$ are $6\mathbb{Z}$, $\mathbb{Z}$, $2\mathbb{Z}$, and $3\mathbb{Z}$.

▶ *Proof.* Let $\pi : R \to R/I$ be the quotient projection map. The bijection is given by

$$\begin{aligned} \{\text{ideals of } R/I\} &\leftrightarrow \{\text{ideals of } R \text{ containing } I\} \\ J' &\mapsto \pi^{-1}(J') \\ \pi(J) &\leftarrow\!\shortmid J \end{aligned}$$

and it is straightforward to verify that they are inverses. ☐

Theorem 1.1.9 (First Isomorphism Theorem)**.**

Let $\phi : R \to S$ be a surjective ring morphism. Then, $S \simeq R/\operatorname{Ker}\phi$.

▶ *Proof.* Straightforward. ☐

§1.2 Properties of Rings

§1.2.1 Special Elements

We have a bunch of definitions of special elements of a ring.

Definition 1.2.1 (Units, zero divisors, nilpotents).

Given a ring R, an element $a \in R$ is

- a **unit** if for some $b \in R$, $ab = 1$;
- a **zero divisor** if for some $b \neq 0 \in R$, $ab = 0$; and
- **nilpotent** if $a^n = 0$ for some $n \geq 1$.

The set of nilpotent elements turns out to be an ideal.

Proposition 1.2.2.

The set $\operatorname{Nil} R \subseteq R$ is an ideal of R, called the **nilradical** of R.

▶ *Proof.* Absorbing multiplication is obvious. To show that $\operatorname{Nil}(R)$ is closed under addition, if $a^m = 0$ and $b^n = 0$, then the binomial expansion of $(a+b)^{m+n}$ consists of monomials of the form $a^i b^j$. At least one of $i \geq m$ and $j \geq n$ must hold, so the monomial is divisible by either a^m or b^n, both of which are 0, so all monomials vanish, which means $(a+b)^{m+n} = 0$, so $a + b \in \operatorname{Nil}(R)$. ☐

Each kind of special element leads to a type of ring.

Definition 1.2.3 (Field, domain, reduced rings).

A ring R is

- a **field** if $R \neq 0$ and every $a \neq 0$ is a unit;
- a **domain** if $R \neq 0$ and 0 is the only zero divisor; and
- **reduced** if 0 is the only nilpotent element.

Remark 1.2.4.

We use the word domain instead of integral domain to avoid confusion caused by the word integral as in Chapter 4)

Example 1.2.5.

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ are fields.
- $\mathbb{Z}$ and $\mathbb{C}[x]$ are domains. (In fact, if R is a domain, then so is $R[x]$, so $\mathbb{C}[x_1, \ldots, x_n]$ is a domain.)
- $\mathbb{C}[x,y]/(xy)$ is not a domain because in this ring, $xy = 0$ but $x, y \neq 0$.
- $\mathbb{C}[x,y]/(xy)$ is reduced.
- $\mathbb{C}[x]/(x^2)$ is not reduced because x is nilpotent.

✍ **Exercise 1.2.6.** What are the zero divisors and nilpotent elements of $\mathbb{Z}/12\mathbb{Z}$?

§1.2.2 PID and UFD

Definition 1.2.7 (PID and UFD).

A domain R is a

- **principal ideal domain (PID)** if every ideal principal.
- **unique factorization domain (UFD)** if every non-zero element $x \in R$ can be written uniquely as a product of irreducible elements

$$x = p_1 \cdots p_n,$$

where uniqueness is up to multiplication by units, i.e., if $x = q_1 \cdots q_m$ is another factorization, then $m = n$ and there exists a permutation π such that $q_{\pi(i)}$ is equal to p_i times a unit for all i. An element $p \in R$ is irreducible if it is not a product of two non-units in R.

We note down two useful properties of PID and UFD proved in undergraduate algebra. The proofs of these are not central to these notes, so we merely sketch it.

Theorem 1.2.8.

(a) Any PID is a UFD.

(b) If R is a UFD, then so is $R[x]$ (hence, by induction, $R[x_1, \dots, x_n]$ is a UFD).

▶ *Proof Sketch.* (a) First, we need to show that every element x is a product of irreducible elements. Obviously, we keep factoring out elements. If this does not terminate, then there would be an infinite chain $x = a_0, a_1, a_2, \dots$ such that a_{i+1} is a proper divisor of a_i, i.e., $(a_0) \subsetneq (a_1) \subsetneq \dots$. Then, the union $\bigcup_{i\geq 0}(a_i)$ is an ideal, say (x), then $(x) = (a_i)$, a contradiction.

Next, we show uniqueness. If p is irreducible, then (p) is maximal, hence prime, so if p divides ab, then p divides either a or b. Thus, if we have two different product of irreducible elements $x = p_1 \cdots p_m = q_1 \cdots q_n$, then p_i divides one of $q_1, \dots, q_n$, hence equal to q_j for some j (up to multiplication by units). Similarly each q_j is equal to p_i for some i. Thus, the multiset of p_i and of q_j are equal.

(b) First, factorization terminates because the degree decreases until it is constant polynomial, at which point we can utilize the fact that factoring in R terminates.

Now, we show that any irreducible element is prime. To do this, we prove the following lemma: “A polynomial $f \in R[x]$ is primitive if and only if no element in R divides all coefficients in f. If f, g is primitive, then fg is primitive.” To prove the lemma, suppose that an irreducible factor p divides all coefficients of fg. Then, $fg = 0$ in $R/(p)[x]$. However, $R/(p)[x]$ is a domain (because $R/(p)$ is a domain), a contradiction.

Let K be the field of fraction of R. If $f, g, h \in R[x]$ such that f is irreducible (hence primitive) and $f \mid gh$, then $f \mid gh$ in $K[x]$, so there exists $d \in R$ such that $\overline{f}(x) = d \cdot gh/f \in R[x]$. Scale down so that $\overline{f}(x)$ is primitive, then the lemma forces $d = 1$, so f divides gh in $R[x]$. Hence, every irreducible element is prime. ☐

Example 1.2.9 (PID and UFD).

- $\mathbb{Z}$, $\mathbb{Z}[i]$, and $\mathbb{C}[x]$ are PID.

- $\mathbb{C}[x,y]$ is a UFD by Theorem 1.2.8 (b), but it is not a PID because ideal (x,y) is not principal; if $(x,y)=(f)$, then x and y must be divisible by f, forcing $f=1$, which is a contradiction.
- $\mathbb{Z}[\sqrt{-5}]$ is not a UFD because $2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5})$, and 2, 3, $1+\sqrt{-5}$, and $1-\sqrt{-5}$ are all irreducible.

§1.2.3 Chinese Remainder Theorem

There is a number-theoretic phenomenon that for example, $\mathbb{Z}/(12)\simeq\mathbb{Z}/(4)\times\mathbb{Z}/(3)$. This fact generalizes to any rings.

Definition 1.2.10 (Coprime ideals).

Given a ring R, two ideals $I,J\subset R$ are **coprime** if $I+J=(1)$.

Theorem 1.2.11 (Chinese Remainder Theorem).

If I and J are coprime, then

(a) $I\cap J=IJ$.

(b) The map $f:R\to R/I\times R/J$ by $a\mapsto(a \bmod I, a \bmod J)$ is surjective.

(c) We have $R/IJ\simeq R/I\times R/J$.

The proof is the same as number theory class.

▶ *Proof.* The fact that I and J are coprime means that there exists $i\in I$ and $j\in J$ for which $i+j=1$.

(a) The inclusion $IJ\subseteq I\cap J$ is clear. Thus, we show that $IJ\supseteq I\cap J$. Let $a\in I\cap J$. Then, we have

$$a=a\cdot 1=a\cdot j+i\cdot a,$$

and each term is in $I\cdot J$.

(b) Let $[x]\in R/I$ and $[y]\in R/J$. Set $a=xj+yi$, and see that $a\equiv xj\equiv x\pmod I$ and $a\equiv yi\equiv y\pmod J$.

(c) By the first isomorphism theorem (Theorem 1.1.9), we have $R/\operatorname{Ker} f\simeq R/I\times R/J$. By (a), we have $\operatorname{Ker} f=I\cap J=IJ$, so we are done. ☐

§1.3 Primes and Maximal Ideals

§1.3.1 Definition and Basic Properties

Definition 1.3.1 (Prime ideals).

An ideal $\mathfrak{p}\subset R$ is a **prime ideal** if $\mathfrak{p}\neq R$ and $ab\in\mathfrak{p}$ implies $a\in\mathfrak{p}$ or $b\in\mathfrak{p}$ (or both).

Definition 1.3.2 (Maximal ideals).

An ideal $\mathfrak{m}\in R$ is a **maximal ideal** if $\mathfrak{m}\neq R$ and there are no ideals I such that $\mathfrak{m}\subsetneq I\subsetneq R$.

Proposition 1.3.3.

(a) An ideal $\mathfrak{p} \subseteq R$ is prime if and only if $R/\mathfrak{p}$ is a domain.

(b) An ideal $\mathfrak{m} \subset R$ is maximal if and only if $R/\mathfrak{m}$ is a field.

Consequently, all maximal ideals are prime.

▶ *Proof.* (a) Clear by simply reduce the definition of prime ideal modulo $\mathfrak{p}$.

(b) By correspondence theorem (Theorem 1.1.8), $\mathfrak{m}$ is maximal if and only if $R/\mathfrak{m}$ has no ideal other than 0 or $R/\mathfrak{m}$.

If $R/\mathfrak{m}$ is a field, then $R/\mathfrak{m}$ has only two ideals, because any nonzero ideal I must contain a nonzero element, which is a unit, forcing I to include all elements in $R/\mathfrak{m}$.

Otherwise, if $R/\mathfrak{m}$ is not a field, then it has a non-unit a, so (a) is a nontrivial ideal of $R/\mathfrak{m}$. ☐

Example 1.3.4 (Prime and Maximal Ideals).

We have the following examples.

- (0) is prime if and only if R is a domain.
- (0) is maximal if and only if R is a field.
- If R is a PID, then all prime ideals of R are (0) and (f) for irreducible element f. Special cases of this are
  - The prime ideals of $\mathbb{Z}$ are (0) and (p), where p is the prime numbers. Only (p) are maximal.
  - The prime ideals of $\mathbb{C}[x]$ are (0) and $(x-\alpha)$, where $\alpha \in \mathbb{C}$.
- Prime ideals of $\mathbb{C}[x_1, \dots, x_n]$ are more numerous. For example,

$$0 \subset (x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, \dots, x_n),$$

  are all prime ideals (Proof: $\mathbb{C}[x_1, \dots, x_n]/(x_1, \dots, x_k) = \mathbb{C}[x_{k+1}, \dots, x_n]$, which is a domain). On the other hand, only $(x_1, \dots, x_n)$ is maximal in this chain.

  We will show later in the text (Hilbert Nullstellensatz, Theorem 4.4.5) that all maximal ideals $\mathbb{C}[x_1, \dots, x_n]$ are in from $(x_1 - \alpha_1, \dots, x_n - \alpha_n)$, where $\alpha_1, \dots, \alpha_n \in \mathbb{C}$.
- Let k be a field and consider the **formal series ring**

$$k[[x]] = \left\{ \sum_{n=0}^{\infty} a_n x^n : a_0, a_1, \dots \in k \right\}$$

  (the sum does not need to converge). It's not hard to show that $f(x) = a_0 + a_1 x + \dots$ is a unit if and only if $a_0 \in k^\times$. Using this, we can show that all ideals of $k[[x]]$ are in form (0) and (x^n) for $n \geq 0$. Only (0) and (x) are prime.

In fact, a ring with unique maximal ideal (like the last example) is relatively simpler to study that it bears a special name.

Definition 1.3.5 (Local ring).

R is a **local ring** if it has a unique maximal ideal.

We also have that $k[[x_1, \dots, x_n]]$ is also local. We will see later in Chapter 3 that the study of rings can be reduced to the study of local rings.

Exercise 1.3.6. Prove that the bijection in the correspondence theorem (Theorem 1.1.8) takes prime ideal to prime ideal and maximal ideal to maximal ideal.

§1.3.2 Zorn's Lemma and Krull's Theorem

Theorem 1.3.7 (Krull's Theorem)**.**

Let R be a ring. Then, any ideal $I \subsetneq R$ is contained in a maximal ideal. In particular, maximal ideals exist.

This theorem is seemingly obvious because if $I = I_0$ is not maximal, then there exists a larger ideal $I_0 \subsetneq I_1$. This continues, and we get a chain of ideals

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \dots.$$

If ring R is horrible (example: $\mathbb{Z}[x_1, x_2, \dots]$ and the chain is $(x_1) \subsetneq (x_1, x_2) \subsetneq \dots$), then this process might continue indefinitely.

The idea is that we need to "go beyond infinity". Zorn's lemma is a tool from set theory that allows us to do that.

A **poset** (or **partially ordered set**) $(\mathcal{P}, \leq)$ is a set $\mathcal{P}$ with a partial ordering $\leq$. The ordering should be reflexive ($a \leq a$), antisymmetric ($a \leq b$ and $b \leq a$ implies $a = b$), and transitive ($a \leq b$ and $b \leq c$ implies $a \leq c$). A **totally ordered set** is a poset whose any two elements are comparable.

The following lemma is equivalent to axiom of choice.

Lemma 1.3.8 (Zorn's lemma)**.**

Let $(\mathcal{P}, \leq)$ be a non-empty poset such that for any totally-ordered subset $\mathcal{T} \subset \mathcal{P}$, there exists some element $a_{\mathcal{P}} \in \mathcal{T}$ such that $a_{\mathcal{T}} \geq t$ for all $t \in \mathcal{T}$. Then, $\mathcal{P}$ has a maximal element, i.e, there exists $m \in \mathcal{P}$ such that $m \geq p$ for all $p \in \mathcal{P}$.

▶ *Proof of Theorem 1.3.7.* Take a poset $(\mathcal{P}, \subseteq)$, where

$$\mathcal{P} = \{\text{ideal } J : I \subseteq J \subsetneq R\}$$

ordered by containment.

We need to verify the condition for Zorn's lemma Lemma 1.3.8. Suppose that $\mathcal{T}$ is a totally-ordered subset of ideals, then we claim that $K = \bigcup_{J \in \mathcal{T}} J$ is an ideal not equal to R. To do this, we need to check three things.

- **Closed under addition.** If $a, b \in K$, then there exists $J, J' \in \mathcal{T}$ such that $a \in J$ and $b \in J'$. Then, $a + b \in \max(J, J')$, which is a subset of K.
- **Absorbs multiplication.** If $a \in K$ and $r \in R$, then $a \in J$ for some $J \in \mathcal{T}$, and so $ra \in J$, which implies $ra \in K$.
- **K is not equal to R.** Note that $1 \notin J$ for all $J \in \mathcal{T}$, so $1 \notin K$.

Hence, K is an element in $\mathcal{P}$. It clearly contains every ideal in $\mathcal{T}$, so the condition of Zorn's lemma is satisfied. Hence, poset $\mathcal{P}$ has a maximal element, which must be a maximal ideal. ☐

§1.4 Radicals

§1.4.1 Nilradical

Recall that $\mathrm{Nil}(R)$ is the set of all nilpotent elements of R. This is also called the **nilradical** of R. We now use Zorn's lemma to prove the following important property of nilradical.

Proposition 1.4.1 (Nilradical is intersection of prime ideals).

We have

$$\mathrm{Nil}(R) = \bigcap_{\mathfrak{p} \subseteq R \text{ prime}} \mathfrak{p}$$

► *Proof.* We first show the direction $\subseteq$. To do this, we have to prove that $\mathrm{Nil}\, R \subset \mathfrak{p}$ for all prime ideal $\mathfrak{p}$. Indeed, $a \in \mathrm{Nil}\, R$, then $a^n = 0 \in \mathfrak{p}$, so $a \in \mathfrak{p}$ by definition of prime ideal.

In the direction $\supseteq$, given $f \notin \mathrm{Nil}(R)$, we need to find a prime ideal not containing f. We use Zorn's lemma. Consider the poset $(\mathcal{P}, \subseteq)$ where

$$\mathcal{P} = \left\{ \text{ideal } I \subsetneq R \ : \ 1, f, f^2, \ldots \text{ are all not in } I \right\}$$

ordered by inclusion.

Notice that $f \notin \mathrm{Nil}(R)$, so $S \neq \emptyset$, so $0 \in S$. Moreover, for any totally ordered subset $\mathcal{T} \subseteq \mathcal{P}$, it is not hard to check that $\bigcup_{J \in \mathcal{T}} J$ is an ideal in $\mathcal{P}$ that dominates every element $\mathcal{T}$. Thus, the condition of Zorn's lemma is satisfied, so $\mathcal{P}$ has a maximal element J. Notice that $f \notin J$.

Now, we claim that J is prime (which will finish the proof). Assume $xy \in J$ but $x, y \notin J$. Then, $J + (x) \supsetneq J$, so $J + (x)$ must contain some power of f. In particular, $f^n \in J + (x)$ for some n and $f^m \in J + (y)$ for some m. However, by multiplying, we get that

$$f^{m+n} \in (J + (x))(J + (y)) = J + (xy) = J,$$

which is a contradiction. □

§1.4.2 Radical Ideal

We have shown that $\mathrm{Nil}(R)$ is the same as the intersection of all prime ideals of R. We generalize this a little bit, restricting to only prime ideals that contains I.

Definition 1.4.2 (Radical ideal).

Given a ring R and an ideal I, we define the **radical ideal**

$$\sqrt{I} = \{a \in R : a^n \in I \text{ for some positive integer } n\}.$$

(Example: if $R = \mathbb{Z}$, then $\sqrt{(48)} = (6)$.)

An ideal I is called **radical** if $\sqrt{I} = I$.

Let $\pi : R \to R/I$ be the quotient map. Then, the condition that $a^n \in I$ for some positive integer n is equivalent to $\pi(a) \in \mathrm{Nil}(R/I)$. Therefore, we have

$$\begin{aligned}
\sqrt{I} &= \pi^{-1}(\mathrm{Nil}(R/I)) \\
&= \pi^{-1}\left(\bigcap_{\mathfrak{p} \subseteq R/I \text{ prime}} \mathfrak{p} \right) && \text{(Proposition 1.4.1)} \\
&= \bigcap_{I \subseteq \mathfrak{p} \subseteq R \text{ prime}} \mathfrak{p}. && \text{(Correspondence theorem Theorem 1.1.8)}
\end{aligned}$$

§1.5 Spectrum and Zariski Topology

Several pictures come from [Che25].

§1.5.1 Varieties

Many aspects of commutative algebra are motivated by algebraic geometry. Since this is not algebraic geometry notes, we will informally introduce algebraic geometry just enough to understand some geometric intuition behind commutative algebra, but we will not do any serious algebraic geometry. **This entire subsection is very informal** and is intended to only give intuition. There is no actual math done in this subsection.

For these notes, a **variety** is a set V of the form

$$V = \{\vec{x} \in \mathbb{C}^n : f_1(\vec{x}) = f_2(\vec{x}) = \cdots = f_m(\vec{x}) = 0\} \ \subseteq \ \mathbb{C}^n,$$

where $f_1, \dots, f_m \in \mathbb{C}[x_1, \dots, x_n]$. To understand variety, we want to consider a **ring of regular functions** associated to it. More specifically, we want to consider a ring R of all **regular functions** $f : V \to \mathbb{C}$, which are rational functions from $V \to \mathbb{C}$ defined everywhere in V.

Example 1.5.1.

- If $V = \mathbb{C}^n$, then $R = \mathbb{C}[x_1, \dots, x_n]$ is our ring of regular functions. Function x_i would take a point in V and output the i-th coordinate of V. Notice that even though we say rational function, we cannot have denominator here.
- Now, suppose that
$$V = \{(x, y) \in \mathbb{C}^2 : x^2 + y^2 = 1\}.$$
Then, now, the function $x^2 + y^2 - 1$ is the same as function 0. Thus, the ring of regular functions needs to be modded out by $(x^2 + y^2 - 1)$, so $R = \mathbb{C}[x, y]/(x^2 + y^2 - 1)$.

Thus, in general, if $V = \{\vec{x} \in \mathbb{C}^n : f_1(\vec{x}) = f_2(\vec{x}) = \cdots = f_m(\vec{x}) = 0\}$, then the ring of regular functions R would be

$$\mathbb{C}[x_1, \dots, x_n]/(f_1, \dots, f_m).$$

Many properties of ring of regular functions R translates to properties of varieties V. We describe some connections below, although none of these are precise.

- Given an ideal $I \subset R$, the set of points in V whose every function in I vanishes is a closed subset of V (in analytical sense).
- Suppose there is another variety V' with ring of regular functions R'. Then, a morphism $\phi : V \to V'$ corresponds to a ring morphism $\phi^* : R' \to R$ that takes a function $f : V' \to \mathbb{C}$ to a function $f \circ \phi : V \to \mathbb{C}$.
- R is a domain if and only if V is irreducible (i.e., is not a union of two subvarieties). Suppose that V is a union of two subvarieties $V_1 \cup V_2$, where V_1 is cut out by equations $f_1(\vec{x}) = \cdots = f_m(\vec{x}) = 0$, while V_2 is cut out by equations $g_1(\vec{x}) = \cdots = g_n(\vec{x}) = 0$. Then, $V_1 \cup V_2$ is cut out by equations $f_i(\vec{x})g_j(\vec{x}) = 0$. In particular, the function f_i and g_j are nonzero regular functions on V, but they multiply to 0, which makes R not a domain.
- R is a field if and only if V has exactly one point. This is because informally, if V has more than one point, we can create a function f vanishing at one point but not the other, and this f would not be invertible and not a unit.
- For the definition of variety defined above, we always have that R is reduced. In particular, cutting out by equation $(x - y)^2 = 0$ or $x - y = 0$ mean the same thing. We can have a more subtle notion of geometric objects where $\mathbb{C}[x, y]/((x - y))$ is simply a line $x = y$, but $\mathbb{C}[x, y]/((x - y)^2)$ carries more information than a line, including an infinitesimal neighborhood around each point in the line $x = y$. This infinitesimal neighborhood is informally called a fuzz.

This notion of geometric object that capture fuzz is a **scheme**, which generalize varieties in a few different directions, one of which is allowing fuzz. We do not study schemes in these notes.

One idea of algebraic geometry is to go backward: given a ring of function R, construct a geometric space that can substitute the variety V above. The space is called $\operatorname{Spec} R$, and it will make all connections above precise.

§1.5.2 Spectrum of a Ring

Definition 1.5.2 (Spectrum).

- The **spectrum** of a ring R, denoted $\operatorname{Spec} R$ is the set of all prime ideals of R.
- The **maximal spectrum** of a ring R is denoted $\operatorname{mSpec} R$ and is the set of all maximal ideals of R.

For example, by Hilbert Nullstellensatz (Theorem 4.4.5), maximal ideal in $\operatorname{mSpec} \mathbb{C}[x_1, \dots, x_n]$ correspond to points in $\mathbb{C}^n$. Maximal ideal $\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n)$ corresponding to point $(a_1, \dots, a_n) \in \mathbb{C}^n$, and for any polynomial f, we have that $f \bmod \mathfrak{m} = f(a_1, \dots, a_n)$ is the value of f evaluated at that point.

In general, we can view a ring as a ring of regular functions. For any ring R and $f \in R$, we want to think of f as defining a "function" on $\operatorname{mSpec} R$. This generalizes to $\operatorname{Spec} R$, and we will explain later (in Remark 1.5.11) why we prefer to use prime ideals instead of maximal ideal.

Definition 1.5.3.

Given $\mathfrak{p} \in \operatorname{Spec} R$ and $f \in R$, the "value" of f when "evaluated" at $\mathfrak{p}$ is $f \bmod \mathfrak{p} \in R/\mathfrak{p}$.

For psychological reason, we occasionally use a different notation for points in $\operatorname{Spec} R$ with the prime ideals of R. Specifically,

- Point $x \in \operatorname{Spec} R$ corresponds to prime ideal $\mathfrak{p}_x \subseteq R$.
- Prime ideal $\mathfrak{p} \subseteq R$ corresponds to point $[\mathfrak{p}] \in \operatorname{Spec} R$.

§1.5.3 Zariski Topology

We now equip a topology of $\operatorname{Spec} R$, which will be a substitute topology for our geometric space.

As a quick reminder, to define a topological space X, one needs the set of **open** sets $\mathcal{U}$ preserved by unions and finite intersections. A set is **closed** iff its complement is open. Such collection is very arbitrary, and many intuition from metric spaces will break down.

Definition 1.5.4 (Zariski topology).

Let R be a ring. For each ideal $I \subseteq R$, define

$$V(I) = \{\mathfrak{p} \in \operatorname{Spec} R : I \subseteq \mathfrak{p}\}.$$

In **Zariski topology** of $\operatorname{Spec} R$, a subset $S \subseteq \operatorname{Spec} R$ is closed if and only if $S = V(I)$ for some ideal $I \subseteq R$.

We have to check that this defines a topology. We verify the following.

- $\emptyset = V((1))$, so $\emptyset$ is closed.
- $\operatorname{Spec} A = V((0))$, so $\operatorname{Spec} A$ is closed.

- $\bigcap_\alpha V(I_\alpha) = V\left(\sum_\alpha I_\alpha\right)$, so the set of $V(I)$'s is indeed closed under intersection.
- $V(I) \cup V(J) = V(IJ)$, so the set of $V(I)$'s is closed under finite unions.

The last one is the least trivial. In one direction, $IJ \subset I$, so $V(IJ) \supset V(I)$, and so $V(IJ) \supset V(I) \cup V(J)$. Now, if $x \in V(IJ)$ but $x \notin V(I), V(J)$, then there exists $i \in I, j \in J$ such that $i, j \notin \mathfrak{p}_x$. However, this implies that $ij \in IJ$ but $ij \notin \mathfrak{p}_x$. This forms a contradiction.

The idea of this topology is that we want the coarsest (having fewest open sets) topology such that functions in R is continuous. This means we need preimage of $\{0\}$ with respect to f to be closed. This preimage is $V(f)$, which we then declare that it's closed. Taking intersection across many f's gives that we must declare $V(I)$ to be closed for all ideal I. This is all the closed sets we need.

Exercise 1.5.5. Prove that $\mathfrak{m}$ is a maximal ideal if and only if the set $\{[\mathfrak{m}]\}$ consisting of a single point $[\mathfrak{m}]$ is closed. Thus, maximal ideals correspond to **closed points**.

Now, let's get into some examples of drawing spectrum.

Example 1.5.6 (Spec k).

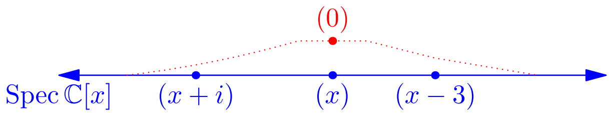
If k is a field, Spec k contains only one point.

Example 1.5.7 (Spec $\mathbb{C}[x]$).

Since prime ideals of $\mathbb{C}[x]$ are (0) and $(x - \alpha)$ for each $\alpha \in \mathbb{C}$, points in Spec $\mathbb{C}[x]$ are

- the **generic point** (0) and
- points $(x - \alpha)$ for each $\alpha \in \mathbb{C}$.

The closed sets of Spec $\mathbb{C}[x]$ are finite subsets of $\{(x-\alpha) : \alpha \in \mathbb{C}\}$. Any open set must contain (0) and all but finitely many points in $\{(x - \alpha) : \alpha \in \mathbb{C}\}$.

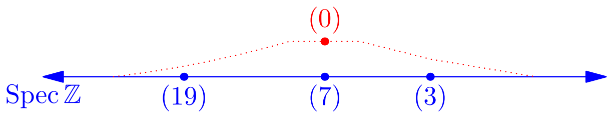


Point $[(0)]$ is more interesting. The set $\{[(0)]\}$ is not closed, but its closure is the entire Spec A.

Example 1.5.8 (Spec $\mathbb{Z}$).

Spec $\mathbb{Z}$ looks exactly the same as the above picture. The points are

- the generic point (0).
- the points (p) for prime p.



Another way to describe the topology of Spec R is by giving open set.

Proposition 1.5.9 (Distinguished open sets).

For each $f \in R$, define the **distinguished open set**

$$D(f) = \{\mathfrak{p} : f \notin \mathfrak{p}\} \subseteq \operatorname{Spec} R.$$

Then, $\{D(f) : f \in R\}$ forms a basis of topology for $\operatorname{Spec} R$. In other words, any open set of $\operatorname{Spec} R$ is a union of set of the form $D(f)$.

▶ *Proof.* Exercise. ☐

§1.5.4 Contraction and Spec Functor

We now have a map that takes a ring A to a topological space $\operatorname{Spec} A$. Now, we want to promote this to a functor. In order to do so, we need the following proposition.

Proposition 1.5.10 (Contraction of prime ideal is prime).

If A, B be rings and $\phi : A \to B$ be a homomorphism. If $\mathfrak{q} \subseteq B$ is a prime ideal, then the contraction $\phi^{-1}(\mathfrak{q})$ is prime.

▶ *Proof.* Suppose $a, b \in A$ such that $ab \in \phi^{-1}(\mathfrak{q})$. Then, $\phi(ab) \in \mathfrak{q}$, so $\phi(a)\phi(b) \in \mathfrak{q}$. Since $\mathfrak{q}$ is prime, we have that $\phi(a) \in \mathfrak{q}$ or $\phi(b) \in \mathfrak{q}$. Thus, $a \in \phi^{-1}(\mathfrak{q})$ or $b \in \phi^{-1}(\mathfrak{q})$, proving that $\phi^{-1}(\mathfrak{q})$ is prime. ☐

Remark 1.5.11.

On the other hand, contraction of maximal ideals need not be maximal ideals. For example, if $A = \mathbb{Z}$, $B = \mathbb{Q}$, ϕ is the inclusion map, and $\mathfrak{q} = (0)$, then $\phi^{-1}\mathfrak{q} = (0)$, which is not a maximal ideal. This is the reason why we prefer to include all prime ideals instead of using only maximal ideals. It is so that we can promote every ring morphism $\phi : A \to B$ to morphism of $\phi^{\#} : \operatorname{Spec} B \to \operatorname{Spec} A$.

The above proposition defines a map from $\operatorname{Spec} B \to \operatorname{Spec} A$ by $[\mathfrak{q}] \mapsto [\phi^{-1}(\mathfrak{q})]$. This induces a **contravariant functor**. In particular, given a ring morphism $\phi : A \to B$, we get a morphism $\phi^{\#} : \operatorname{Spec} B \to \operatorname{Spec} A$ of spectrum in the opposite direction.

Exercise 1.5.12. Show that $\phi^{\#}$ is continuous (with respect to Zariski topology).

Example 1.5.13.

The quotient projection map $\pi : R \to R/I$. induces the map $\pi^{\#} : \operatorname{Spec} R/I \to \operatorname{Spec} R$. Map $\pi^{\#}$ is a homeomorphism from $\operatorname{Spec} R/I$ to a closed subset $V(I)$ of $\operatorname{Spec} R$.

Exercise 1.5.14. The inclusion map $\mathbb{R}[x] \to \mathbb{C}[x]$ induces a map $\operatorname{Spec} \mathbb{C}[x] \to \operatorname{Spec} \mathbb{R}[x]$. Draw picture of $\operatorname{Spec} \mathbb{R}[x]$ and $\operatorname{Spec} \mathbb{C}[x]$ that visualizes this map.

Now, go back to Section 1.5.1 and convince yourself that the space $\operatorname{Spec} R$ substitute variety V and still makes the connection outlined in the bulleted list valid.

§1.5.5 Spec $\mathbb{Z}[x]$ and Spec $\mathbb{C}[x, y]$

We draw a picture of Spec $\mathbb{Z}[x]$ and Spec $\mathbb{C}[x, y]$. To do this, we use the following theorem that we will not prove.

Theorem 1.5.15 (Ideals of $A[y]$ where A is a PID).

Let A be a PID. Then, the prime ideals of $A[y]$ are

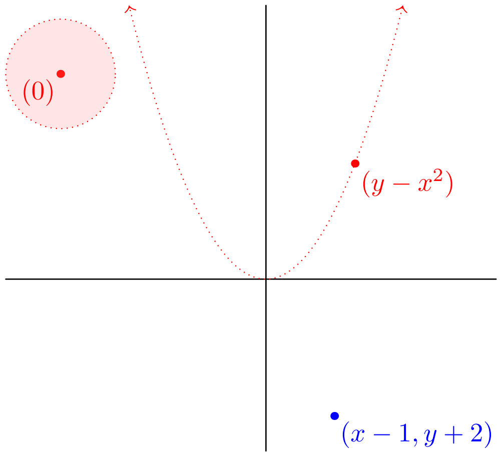
- the zero ideal (0);
- the ideal $(f(y))$, where f irreducible;
- pick a prime element $p \in A$ and $g(y) \in A[y]$ such that $\overline{g}(y) \in A/(p)[y]$ is irreducible (in field $A/(p)$), then we have $(p, g(y))$.

Only the last category is a maximal ideal.

▶ **Spec $\mathbb{C}[x, y]$** Now let's try to draw Spec $\mathbb{C}[x, y]$ (i.e., $A = \mathbb{C}[x]$). We have the ideals (0) and $(f(x, y))$ for the first two categories. For the last one, all prime elements must be in form $p = (x - \alpha)$, and $A/(p) \simeq \mathbb{C}$. Thus, an irreducible polynomial in $A/p[y] = \mathbb{C}[y]$ must be in form $y - \beta$, giving ideals $(x - \alpha, y - \beta)$ for $(\alpha, \beta) \in \mathbb{C}^2$. Therefore, Spec $\mathbb{C}[x, y]$ looks like the following:

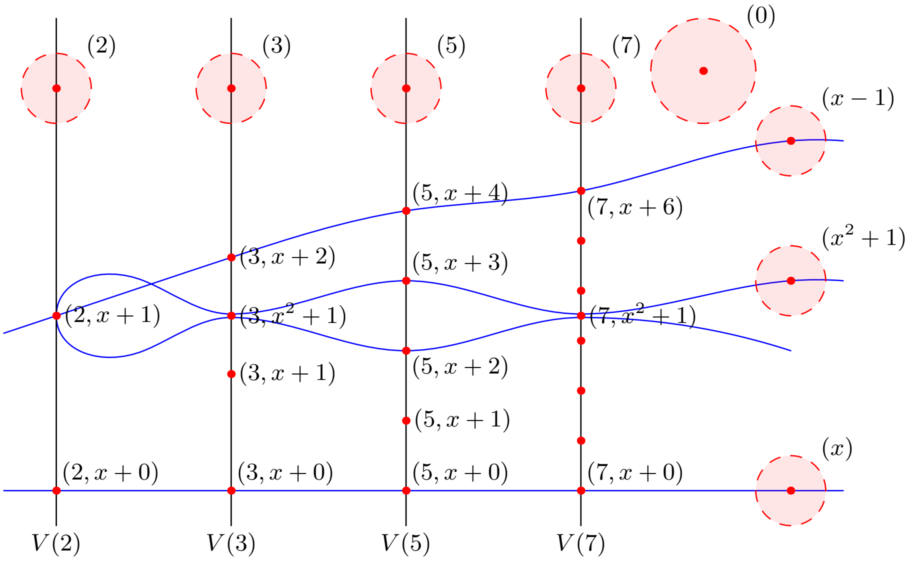
- The ideal $(x - \alpha, y - \beta)$, which form a plane $\mathbb{C}^2$.
- The ideal (f) for each irreducible $f \in \mathbb{C}[x, y]$, which will look like a cloud above the irreducible curve corresponding to .
- The generic point, which look like a cloud above everything.

Here is a picture that shows three types of points.



▶ **Spec $\mathbb{Z}[x]$** Spec $\mathbb{Z}[x]$ (i.e., $A = \mathbb{Z}$) looks pretty similar, except that the horizontal axis will be replaced by primes. The points are as follows.

- Maximal ideals, which are of the form $(p, f(x))$ where $f \in \mathbb{F}_p[x]$.
- For each irreducible polynomial $f \in \mathbb{Z}[x]$, the point (f), which is a cloud passing through $(p, \overline{f}(x))$ for each prime p.
- For each prime p, the ideal (p), which is a cloud above $(p, f(x))$ for any polynomial f.
- The generic point (0), which is a cloud above everything.



§1.6 Problems

Problem 1.A. Let A be a ring.

(a) Is it true that $I(J+K) = IJ + IK$ for all ideals I, J, K of A?

(b) Is it true that $I(J \cap K) = IJ \cap IK$ for all ideals I, J, K of A?

Problem 1.B. Let A be a ring and ideals I and J are coprime (i.e., $I + J = A$). Prove that for all positive integers m, n, ideals I^m and J^n are coprime.

Problem 1.C. Let A be a ring such that for all $x \in A$, there exists an integer $n > 1$ (possibly depending on x) such that $x^n = x$. Prove that every prime ideal of A is maximal.

Problem 1.D. Let A be a ring. Using Zorn's lemma, prove that A has a **minimal prime ideal**, a prime ideal minimal under inclusion.

Problem 1.E (Prime Avoidance, **to be used later).** Let A be a ring and $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be prime ideals. Suppose that I is an ideal contained in $\bigcup_{i=1}^n \mathfrak{p}_i$. Prove that $I \subseteq \mathfrak{p}_i$ for some i.

Problem 1.F. Let A be a ring. Prove that the following are equivalent.

(a) A has exactly one prime ideal.

(b) Every element of A is either nilpotent or a unit.

(c) $A / \operatorname{Nil} A$ is a field.

Problem 1.G. Prove that $\operatorname{Spec} A$ is quasicompact (Definition A.3.4) for any ring A.

Problem 1.H. Let A be a ring. Prove that the following are equivalent.

(a) $\operatorname{Spec} A$ is a disjoint union of two closed sets X_1 and X_2.

(b) There exists nonzero elements $e_1, e_2 \in A$ such that $e_1 + e_2 = 1$ and $e_1 e_2 = 0$.

(c) $A = A_1 \times A_2$ for some rings A_1 and A_2.

Problem 1.I. Is $\operatorname{Spec} \prod_{n=1}^{\infty} \mathbb{F}_2$ homeomorphic to the disjoint union $\coprod_{n=1}^{\infty} \operatorname{Spec} \mathbb{F}_2$?

2 Modules

There are two key reasons why we want to study modules in commutative algebra.

- Modules is an analogue of vector spaces for rings. Thus, studying modules will allow us to do linear algebras over a ring.
- Modules unify various structures in commutative algebra, including ideals I, quotient rings R/I, and their direct sum / direct product, allowing us to treat those with an equal footing.

This chapter introduces basic notions and properties of modules.

§2.1 Modules

§2.1.1 Definition and Basic Properties

Given a ring R, a **module** M is an abelian group $(M, +)$ with mutliplication by elements in R: a map $R \times M \to M$ satisfying all you would expect from a vector space:

- $a(m_1 + m_2) = am_1 + am_2$
- $a \cdot (bm) = (ab)m$.

Example 2.1.1.

- When $R = k$, a field, R-module is a k-vector space.
- When $R = \mathbb{Z}$, a $\mathbb{Z}$-module is just an abelian group.
- When $R = \mathbb{C}[x]$, an $\mathbb{C}[x]$-module is a $\mathbb{C}$-vector space associated with a linear map representing a multiplication by x.

If there is a subset $N \subset M$ preserved by addition and scalar multiplication, then N is an R-**submodule** of M.

We can also define an R-**module homomorphism** to be a map between two R-modules $\phi : M \to N$ that is a group homomorphism and $\phi(am) = a\phi(m)$.

The category of R-module is denoted R-$\mathbf{Mod}$.

§2.1.2 Constructions of Modules

We have some constructions of modules.

▶ **Quotient** For any submodule $N \subset M$, one can define the **quotient module** M/N by defining equivalence class on cosets as usual. We also have the following universal property:

For any R-module P and a map $\phi : M \to P$, such that $\phi(N) = 0$, then there exists unique ring homomorphism $\overline{\phi} : M/N \to P$ such that $\phi = \overline{\phi} \circ \pi$.

▶ **Kernel, Image, Cokernel** Given $\phi : M \to N$, then

$$\begin{array}{rrcll} \textbf{kernel} & \operatorname{Ker}\phi & := & \{m \in M : \phi(m) = 0\} & \subseteq M \\ \textbf{image} & \operatorname{Im}\phi & := & \{\phi(m) : m \in M\} & \subseteq N \\ \textbf{cokernel} & \operatorname{Coker}\phi & := & N/\operatorname{Im}\phi & \end{array}$$

are all modules. The following isomorphism theorems follow similarly from ones in group theory:

- $M/\operatorname{Ker}\phi \simeq \operatorname{Im}\phi$
- Given a chain of modules $L \subseteq M \subseteq N$, we have $(N/L)/(M/L) \simeq N/M$.

▶ **Hom** Given two modules M, N, $\operatorname{Hom}_R(M, N)$ is also a module. The operation is defined by

- $(\phi_1 + \phi_2)(m) = \phi_1(m) + \phi_2(m)$
- $(a\phi)(m) = a\phi(m)$.

When, $M = N$, there is another notation $\operatorname{End}_R(M) := \operatorname{Hom}_R(M, M)$, which is a noncommutative ring whose multiplication is given by composition.

▶ **Submodules Generated by Ideal** Given an R-module M and $I \subset R$, we can define a module

$$IM := \left\{ \sum_{i=1}^{k} a_i m_i : a_i \in I, m_i \in M \right\}.$$

▶ **Annihilator** We have the **annihilator** of an element:

$$\operatorname{Ann}(m) := \{a \in R : am = 0\}$$

and of the entire module

$$\operatorname{Ann}(M) := \{a \in R : am = 0 \text{ for all } m \in M\}.$$

▶ **Restriction of Scalar** Let $\kappa : R \to S$ be a ring homomorphism. Let N be a S-module, then we can define the **restriction of scalar**, which is an R-module ${}_R N$ (or $\operatorname{Res}_R(N)$) by using the same abelian group N and define $a \cdot n = \kappa(a) \cdot n$. This is a functor from S-**Mod** to R-**Mod**.

▶ **Direct sum and direct product** Given a collection of modules $(M_\alpha)_{\alpha\in T}$, the **direct product** (also known as **product**) is defined by

$$\prod_{\alpha \in T} M_\alpha := \{(m_\alpha)_{\alpha\in T}\}.$$

(If it is a finite collection, we write $M_1 \times M_2 \times \cdots \times M_n$.) The universal property is similar to universal property of products in Appendix A.2: if $\tau_\alpha : P \to M_\alpha$, then there exists unique $\tau : P \to \prod M_\alpha$.

The **direct sum** (also known as **coproduct**) is defined as

$$\bigoplus_{\alpha\in T} M_\alpha = \{(m_\alpha)_{\alpha\in T} : \text{ only finitely many } m_\alpha \text{ are nonzero.}\}$$

(If it is a finite collection, we write $M_1 \oplus M_2 \oplus \cdots \oplus M_n$.) Let $i_\alpha : M_\alpha \to \bigoplus M_\alpha$ be the inclusion map. Then, we have the universal property: for any $\phi_\alpha : M_\alpha \to P$, then there exists unique $\phi : \bigoplus M_\alpha \to P$ such that $\phi_\alpha = \phi \circ i_\alpha$. This is exactly the same as the universal property of product, but all arrows are reversed.

A **free** R-module is the direct sum of copies of R. We write it as $R^{\oplus n}$ for integer $n \geq 0$ or $R^{\oplus T}$ for some set T.

▶ **Generators** An R-module M is a

- **finitely-generated** (or just **finite**) if there exists a surjective map $\phi : R^{\oplus n} \to M$ for some integer $n \geq 0$.
- **finitely-presented** if the ϕ above exists and $\operatorname{Ker}\phi$ is finitely-generated.
- **cyclic** if the ϕ above exists with $n = 1$ (i.e., $M = R/I$ for some ideal I).

§2.1.3 Modules Over PID

We recall the following theorem from undergraduate algebra.

Theorem 2.1.2 (PID Structure Theorem)**.**

Let R be a PID, then every **finitely-generated** R-module M is a direct sum of cyclic modules. In particular, there exists $r \geq 0$ and $a_1, \ldots, a_n \in R$ such that

$$M \simeq R^{\oplus r} \oplus \bigoplus_{i=1}^{n} R/(a_i).$$

▶ *Proof.* At least in the case when R is a Euclidean domain, this was done in undergraduate algebra [Art11, Theorem 14.7.3]. The process of obtaining Smith normal form can be modified slightly to work on any PID. In particular, one must replace the use of Euclidean division to using the fact that for all $a, b \in R$, there exists $x, y \in R$ such that $ax + by = \gcd(a, b)$. ☐

§2.2 Cayley-Hamilton Theorem and Consequences

§2.2.1 Cayley-Hamilton Theorem

Theorem 2.2.1 (Cayley-Hamilton Theorem)**.**

Let R be a ring. Let $A = \operatorname{Mat}_{n\times n}(R) = \left(a_{ij}\right)_{1\leq i,j\leq n}$. We define the **characteristic polynomial** by

$$p_A(t) = \det(tI_n - A) = \sum_{k=0}^{n} c_k t^k.$$

Then, $p_A(A) = 0$.

▶ *Proof.* The proof is in three steps.

Step 1. $R = \mathbb{C}$ and A has distinct eigenvalues. Let the eigenvalues be $\lambda_1, \ldots, \lambda_n$ and the corresponding eigenvectors be $v_1, \ldots, v_n$. Then, since

$$p_A(t) = (t - \lambda_1)\ldots(t - \lambda_n),$$

we get that $p_A(A)v_j = 0$ for all j because the factor $A - \lambda_j$ alone is sufficient to annihilate v_j. Since $v_1, \ldots, v_n$ spans $\mathbb{C}^n$, it follows that $p_A(A)v = 0$ for all $v \in \mathbb{C}^n$, so $p_A(A) = 0$.

Step 2. $R = \mathbb{Z}[x_{11}, x_{12}, \ldots x_{nn}]$ and A is of the following form

$$A = \begin{pmatrix} x_{11} & \ldots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{n1} & \ldots & x_{nn} \end{pmatrix}.$$

To prove this, simply replace x_{ij} with a complex number so that x_{ij} are transcendentally independent.

Step 3. General R. From the above case, substitute x_{ij} with $a_{ij} \in R$, and since $p_A(A)$ vanish as polynomial ring $\mathbb{Z}[x_{11}, \ldots, x_{nn}]$, it must still vanish when plugging in x_{ij} with a_{ij}. ☐

The above proof shows a more general principle of **permanence of identities**: if one has identity that is true over $\mathbb{C}$, one can carry through the above steps to show that such identity hold for any ring.

We now explain some consequence of this theorem.

Corollary 2.2.2 (Cayley-Hamilton; module version).

Let M be a finitely-generated R-module. Let $\phi : M \to M$ be an endormorphism such that $\phi(M) \subset IM$ for some ideal $I \subset R$. Then,

$$\phi^n + c_{n-1}\phi^{n-1} + \cdots + c_1\phi + c_0 = 0,$$

for some $c_0, \dots, c_{n-1} \in I$.

▶ *Proof.* View M as a quotient of $R^{\oplus n}$ for some n. Let $e_1, \dots, e_n$ be a basis of $R^{\oplus n}$, so their reductions $\overline{e}_1, \dots, \overline{e}_n$ generates M.

We claim that there exists $a_{ij} \in I$ such that $\phi(\overline{e}_i) = \sum_{j=1}^n a_{ij}\overline{e}_{ij}$. To see this, we note that since $\phi(\overline{m}_i) \in IM$, it is a sum of elements in form im for $i \in I$ and $m \in M$. However, m is an R-linear combination of $\overline{e}_1, \dots, \overline{e}_n$, so im (and hence $\phi(\overline{m}_i)$) is an I-linear combination of $\overline{e}_1, \dots, \overline{e}_n$.

The elements $(a_{ij})_{1 \le i,j \le n}$ form a matrix $A \in \mathrm{Mat}_{n\times n}(R)$. Thus, by Cayley-Hamilton theorem (Theorem 2.2.1), we get that there exists $c_0, \dots, c_{n-1}$ such that

$$A^n + c_{n-1}A^{n-1} + \cdots + c_1A + c_0 = 0.$$

Reducing this equation into M gives

$$\phi^n + c_{n-1}\phi^{n-1} + \cdots + c_1\phi + c_0 = 0.$$

Note that $c_0, c_1, \dots, c_{n-1} \in I$ because $c_0, \dots, c_{n-1}$ come from characteristic polynomial of A, and each entry of A is in I. Hence, we are done. ☐

§2.2.2 Nakayama's Lemma

We will now use Corollary 2.2.2 to deduce an important result called **Nakayama's lemma** that will appear sporadically throughout the text. (If you don't believe me, Ctrl+F the word "Nakayama" in this file.)

Lemma 2.2.3 (Nakayama's Lemma).

Suppose that M is a finitely-generated R-module such that $IM = M$, then there exists $i \in I$ such that $im = m$ for all $m \in M$.

(Mnemonic: $IM = M$ implies $im = m$.)

▶ *Proof.* Apply the previous corollary (Corollary 2.2.2) to $\phi = \mathrm{id}_M$. Then, we have that

$$(\mathrm{id})^n + c_{n-1}(\mathrm{id})^{n-1} + \cdots + c_1(\mathrm{id}) + c_0 = 0,$$

for some $c_0, \dots, c_{n-1} \in I$. This equation simplifies to

$$(1 + c_{n-1} + \cdots + c_1 + c_0)\mathrm{id} = 0.$$

Since $c_{n-1}, c_{n-2}, \dots, c_0 \in I$, we may take $i = -(c_0 + c_1 + \cdots + c_{n-1})$. ☐

Remark 2.2.4.

The hypothesis that M is finitely-generated is necessary. A counterexample if M is not assumed to be finitely-generated is $R = \mathbb{Z}$ and $M = \mathbb{Q}$. We have $M = 5M$, but $\mathrm{Ann}(M) = 0$.

The most prominent application of Nakayama's lemma is in local ring. Recall that a ring is local iff it has a unique maximal ideal. If R is local and $y \notin \mathfrak{m}$, then $(y) = R$, so y is a unit. Thus, **if R is a local ring with maximal ideal $\mathfrak{m}$, any element not in $\mathfrak{m}$ is a unit.**

Corollary 2.2.5 (Nakayama on local ring)**.**

If M is finitely-generated R-module, where R is a local ring. Suppose that $M = \mathfrak{m}M$, then $M = 0$.

▶ *Proof.* Apply Nakayama again. There exists $a \in \mathfrak{m}$ such that $(1 + a)M = 0$. However, $1 + a$ is a unit! Hence, we are done. ☐

Let us rephrase the above corollary in to a more useful form.

Corollary 2.2.6 (Nakayama on generators)**.**

Let R be a local ring, and M be a finitely-generated R-module. Suppose that $(m_1, \dots, m_n) \in M$ such that the quotient projection $(\overline{m}_1, \dots, \overline{m}_n) \in M/\mathfrak{m}M$ span $M/\mathfrak{m}M$. Then, $(m_1, \dots, m_n)$ generate M.

▶ *Proof.* Let N be submodule generated by $m_1, \dots, m_n$. From the generation assumption, we know that $N + \mathfrak{m}M = M$, so by quotienting with N, we have $\mathfrak{m}(M/N) = M/N$, so M/N is zero. ☐

This corollary is actually very powerful. $M/\mathfrak{m}M$ is a $R/\mathfrak{m}$-module, but $R/\mathfrak{m}$ is a field, so $M/\mathfrak{m}M$ is actually a vector space, and it's then easy to check whether the generator spans. This reduces the question of generation into the world of linear algebra.

§2.3 Exactness

§2.3.1 Exact Sequences

Exact sequences is an expressive language that allows us to concisely and graphically express many statements about maps between modules. They are used more extensively in algebraic topology to manipulate a sheer number of spaces and maps, but for us, we will mostly use this as a language to state theorems.

Definition 2.3.1 (Exact sequences)**.**

The sequence of mappings

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

is **exact** iff $\operatorname{Im} f = \operatorname{Ker} g$.

Similarly, the long sequence

$$\dots \longrightarrow M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \to \dots$$

is exact at M_i iff $\operatorname{Im} f_{i-1} = \operatorname{Ker} f_i$. The whole diagram is an **exact sequence** if it is exact at all M_i's.

Now, let's give some examples.

Example 2.3.2.

We have some basic examples of exactness.

- $0 \longrightarrow L \xrightarrow{\psi} M$ is exact iff ψ is injective.
- $M \xrightarrow{\phi} N \longrightarrow 0$ is exact iff ϕ is surjective.
- $0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\phi} N$ is exact iff $L \simeq \operatorname{Ker} \phi$.
- $L \xrightarrow{\psi} M \xrightarrow{\phi} N \longrightarrow 0$ is exact iff $\operatorname{Coker} \psi \simeq N$.

Definition 2.3.3 (Short exact sequence).

A **short exact sequence** is an exact sequence of the form $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$,

Example 2.3.4 (Example of short exact sequences).

- If $R = \mathbb{Z}$, then we have
$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0.$$
- More generally, if N is a submodule of M, we have a short exact sequence
$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0.$$
- Even more generally, if $\phi : M \to N$ is a module morphism, then we have a short exact sequence
$$0 \longrightarrow \operatorname{Ker} \phi \longrightarrow M \xrightarrow{\phi} \operatorname{Im} \phi \longrightarrow 0.$$
(The map $\operatorname{Ker} \phi \longrightarrow M$ is inclusion map).
- For any modules M, N, we have the short exact sequence
$$0 \to M \to M \oplus N \to N \to 0,$$
where the former is by $m \mapsto (m, 0)$ and the latter is by $(m, n) \mapsto n$.

One source of exact sequence that we will use very late in the text is **snake lemma**.

Lemma 2.3.5 (Snake Lemma).

Suppose that there is a commutative diagram whose both rows are exact:

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r, "f"] \arrow[d, "\alpha"] & M \arrow[r, "g"] \arrow[d, "\beta"] & N \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & L' \arrow[r, "f'"'] & M' \arrow[r, "g'"'] & N' \arrow[r] & 0
\end{tikzcd}$$

Then, there is a long exact sequence

$$0 \longrightarrow \operatorname{Ker} \alpha \longrightarrow \operatorname{Ker} \beta \longrightarrow \operatorname{Ker} \gamma \xrightarrow{\delta} \operatorname{Coker} \alpha \longrightarrow \operatorname{Coker} \beta \longrightarrow \operatorname{Coker} \gamma \longrightarrow 0.$$

► *Proof Sketch.* The proof of this is a long, arduous diagram chasing with no insights required, so you do not need to understand the proof unless you really want to. In fact, I will only tell the definition of all the maps and leave the remaining checking to the (intersested) readers.

You should check yourself that all maps $\operatorname{Ker}\alpha \to \operatorname{Ker}\beta$, $\operatorname{Ker}\beta \to \operatorname{Ker}\gamma$, $\operatorname{Coker}\alpha \to \operatorname{Coker}\beta$, and $\operatorname{Coker}\beta \to \operatorname{Coker}\gamma$ are induced from f, g, f', and g', respectively. Thus, the most non-obvious map to define is $\delta : \operatorname{Ker}\gamma \to \operatorname{Coker}\alpha$.

Let $n \in \operatorname{Ker}\gamma \subseteq N$. Then, since g is surjective, pick **any** $m \in M$ such that $g(m) = n$. Now, since diagram commutes, $g'(\beta(m)) = \gamma(g(m)) = 0$, so $\beta(m) \in \operatorname{Ker} g' = \operatorname{Im} f'$, so there exists unique $\ell \in L'$ such that $f'(\ell) = \beta(m)$. We now declare $\delta(n) = [\ell]$, the class of ℓ.

We have to show that this does not depend on the choice of m. Suppose that I have another choice, say m^*. Then, $g(m - m^*) = 0$, so $m - m^* \in \operatorname{Ker} g = \operatorname{Im} f$, and so there exists $x \in L$ such that $f(x) = m - m^*$. Then, if the values of ℓ obtained from m and m^* are are ℓ and ℓ^*, respecitvely, then

$$f'(\ell - \ell^*) = \beta(m - m^*) = \beta(f(x)) = f'(\alpha(x)) \implies \ell - \ell^* = \alpha(x) \in \operatorname{Im}\alpha,$$

so ℓ and ℓ^* are mapped to the same class in $\operatorname{Coker}\alpha = L'/\operatorname{Im}\alpha$, implying that this map does not depend on the choice of m.

We omit all checks of exactness. ☐

§2.3.2 Exact Functor

In commutative algebra, the most common type of results about exact sequences is of the form whether a functor preserves exact sequence or not. We begin with a (not very important) definition.

Definition 2.3.6 (Additive Functor).

Given rings R, S. We say that a covariant functor $F : R\text{-}\mathbf{Mod} \to S\text{-}\mathbf{Mod}$ is an **additive functor** if the map $\operatorname{Hom}_R(A, B) \to \operatorname{Hom}_S(F(A), F(B))$ is an abelian group homomorphism.

Similarly, a contravariant functor $F : R\text{-}\mathbf{Mod} \to S\text{-}\mathbf{Mod}$ is an additive functor if the map $\operatorname{Hom}_R(A, B) \to \operatorname{Hom}_S(F(B), F(A))$ is an abelian group homomorphism.

Example 2.3.7.

Here are some example of additive functors.

- **The $\operatorname{Hom}_R(P, \bullet)$ functor.** Fix an R-module P, we have the covariant functor

$$\begin{aligned} \operatorname{Hom}_R(P, \bullet) : R\text{-}\mathbf{Mod} &\to R\text{-}\mathbf{Mod} \\ M &\mapsto \operatorname{Hom}_R(P, M). \end{aligned}$$

  To define the induced map, for any $\phi : M \to N$, we need to define a map $\phi_* : \operatorname{Hom}(P, M) \to \operatorname{Hom}(P, N)$. This map is simply compose by ϕ: mapping π to $\phi \circ \pi$ (so we have diagram $P \longrightarrow M \xrightarrow{\phi} N$). One can check that it is additive.

- **The $\operatorname{Hom}_R(\bullet, P)$ functor.** Similarly, we have the contravariant functor

$$\begin{aligned} \operatorname{Hom}_R(\bullet, P) : R\text{-}\mathbf{Mod} &\to R\text{-}\mathbf{Mod} \\ M &\mapsto \operatorname{Hom}_R(M, P). \end{aligned}$$

  To define the induced map, for any $\phi : M \to N$, we need to define a map $\phi^* : \operatorname{Hom}(N, P) \to \operatorname{Hom}(M, P)$. This map is simply compose by ϕ: mapping π to $\pi \circ \phi$ (so we have diagram $M \xrightarrow{\phi} N \longrightarrow P$).

- **The "Mod I" functor** For any ideal $I \subset R$, we have the covariant functor

$$\begin{aligned} F : R\text{-}\mathbf{Mod} &\to R/I\text{-}\mathbf{Mod} \\ M &\mapsto M/IM. \end{aligned}$$

  For each map $\phi : M \to N$, one can define $\phi_* : M/IM \to I/IN$ so that it commutes with quotient projection. This functor is additive.

Definition 2.3.8 (Left and right exact functors)**.**

An additive covariant functor is

- **left-exact** if for any left-exact sequence $0 \to A \to B \to C$, the sequence
$$0 \to F(A) \to F(B) \to F(C)$$
is exact.
- **right-exact** if for any right-exact sequence $A \to B \to C \to 0$, the sequence
$$F(A) \to F(B) \to F(C) \to 0$$
is exact.
- **exact** if it is both left-exact and right-exact. (In particular, it perserves injectivity, surjectivity, kernels, and cokernels.)

Similarly, an additive contravariant functor is

- **left-exact** if for any exact sequence $A \to B \to C \to 0$, the sequence $0 \to F(C) \to F(B) \to F(A)$ is exact.
- **right-exact** if for any exact sequence $0 \to A \to B \to C$, the sequence $F(C) \to F(B) \to F(A) \to 0$ is exact.
- **exact** if it is both left-exact and right-exact.

Example 2.3.9 (Trivial Examples of Exact Functors)**.**

The identity functor is exact. The functor $M \mapsto M \oplus M$ is exact.

However, being exact is generally quite a strong condition. Let us now investigate functors from Example 2.3.7.

Proposition 2.3.10.

(a) The functor $\mathrm{Hom}_R(P, \bullet)$ is left-exact (i.e., exact sequence $0 \to A \to B \to C$ gives exact sequence $0 \to \mathrm{Hom}(P, A) \to \mathrm{Hom}(P, B) \to \mathrm{Hom}(P, C)$).

(b) The functor $\mathrm{Hom}_R(\bullet, P)$ is left-exact (i.e., exact sequence $A \to B \to C \to 0$ gives exact sequence $0 \to \mathrm{Hom}(C, P) \to \mathrm{Hom}(B, P) \to \mathrm{Hom}(A, P)$).

(c) The mod-I functor is right-exact (i.e., exact sequence $A \to B \to C \to 0$ gives exact sequence $A/IA \to B/IB \to C/IC \to 0$).

▶ *Proof.* (a) Given $0 \to A \xrightarrow{\phi} B \xrightarrow{\pi} C$ is exact. We need to show that
$$0 \longrightarrow F(A) \xrightarrow{\phi_*} F(B) \xrightarrow{\pi_*} F(C)$$
is exact.

First, we show exactness at $F(A)$, i.e., ϕ_* is injective. Suppose $\phi_*(g) = \phi \circ g = 0$ for some g, then for all $p \in P$, $\phi(g(p)) = 0$. However, ϕ is injective, so $g(p) = 0$ for all $p \in P$, so $g = 0$.

Now, we show exactness at $F(B)$, i.e., $\operatorname{Im} \phi_* = \operatorname{Ker} \pi_*$. First, note that $\pi_*(\phi_*(f)) = f \circ \phi \circ \pi = 0$, so $\operatorname{Im} \phi_* \subseteq \operatorname{Ker} \pi_*$. In other direction, let $g \in \mathrm{Hom}_R(P, B)$ such that $\pi_*(g) = \pi \circ g = 0$. We want to show that $g = \phi \circ f = \phi_*(f)$ for some f. We have that for all $p \in P$, $\pi(g(p)) = 0$, so

$g(p) \in \operatorname{Ker} \pi = \operatorname{Im} \phi$. With that in mind, we can define $f(p)$ to be the (unique) preimage of $g(p)$ w.r.t. ϕ, so $\phi(f(p)) = g(p)$. It is easy to see that f is a module morphism, and then we are done.

(b) Left as an exercise.

(c) You can try to prove this now, but this is a special case of Theorem 2.5.6 that we will prove later. ☐

Exercise 2.3.11. Come up with counterexamples to show that the three functors in Proposition 2.3.10 are not exact.

It's worth noting that these proofs are particularly long and tedious, but it's pretty routine. At each step, there is only one thing you could possibly do.

One might wonder if exact functor also holds for long exact sequence. It turns out that this is the case.

Lemma 2.3.12.

Suppose F is an exact functor, then for any exact chain $L \xrightarrow{f} M \xrightarrow{g} N$, the induced map $F(L) \xrightarrow{F(f)} F(M) \xrightarrow{F(g)} F(N)$ is exact.

▶ *Proof.* We have three exact sequences, each implying a new one by applying F:

$$0 \to \operatorname{Ker} f \to L \to \operatorname{Im} f \to 0 \implies F(\operatorname{Ker} f) \to F(L) \to F(\operatorname{Im} f) \to 0 \tag{2.1}$$
$$0 \to \operatorname{Ker} g \to M \to \operatorname{Im} g \to 0 \implies 0 \to F(\operatorname{Ker} g) \to F(M) \to F(\operatorname{Im} g) \to 0 \tag{2.2}$$
$$0 \to \operatorname{Im} g \to N \to \operatorname{Coker} g \to 0 \implies 0 \to F(\operatorname{Im} g) \to F(N). \tag{2.3}$$

The first exact sequence (2.1) implies that $\operatorname{Im} F(f) = F(\operatorname{Im} f)$. On the other hand,

$$\begin{aligned} \operatorname{Ker}(F(g)) = \operatorname{Ker}(F(M) \to F(N)) &\overset{(2.3)}{=} \operatorname{Ker}(F(M) \to F(\operatorname{Im} g)) \\ &\overset{(2.2)}{=} F(\operatorname{Ker} g) = F(\operatorname{Im} f). \end{aligned}$$

Combining these two information gives exactness at $F(M)$. ☐

§2.4 Colimits

This section is only used in the proof of Chapter 10 (and only play supplementary role where it is used). It may be skipped in the first reading.

Several properties about module (such as Cayley-Hamilton theorem and its consequences in Section 2.2) requires hypothesis that the module is finitely-generated. Colimits will allow us to extend some of those facts to infinitely-generated modules.

As an example, consider

$$\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{a}{2^n} : a, n \in \mathbb{Z}\right\} \subset \mathbb{Q}.$$

This is not a finitely-generated $\mathbb{Z}$-module. However, one can write a chain of modules

$$\frac{1}{2}\mathbb{Z} \subset \frac{1}{4}\mathbb{Z} \subset \frac{1}{8}\mathbb{Z} \subset \cdots \subset \mathbb{Z}\left[\frac{1}{2}\right],$$

and one has the inclusion map

$$\frac{1}{2}\mathbb{Z} \xrightarrow{\cdot 2} \frac{1}{4}\mathbb{Z} \xrightarrow{\cdot 2} \frac{1}{8}\mathbb{Z} \xrightarrow{\cdot 2} \cdots.$$

We will now generalize this a bit by introducing a **directed system**. Throughout this section, let R be a ring.

§2.4.1 Directed System and Colimit

Definition 2.4.1 (Directed System).

Given a poset I, a **directed system** M_I of R-modules for I is given by

- for each $i \in I$, we have an R-module M_i;
- if $i \leq j$, we have $f_{ij} : M_i \to M_j$ such that if $i \leq j \leq k$, we have $f_{ik} = f_{jk} \circ f_{ij}$.

Example 2.4.2.

If $I = \mathbb{N}$ ordered by the usual $\leq$, then a directed system on I is a sequence of modules and morphism

$$M_1 \xrightarrow{f_{12}} M_2 \xrightarrow{f_{23}} M_3 \longrightarrow \ldots$$

Now, we want to take the limit of the directed system. Given a directed system M_I, we want a universal R-module M such that

- for each $i \in I$, we have $p_i : M_i \to M$.
- for each $i \leq j$, we have $p_j \circ f_{ij} = p_i$.

(i.e., we want all the arrows to be consistent).

$$\begin{tikzcd}
& & M & \\
M_i \arrow[r, "f_{ij}"'] \arrow[urr, "p_i"] & M_j \arrow[ur, "p_j"'] & & \ldots \arrow[ul]
\end{tikzcd}$$

Therefore, we are going to state this in terms of universal property.

Definition 2.4.3 (Colimit).

Given a directed system M_I we say that an R-module M is a **colimit** (or **direct limit**) if

(a) there exists $p_i : M_i \to M$ such that whenever $i \leq j$, we have $p_j \circ f_{ij} = p_i$ (i.e., everything commutes).

(b) for any R-module N and mapping $q_i : M_i \to N$ satisfying the above condition, there exists unique $\phi : M \to N$ such that $q_i = \phi \circ p_i$ for all $i \in I$.

$$\begin{tikzcd}
& & N & \\
& & M \arrow[u, "\exists!\phi"'] & \\
M_i \arrow[r, "f_{ij}"'] \arrow[urr, "p_i"] \arrow[uurr, bend left, "q_i"] & M_j \arrow[ur, "p_j"'] \arrow[uur, "q_j"] & & \ldots \arrow[ul] \arrow[uul, bend right]
\end{tikzcd}$$

and we denote it by $M := \varinjlim_{i \in I} M_i$.

Example 2.4.4.

If the poset I has no relation, then $\varinjlim M_i = \bigoplus_{i \in I} M_i$.

Let us prove that colimit exists and unique.

Proposition 2.4.5 (Colimit exists and is unique).

For each directed system M_I, $\varinjlim M_i$ exists and is unique (of course up to isomorphism).

▶ *Proof.* The uniqueness part follows the same pattern as universal property arguments, e.g., in Appendix A.2. Thus, we focus on proving existence. We start with $\bigoplus_{i\in I} M_i$. Consider the submodule $K \subset \bigoplus_{i\in I}$ generated by

$$(0, \dots, 0, m_i, \dots, -f_{ij}(m_i), 0, \dots, 0).$$

We claim that $\left(\bigoplus_{i\in I} M_i\right)/K$ works as the colimit. The map p_i is by the composition $M_i \to \bigoplus_{i\in I} M_i \to \left(\bigoplus_{i\in I} M_i\right)/K$. The commuting criterion is satisfied by the modding out by K.

Now, given N, by universal properties for direct sum, we have the map $h : \bigoplus_{i\in I} M_i \to N$. Now, the condition that $q_i = q_j \circ f_{ij}$ implies that $K \subset \operatorname{Ker} h$, so h descends to $\left(\bigoplus_{i\in I} M_i\right)/K \to N$, and we are done. ☐

Example 2.4.6 (A boring example).

Consider the directed system with two elements, and consider the directed system $M_1 \xrightarrow{f} M_2$. Then,

$$\varinjlim M_I = \frac{M_1 \oplus M_2}{(m_1, -f(m_1))} \simeq M_2$$

More generally, if I has a maximal element, then the colimit is going to be just the module at the maximum element.

Example 2.4.7 (A more interesting example).

We let $I = \mathbb{N}$ but with relation being divisibility (i.e., $i \prec j$ iff $i \mid j$). Let

$$M_i = \frac{1}{i}\mathbb{Z} \subset \mathbb{Q},$$

then one can show that $\varinjlim M_i = \mathbb{Q}$.

At the beginning, we said that the reason why we introduce colimits because we want to study any modules from finitely generated modules. Let's now make this more precise by proving that colimits actually generate all modules.

Proposition 2.4.8 (Colimit of finitely-generated submodules).

Given an R-module M, there exists a poset I and a directed system of finitely generated modules M_I such that $M = \varinjlim M_I$.

▶ *Proof.* This proof is mostly tautological. Let

$$I = \{\text{poset indexed by finitely generated submodules of } M\}.$$

Element $i \in I$ correspond to module M_i. We let $i \le j$ iff $M_i \subset M_j$, and the maps is by inclusion. Since $M_i \subset M$ and $\bigcup_{i\in I} M_i = M$, we can easily verify from universal property $\varinjlim M_i = M$. ☐

Remark 2.4.9 (Colimit indexed over a small category).

One can think of I as a category: the objects are elements of I, and there is a map $i \to j$ iff $i \le j$. In that case, a directed system M_I would be a functor from I to R-**Mod**.

Thus, one can generalize this by replacing a poset I with an arbitrary **small category** C

(a small category is a category whose a collection of objects and morphisms are both sets). A **directed system** indexed over C is a functor from C to R-**Mod**, and the colimit can be defined very similarly. It turns out that colimit still exists and is unique.

§2.4.2 Filtered Colimit Preserves Exactness

It turns out that under a mild condition on I, colimit preserves exactness. Let us make this more precise.

Definition 2.4.10.

A poset I is **filtered** if and only if any finite subset $S \subseteq I$ has an upper bound u such that $u \geq s$ for any $s \in S$.

(Equivalently, $I \neq \emptyset$ and any two elements in I has an upper bound.)

Example 2.4.11 (Filtered posets)**.**

Most posets that we are considering the colimit is filtered.

- $\mathbb{N}$ with standard $\leq$ is filtered.
- $\mathbb{N}$ with divisibility relation (cf. Example 2.4.7) is filtered; given $m, n \in \mathbb{N}$, mn is divisible by both m and n, hence an upper bound.
- The poset corresponding to colimit in Proposition 2.4.8 is filtered. This is because for any finitely-generated submodules $N_1, \ldots, N_k$, their sum $N_1 + \cdots + N_k$ is a finitely-generated submodule of M and is an upper bound of $\{N_1 \ldots, N_k\}$.

On the other hand, it is easy to come of with poset that is not filtered: take $I = \{1, 2, 3\}$ with only relation $1 \leq 2$ and $1 \leq 3$.

Definition 2.4.12 (Morphism of directed systems)**.**

Given directed system M_I and N_I, a morphism from M_I to N_I is given by $\phi_i : M_i \to N_i$ for each i such that for each $i \leq j$, the diagram

$$\begin{tikzcd}
M_i \arrow[r, "f_{ij}"] \arrow[d, "\phi_i"] & M_j \arrow[d, "\phi_j"] \\
N_i \arrow[r, "g_{ij}"] & N_j
\end{tikzcd}$$

commutes. This promotes $\varinjlim$ to a functor.

Theorem 2.4.13 (Colimit preserves exactness)**.**

Let I be a **filtered** poset. Suppose that

$$L_I \xrightarrow{\{\psi_i\}} M_I \xrightarrow{\{\phi_i\}} N_I$$

is a sequence of morphisms of directed systems such that $L_i \xrightarrow{\psi_i} M_i \xrightarrow{\phi_i} N_i$ is exact for all $i \in I$. Then, we have the exact sequence

$$\varinjlim L_I \longrightarrow \varinjlim M_I \longrightarrow \varinjlim N_I .$$

We start with the following lemma, which is where the filtered condition comes into play.

Lemma 2.4.14.

Let I be a **filtered** poset, M_I be a directed system, and $M = \varinjlim M_I$. Let $p_i : M_i \to M$ be the usual inclusion. Then,

(a) $M = \bigcup_{i \in I} p_i(M_i)$

(b) Given m_i such that $p_i(m_i) = 0$, there exists $j \geq i$ such that $p_{ij}(m_i) = 0$.

▶ *Proof.* We do each part separately.

(a) We use the construction of colimit that M is a quotient of $\bigoplus_{i \in I} M_i$. Given $m \in M$. Thus,

$$m = p_{i_1}(m_{i_1}) + \cdots + p_{i_n}(m_{i_n}) \tag{2.4}$$

for some $i_1, \ldots, i_n \in I$ and $m_{i_1} \in M_{i_1}, \ldots, m_{i_n} \in M_{i_n}$.

Pick $j \geq i_1, i_2, \ldots, i_n$. Thus, for any $\alpha \in \{1, \ldots, n\}$, we have $p_{i_\alpha}(m_{i_\alpha}) = p_j(f_{i_\alpha j}(m_{i_\alpha}))$ by commuting condition, and so each of the summand in (2.4) is in $p_j(M_j)$, implying the conclusion.

(b) Suppose that $p_i(m_i) = 0$, then in $\bigoplus_{i \in I} M_i$, we have that $m_i \in K$, where K is the submodule in the explicit construction of colimits. In particular, there exists

- $i_1, i_2, \ldots, i_n, j_1, j_2, \ldots, j_n \in I$;
- $a_1, \ldots, a_n \in R$; and
- $m_{i_1} \in M_{i_1}, m_{i_2} \in M_{i_2}, \ldots, m_{i_n} \in M_{i_n}$

such that

$$a_1(m_{i_1} - p_{i_1 j_1}(m_{i_1})) + \cdots + a_n(m_{i_n} - p_{i_n j_n}(m_{i_n})) = m_i \tag{2.5}$$

Let t be an upper bound of $i_1, \ldots, i_n, j_1, \ldots, j_n$. Thus, there is a map $M_{i_1}, \ldots, M_{i_n}, M_{j_1}, \ldots, M_{j_n} \to M_t$. By universal property of direct sum, we get a map

$$f : M_{i_1} \oplus \cdots \oplus M_{i_n} \oplus M_{j_1} \oplus \cdots \oplus M_{j_n} \to M_t.$$

Taking f on (2.5), we get that (now in M_t)

$$a_1\big(p_{i_1 t}(m_{i_1}) - p_{j_1 t}(p_{i_1 j_1}(m_{i_1}))\big) + \cdots + a_n\big(p_{i_n t}(m_{i_n}) - p_{j_n t}(p_{i_1 j_1}(m_{i_n}))\big) = p_{it}(m_i),$$

and noticing that $p_{i_k t}(m_{i_k}) = p_{j_k t}(p_{i_k j_k}(m_{i_k}))$, we see that the left hand side is zero, meaning that $p_{it}(m_i) = 0$, as desired. ☐

▶ *Proof of Theorem 2.4.13.* We use the following notations.

- Let $f_{ij} : L_i \to L_j$, $g_{ij} : M_i \to M_j$, and $h_{ij} : N_i \to N_j$ be the transition functions in the directed systems L_I, M_I, and N_I.
- Let $L = \varinjlim L_I$, $M = \varinjlim M_I$, and $N = \varinjlim N_I$.
- Let the resulting maps be $\psi : L \to M$ and $\phi : M \to N$.

It suffices to show exactness at M.

We show that $\operatorname{Ker} \psi \subseteq \operatorname{Im} \phi$ Let $m \in M$ such that $\psi(m) = 0$. By Lemma 2.4.14 (a), m is image of $m_i \in M_i$ for some i. Then, since $\psi(m) = 0$, we get that $\psi_i(m_i) = 0$. Thus, by Lemma 2.4.14 (b), there exists $j \geq i$ such that $h_{ij}(\psi_i(m_i)) = 0$. Thus, $\psi_j(g_{ij}(m_i)) = 0$.

By exactness at M_j, there exists $\ell_j \in L_j$ such that $\psi_j(\ell_j) = g_{ij}(m_i)$. Taking p_j both sides gives $p_j(\psi_j(\ell_j)) = p_j(g_{ij}(m_i))$. However, the left hand side is $\psi(p_j(\ell_j))$, while the right hand side is $p_i(m_i) = m$, so m lies in the image.

The proof that $\operatorname{Im} \phi \subseteq \operatorname{Ker} \psi$ is essentially the reverse of this argument, hence left as an exercise. ☐

§2.5 Tensor Product

Tensor product is a way to take *product* of modules. For general modules, the result is pretty strange, so let us briefly describe what happens in a simpler case of vector spaces.

Given two k-vector spaces V and W, one construct the tensor product, which is a vector space $V \otimes_k W$ by considering a big vector space generated by symbols $v \otimes w$ for each $v \in V$ and $w \in W$, modulo the following relations:

- $av \otimes w = v \otimes aw = a(v \otimes w)$ for every $a \in k$ and $v, w \in V$; and
- $(v + v') \otimes w = (v \otimes w) + (v' \otimes w)$ for every $v, v' \in V$ and $w \in W$.
- $v \otimes (w + w') = (v \otimes w) + (v \otimes w')$ for every $v \in V$ and $w, w' \in W$.

If $\{e_i\}_{i \in I}$ is a basis of V and $\{f_j\}_{j \in J}$ is a basis of W, then $V \otimes W$ has basis $\{e_i \otimes f_j : i \in I, j \in J\}$. (Proving that this set spans $V \otimes W$ is easy, but proving that this set is linearly independent requires work.) In particular, $\dim(V \otimes_k W) = (\dim V)(\dim W)$.

One can define tensor product of modules similarly to above (i.e., tensor product $M \otimes_R N$ of R-modules M and N is generated by $m \otimes n$, modulo the relations similar to above). However, this definition makes it inconvenient to deduce properties. Thus, we change tack by considering defining tensor product by a universal property. Through this, we see that tensor product tied closely with bilinear map. In particular, there is a bijective correspondence between

$$\{\text{module morphisms } M \otimes_R N \to P\} \longleftrightarrow \{\text{bilinear maps } M \otimes N \to P\}.$$

This construction takes time to get used to, but we will see various applications throughout the entire notes. The most prominent application being the ability to "change the coefficients" from e.g., $\mathbb{R}$-algebra to $\mathbb{C}$-algebra.

§2.5.1 Definition

► Bilinear maps

Definition 2.5.1 (Bilinear maps)**.**

Given modules M, N, P, the map

$$\phi : M \times N \to P$$

is **bilinear** if and only if ϕ is R-linear in each entry.

Each map

$$f_\phi : M \to \operatorname{Hom}_R(N, P)$$

induces a bilinear map

$$\begin{aligned} \phi : M \times N &\to P \\ (m, n) &\mapsto f_\phi(m)(n). \end{aligned}$$

This establishes a natural isomorphism between

$$\{\text{bilinear maps } M \times N \to P\} \longleftrightarrow \operatorname{Hom}_R(M, \operatorname{Hom}_R(N, P)). \tag{2.6}$$

► Universal property Tensor product can be thought of as a "universal module" represent those bilinear maps.

Definition 2.5.2 (Tensor products).

Given R-modules M, N, the **tensor product** $M \otimes_R N$ is an R-module T with a bilinear map $\phi : M \times N \to T$ such that for any R-module P and a bilinear map $\psi : M \times N \to P$, there exists unique module homomorphism $\pi : T \to P$ such that $\psi = \pi \circ \phi$.

$$\begin{tikzcd}
M \times N \arrow[rr, "\text{bilinear}"] \arrow[dr] & & P \\
& T \arrow[ur] &
\end{tikzcd}$$

As usual with universal properties, $M \otimes_R N$ is unique up to isomorphism. Thus, we need to prove that $M \otimes_R N$ exists.

▶ *Proof that $M \otimes_R N$ exists.* Take an enormous free module

$$F = \bigoplus_{(m,n)\in M\times N} Re_{(m,n)}.$$

We have the obvious map $M \times N \to F$. Now, we need to mod out by something to force maps to be bilinear. We let S be the submodule generated by

$$\begin{aligned}
re_{(m,n)} - e_{(rm,n)} \\
re_{(m,n)} - e_{(m,rn)} \\
e_{(m+m',n)} - e_{(m,n)} - e_{(m',n)} \\
e_{(m,n+n')} - e_{(m,n)} - e_{(m,n')}.
\end{aligned}$$

(i.e., the things we want it to be zero). Then, one can compose $M \times N \to F \to F/S$ to get $\phi : M \times N \to F/S$, which is bilinear.

Now, for any P and $\psi : M \times N \to P$ bilinear, define $\widetilde{\pi} : F \to P$ by $e_{(m,n)} = \psi(m,n)$. Notice that since ψ is bilinear, $\widetilde{\pi}$ descends to $\pi : F/S \to P$, one can take $M \otimes_R N = F/S$. ☐

We also commonly denote $m \otimes n$ to be the image of (m,n) under $M \times N \to M \otimes_R N$. From the construction above, we get that

$$\boxed{M \otimes_R N \text{ is generated by } \textbf{pure tensors } \{m \otimes n : m \in M, n \in N\}}.$$

§2.5.2 Properties of Tensor Product

As we can see in the construction, the construction of tensor products is very annoying to work with. Thus, we will prove properties of tensor product by using its universal properties instead.

Proposition 2.5.3 (Basic properties of tensor products).

Let R be a ring and M, N, P be modules.

(a) $M \otimes_R N \simeq N \otimes_R M$ (and the map is $m \otimes n \mapsto n \otimes m$).

(b) $M \otimes_R R \simeq M$ (and the map is $m \otimes r \mapsto rm$).

(c) $(M \oplus N) \otimes_R P \simeq (M \otimes_R P) \oplus (N \otimes_R P)$ (and the map is $(m+n) \otimes p \mapsto (m \otimes p) + (n \otimes p)$)

(d) $(M \otimes_R N) \otimes_R P \simeq M \otimes_R (N \otimes_R P)$ (and the map is $(m \otimes n) \otimes p \mapsto m \otimes (n \otimes p)$).

(e) $M \otimes R/I \simeq M/IM$ for all ideal $I \subseteq R$.

▶ *Proof.* The proofs below all follows the same pattern: we construct maps in both directions using universal property. This is best illustrated through the first few proofs.

(a) We have the bilinear map

$$\begin{aligned} M \times N &\to N \otimes_R M \\ (m,n) &\mapsto n \otimes m, \end{aligned}$$

so by universal property, we get a map

$$\begin{aligned} f : M \otimes_R N &\to N \otimes_R M \\ m \otimes n &\mapsto n \otimes m. \end{aligned}$$

Similarly, one can construct $g : N \otimes_R M \to M \otimes_R N$ which takes $n \otimes m$ to $m \otimes n$. Note that $f(g(m \otimes n)) = m \otimes n$, so $f \circ g$ and id coincide at pure tensors. Since $M \otimes_R N$ is generated by pure tensors, it follows that $f \circ g = \text{id}$. Similarly, $g \circ f = \text{id}$, so we are done.

(b) We have the bilinear map

$$\begin{aligned} M \times R &\to M \\ (m,r) &\mapsto rm, \end{aligned}$$

so it projects down to the map $f : M \otimes_R R \to M$ sending $m \otimes r$ to rm. In another direction, one has the map $g : M \to M \otimes_R R$ sending $m \mapsto m \otimes 1$.

To check that they are inverses, note that $f(g(m)) = f(m \otimes 1) = m$, so $f \circ g = \text{id}$. Similarly,

$$g(f(m \otimes r)) = g(rm) = rm \otimes 1 = r(m \otimes 1) = m \otimes r,$$

so $g \circ f$ and id coincide at pure tensors, implying that $g \circ f = \text{id}$.

(c) Same pattern as before. We have the bilinear map

$$\begin{aligned} (M \oplus N) \otimes_R P &\to (M \otimes_R P) \oplus (N \otimes_R P) \\ (m,n), p &\mapsto m \otimes p, n \otimes p, \end{aligned}$$

inducing a map $f : (M \oplus N) \otimes_R P \to (M \otimes_R P) \oplus (N \otimes_R P)$.

Next, we construct the map from $(M \otimes_R P) \oplus (N \otimes_R P) \to (M \oplus N) \otimes_R P$. We note that the map

$$\begin{aligned} M \times P &\to (M \oplus N) \otimes_R P \\ m, p &\mapsto (m, 0) \otimes p \end{aligned}$$

is bilinear, so it descend down to the map $M \otimes_R P \to (M \oplus N) \otimes_R P$ that takes $m \otimes p$ to $(m,0) \otimes p$. Similarly, there is a map $N \otimes_R P \to (M \oplus N) \otimes_R P$ that takes $n \otimes p$ to $(0,n) \otimes p$. Thus, we get a map

$$\begin{aligned} g : (M \otimes_R P) \oplus (N \otimes_R P) &\mapsto (M \oplus N) \otimes_R P \\ m \otimes p, n \otimes p' &\mapsto (m,0) \otimes p + (0,n) \otimes p'. \end{aligned}$$

We leave the reader to check that f and g are inverses.

(d) One can follow the same argument as above. The other way is define a symmetric triple tensor product $M \otimes_R N \otimes_R P$ by the universal property that any trilinear map $M \times N \times P \to Q$ factors through $M \otimes_R N \otimes_R P$. Then, show that $(M \otimes_R N) \otimes_R P \simeq M \otimes_R N \otimes_R P$.

(e) Define the map $M \times R/I \to M/IM$ by $(m, [a]) \mapsto [am]$. This gives a map $f : M \otimes_R R/I \to M/IM$. In other direction, consider the map $M \to M \otimes_R R/I$ by sending $m \in M$ to $m \otimes [1]$. Notice that im (for $i \in I$ and $m \in M$) is mapped to $im \otimes [1] = i(m \otimes [1]) = (m \otimes [i]) = 0$, so the map sends IM to 0, hence descends down to $g : M/IM \to M \otimes R/I$. It's easy to see that f and g are inverses. ☐

Remark 2.5.4.

(c) works with infinite direct sum: $M \otimes_R \bigoplus_{i\in I} N_i = \bigoplus_{i\in I}(M \otimes_R N_i)$.

Let's do some examples of tensor product.

Example 2.5.5 (Computing tensor products).

- $R^{\oplus n} \otimes_R M = M^{\oplus n}$ (by Proposition 2.5.3 (b) and (c)).
- In particular, $R^{\oplus m} \otimes_R R^{\oplus n} = R^{\oplus mn}$. If $\{e_1, \dots, e_m\}$ and $\{f_1, \dots, f_n\}$ are bases of $R^{\oplus m}$ and $R^{\oplus n}$, respectively, then $R^{\oplus m} \otimes_R R^{\oplus n}$ has basis $\{e_i \otimes f_j : 1 \le i \le m, 1 \le j \le n\}$. A special case of this is when $R = k$, in which we recover tensor product of vector spaces.
- We have $R/I \otimes R/J = R/(I+J)$ because by Proposition 2.5.3 (e),

$$\begin{aligned} R/I \otimes_R R/J &= (R/I) \,/\, (J(R/I)) \\ &= (R/I) \,/\, ((I+J)/I) \\ &= R/(I+J). \end{aligned}$$

- In particular, $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/\gcd(m,n)\mathbb{Z}$.
- By PID structure theorem (Theorem 2.1.2), every finitely-generated $\mathbb{Z}$-module is a direct sum of $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$. Thus, we know how to compute tensor product of any two finitely-generated $\mathbb{Z}$-modules. For example, we can compute

$$(\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z})$$

by expanding four terms and computing the direct sum of these. We get that the tensor product is

$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus 0 \oplus \mathbb{Z}/7\mathbb{Z}.$$

§2.5.3 Right Exactness of Tensor Product

Let R be a ring, and let M be an R-module. We have the functor

$$\begin{aligned} \bullet \otimes_R M : R\textbf{-Mod} &\to R\textbf{-Mod} \\ N &\mapsto N \otimes_R M. \end{aligned}$$

To define this functor, we need to, given morphism $\phi : N \to P$, define a map $N \otimes_R M \to P \otimes_R M$. To do this, we note that the map

$$\begin{aligned} N \times M &\to P \otimes_R M \\ (n, m) &\mapsto \phi(n) \otimes m \end{aligned}$$

is bilinear, and so by universal property of tensor, we get the map $\phi_* : N \otimes_R M \to P \otimes_R M$ (the map is also often denoted $\phi \otimes \mathrm{id}$) that sends $n \otimes m$ to $\phi(n) \otimes m$.

It turns out that this functor is right-exact.

Theorem 2.5.6 (Tensor is Right Exact).

Fix an R-module M, the functor $M \otimes_R \bullet$ is right-exact.

This theorem is useful in computing tensor product of quotient because given the exact sequence

$$N \xrightarrow{f} M \longrightarrow M/N \longrightarrow 0,$$

then the theorem gives the exact sequence

$$N \otimes_R P \xrightarrow{f_*} M \otimes_R P \longrightarrow M/N \otimes_R P \longrightarrow 0,$$

and so

$$M/N \otimes_R P = \operatorname{Coker} f_*.$$

Therefore, given $M \otimes_R P$ and $N \otimes_R P$, one can compute $M/N \otimes_R P$.

The idea of this proof is the following proposition.

Proposition 2.5.7 (Tensor and Hom are adjoint)**.**

For any R-modules M, N, P, we have

$$\operatorname{Hom}_R(M \otimes_R N, P) = \operatorname{Hom}_R(M, \operatorname{Hom}_R(N, P))$$

▶ *Proof.* By universal properties, there is an isomorphism between

$$\operatorname{Hom}_R(M \otimes_R N, P) \longleftrightarrow \{\text{bilinear maps } M \times N \to P\}.$$

However, from (2.6), this has a correspondence to $\operatorname{Hom}_R(M, \operatorname{Hom}_R(N, P))$. □

Lemma 2.5.8 (Converse of exactness of Hom)**.**

Let R be a ring, and let A, B, C be R-modules. Suppose that we have a sequence of maps

$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0.$$

If the sequence after applying $\operatorname{Hom}_R(\bullet, T)$ functor

$$0 \longrightarrow \operatorname{Hom}_R(C, T) \longrightarrow \operatorname{Hom}_R(B, T) \longrightarrow \operatorname{Hom}_R(A, T)$$

is exact for all R-module T, then the $A \to B \to C \to 0$ is exact.

▶ *Proof.* The proof is in three steps.

1. **$\operatorname{Im} f \subseteq \operatorname{Ker} g$.** Take $T = C$. Then, the identity map $\operatorname{id} \in \operatorname{Hom}_R(C, T)$ is sent to $\operatorname{id} \circ f \in \operatorname{Hom}_R(B, T)$ and then $\operatorname{id} \circ f \circ g \in \operatorname{Hom}_R(A, T)$, so by exactness at $\operatorname{Hom}_R(B, T)$, $\operatorname{id} \circ f \circ g = 0$, so $f \circ g = 0$, which implies $\operatorname{Im} f \subseteq \operatorname{Ker} g$.
2. **g is surjective.** We pick $T = C/\operatorname{Im} g$ and let $\pi : C \to C/T$ be the projection map. Then, note that under the map $\operatorname{Hom}_R(C, T) \to \operatorname{Hom}_R(B, T)$, element $\pi \in \operatorname{Hom}_R(C, T)$ is sent to $\pi \circ g = 0$. However, this map is injective by exactness at $\operatorname{Hom}_R(C, T)$, so $\pi = 0$, and so g is surjective.
3. **$\operatorname{Ker} g \subseteq \operatorname{Im} f$.** We set $T = B/\operatorname{Im} f$ and let $\phi : B \to T$ be the projection map. Under the map $\operatorname{Hom}_R(B, T) \to \operatorname{Hom}_R(A, T)$, element $\phi \in \operatorname{Hom}_R(B, T)$ is sent to $\phi \circ f = 0$. Thus, $\phi \in \operatorname{Ker}(\operatorname{Hom}_R(B, T) \to \operatorname{Hom}_R(A, T))$.

   By exactness at $\operatorname{Hom}_R(B, T)$, ϕ is in image from $\operatorname{Hom}_R(C, T)$. In other words, there exists $\psi : C \to B/\operatorname{Im}(f)$ such that $\psi \circ g = \phi$. Therefore, if $b \in \operatorname{Ker} g$, then $g(b) = 0$, so $\phi(b) = 0$, implying that $b \in \operatorname{Im} f$. □

Now, we are ready to prove Theorem 2.5.6

▶ *Proof of Theorem 2.5.6.* Given the exact

$$L \to N \to P \to 0,$$

we want to show that

$$M \otimes_R L \to M \otimes_R N \to M \otimes_R P \to 0$$

is exact. By Lemma 2.5.8, it suffices to show that

$$0 \to \mathrm{Hom}_R(M \otimes_R P, T) \to \mathrm{Hom}_R(M \otimes_R N, T) \to \mathrm{Hom}_R(M \otimes_R L, T)$$

is exact. However, by Tensor-Hom adjunction (Proposition 2.5.7), we have $\mathrm{Hom}_R(M \otimes_R P, T) \simeq \mathrm{Hom}_R(P, \mathrm{Hom}_R(M, T))$. Thus, it suffices to show that

$$0 \to \mathrm{Hom}_R(P, \mathrm{Hom}_R(M, T)) \to \mathrm{Hom}_R(N, \mathrm{Hom}_R(M, T)) \to \mathrm{Hom}_R(L, \mathrm{Hom}_R(M, T))$$

is exact, but this follows from $\mathrm{Hom}_R(\bullet, \mathrm{Hom}_R(M, T))$ is left-exact by Proposition 2.3.10 (a). ☐

Remark 2.5.9.

A special case of Theorem 2.5.6 is when $M = R/I$, in which case $N \mapsto N \otimes_R R/I = N/IN$, giving the mod-$I$ functor. This proves Proposition 2.3.10 (c).

▶ Flat Modules

Definition 2.5.10 (Flat modules)**.**

A module M is **flat** if $M \otimes_R \bullet$ is exact (equivalent to preserve injection).

Example 2.5.11 (Examples of flat modules)**.**

- Free modules $R^{\oplus n}$ are flat.
- More generally, $(M_i)_{i \in I}$ is flat for all i if and only if $\bigoplus_{i \in I} M_i$ is flat.
- $\mathbb{Z}/2\mathbb{Z}$-module is not a flat $\mathbb{Z}$-module because tensoring $\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}$ with $\mathbb{Z}/2\mathbb{Z}$ gives a zero map.
- More generally, any flat module is torsion-free: if M is a flat R-module, then there is no $a \in R$ that is not a zero divisor such that $am = 0$ for all $m \in M$.
- In particular, using the above bulllet point when $R = \mathbb{Z}$ and applying PID Structure theorem (Theorem 2.1.2), we deduce that every **finitely-generated** flat $\mathbb{Z}$-module is free (i.e. of the form $\mathbb{Z}^{\oplus n}$).
- However, we will prove later in Corollary 3.2.4 that $\mathbb{Q}$ is a flat $\mathbb{Z}$-module.

We will study flat modules in detail in Chapter 10.

§2.5.4 Base Change

Definition 2.5.12 (R-algebra)**.**

Given a ring R, an R-**algebra** is a ring S with homomorphism $f : R \to S$. It has the obvious R-module structure.

Let S be an R-algebra. Recall the “restriction of scalar” functor that given an S-module N, one can construct the R-module ${}_R N$ by forgetting multiplication in S. What about other direction?

In another direction, we have the following construction.

Definition 2.5.13 (Base Change)**.**

Given an R-module M, the **base change** of M to an S-module is the module $M \otimes_R S$. It has the structure of S-module, and the scalar multiplication is defined by

$$x(m \otimes y) = m \otimes xy.$$

Example 2.5.14.

If $M = \mathbb{R}^3$, $R = \mathbb{R}$, and $S = \mathbb{C}$, then $M \otimes_R S = \mathbb{C}^3$. This operation is not inverse with restriction of scalars, because if we restrict $\mathbb{C}^3$ back to $\mathbb{R}$-module, we will get $\mathbb{R}^6$ instead.

If M is an R-algebra, it turns out that you get the algebra structure as well.

Proposition 2.5.15 (Tensor product of algebras)**.**

Let R be a ring and S, T be R-algebras, then $S \otimes_R T$ is an R-algebra, and the multiplication structure is given by

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb'$$

► *Proof.* To promote an R-module to R-algebra, we need to define the multiplication map between two elements in $S \otimes_R T$. We have the map

$$\begin{aligned} (S \times T) \times (S \times T) &\to S \otimes_R T \\ a, b, a', b' &\mapsto aa' \otimes bb', \end{aligned}$$

which is bilinear in a and b (when a' and b' are fixed) and bilinear in a' and b' (when a and b are fixed). Thus, by universal property of tensor product, it descends down to the desired multiplication map. One can check that this satisfies all ring axioms (the identity is $1 \otimes 1$, and associativity, commutativity, and distributivity holds). ☐

To compute base change, we have the following useful lemmas.

Lemma 2.5.16 (Base change polynomial rings)**.**

Let S be an R-algebra. Then,

(a) We have $R[x_1, \ldots, x_n] \otimes_R S \simeq S[x_1, \ldots, x_n]$ as S-algebras.

(b) Suppose that $f_1, \ldots, f_m \in R[x_1, \ldots, x_n]$ and g_i is the image of f_i in $S[x_1, \ldots, x_n]$, then

$$\frac{R[x_1, \ldots, x_n]}{(f_1, \ldots, f_m)} \otimes_R S = \frac{S[x_1, \ldots, x_n]}{(g_1, \ldots, g_m)}$$

as S-algebras.

► *Proof.* (a) Follows the same pattern as all tensor product proofs in Proposition 2.5.3, so we will not go in full detail. In one direction, we can send $sx_1^{e_1} \cdots x_n^{e_n}$ to $s \otimes x_1^{e_1} \cdots x_n^{e_n}$. To find the inverse map, note that

$$\begin{aligned} R[x_1, \ldots, x_n] \otimes_R S &\to S[x_1, \ldots, x_n] \\ rx_1^{e_1} \cdots x_n^{e_n} \otimes s &\mapsto rsx_1^{e_1} \cdots x_n^{e_n} \end{aligned}$$

is bilinear, giving the desired inverse map by universal property of tensor.

(b) We use right-exactness of tensor product Theorem 2.5.6. Tensor

$$(f_1, \dots, f_m) \longrightarrow R[x_1, \dots, x_n] \longrightarrow \frac{R[x_1, \dots, x_n]}{(f_1, \dots, f_m)} \longrightarrow 0$$

with S to get a right-exact sequence

$$(g_1, \dots, g_m) \longrightarrow S[x_1, \dots, x_n] \longrightarrow \frac{R[x_1, \dots, x_n]}{(f_1, \dots, f_m)} \otimes_R S \longrightarrow 0,$$

which implies the result. □

Thus, for example,

$$\frac{\mathbb{R}[x,y]}{(y^3 - x^2 - 2025x)} \otimes_{\mathbb{R}} \mathbb{C} = \frac{\mathbb{C}[x,y]}{(y^3 - x^2 - 2025x)}.$$

Therefore, base change is essentially a process to change the coefficient rings to $\mathbb{C}$.

Example 2.5.17.

We have

$$\begin{aligned}
\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} &= \frac{\mathbb{R}[x]}{(x^2+1)} \otimes_{\mathbb{R}} \mathbb{C} \\
&= \frac{\mathbb{C}[x]}{(x^2+1)} && \text{(Lemma 2.5.16)} \\
&= \frac{\mathbb{C}[x]}{(x+i)} \times \frac{\mathbb{C}[x]}{(x-i)} \\
&= \mathbb{C} \times \mathbb{C}.
\end{aligned}$$

Thus, $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \times \mathbb{C}$ as $\mathbb{R}$-algebra. Can you describe the bijection explicitly?

§2.6 Problems

Problem 2.A. Let $A = \mathbb{C}[x,y]/(xy)$ and M be an A-module with generators a and b and single relation $xa + yb = 0$. Prove that M is not free.

Problem 2.B. Let $A = \mathbb{Z}[\sqrt{-5}]$ and $I = (2, 1 + \sqrt{-5})$ be an ideal. Prove that

(a) $I \oplus I \simeq A \oplus A$ (as A-modules);

(b) $I \otimes_A I \simeq A$.

See Problem 7.D for a general result.

(Recommended approach for (b): right-exactness.)

Problem 2.C. Let A be a ring and I be a finitely-generated ideal such that $I^2 = I$. Prove that there exists $x \in I$ such that $I = (x)$ and $x^2 = x$.

Problem 2.D. Let A be a local ring, and let P and Q be A-modules such that $P \oplus Q \simeq A^{\oplus n}$ for some integer $n \geq 0$. Prove that P and Q are free.

Problem 2.E. Let A be a ring and M be a finitely-generated module. Prove that any surjective map $\phi : M \to M$ is an isomorphism.

(Hint: apply Nakayama's lemma on an $A[x]$-module.)

Problem 2.F. Let R be a ring, and let P be an R-module.

(a) Prove that the following are equivalent:

  (i) For every surjective map $\phi : P \to N$, there exists a map $\psi : N \to P$ such that $\phi \circ \psi = \mathrm{id}$.
  (ii) If $0 \to M \to P \to N \to 0$ is an exact sequence, then $P \simeq M \oplus N$.
  (iii) There exists a module Q such that $P \oplus Q$ is free.
  (iv) For every surjective map of modules $\phi : M \to N$, the induced map $\phi_* : \mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, N)$ is surjective (i.e., $\mathrm{Hom}_R(P, \bullet)$ is an exact functor).

Module P is said to be **projective** if it satisfies the above (equivalent) conditions. Free modules are projective. By Problem 2.D, any finitely-generated projective modules over local ring is free. It is true, but much more difficult to prove, that any projective module over local ring is free. See [Stacks, Tag 0593] for the proof.

(b) Prove that projective modules are flat.[1]

(c) Prove that $\mathbb{Q}$ is not a projective $\mathbb{Z}$-module.

Problem 2.G. Prove that colimit commutes with tensor product. In other words, given that I is a filtered poset, $(M_i)_{i\in I}$ is a directed system of R-modules, and N is an R-module, prove that

$$\varinjlim_{i\in I}(M_i \otimes_R N) \simeq \left(\varinjlim_{i\in I} M_i\right) \otimes_R N.$$

(Recommended approach: universal property.)

Problem 2.H. Compute the following tensor products.

(a) $k[x, y] \otimes_{k[x]} k[x, y]$, as a $k[x]$-algebra.

(b) $\mathbb{Q}(\sqrt[3]{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2})$, as a $\mathbb{Q}$-algebra (for this one, answer as a product of fields).

(c) $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}$ as a $\mathbb{Z}$-module.

Problem 2.I. A rectangle is *great* if and only if it has at least one rational side length. Suppose that a rectangle R is tiled (with no overlap or empty space) by several axis-aligned great rectangles. Prove that R is great.

---

[1] Conversely, you will see in Corollary 10.2.8 that **finitely-generated** flat modules are projective.

3 Localization

In this chapter, we will discuss one of the most important construction in commutative algebra: localization. The motivation of localization is the construction of the fraction field $\operatorname{Frac} R$ from an integral domain R. We would like to generalize this construction to specify which element can and cannot be the denominator. Soon, we will quickly see that this construction allows us to "zoom into" the ring R and study them at the level of either open sets (read: $D(f)$ for $f \in R$) or points (read: prime ideals $\mathfrak{p}$). In the latter case, we get a local ring, which is usually easier to study.

§3.1 Localization of Rings

§3.1.1 Definition and Explicit Construction

We will define localization by its universal property and then construct it later.

Definition 3.1.1 (Multiplicative set)**.**

Given a ring R, a subset $S \subseteq R$ is a **multiplicative set** if and only any finite product of elements in S is in S. In particular, the empty product, 1, must be in S.

Definition 3.1.2 (Localization)**.**

Let R be a ring. Let $S \subset R$ be a multiplicative set. Then, the **localization of ring** $S^{-1}R$ is a ring with map $\phi : R \to S^{-1}R$ such that

- $\phi(s)$ is a unit for all $s \in S$.
- **Universal property.** For any R-Algebra A with map $\psi : R \to A$ such that $\psi(s)$ is a unit for all $s \in S$, the map ψ factors through $S^{-1}R$: there is a unique map $\widetilde{\psi} : S^{-1}R \to A$ such that $\psi = \widetilde{\psi} \circ \phi$.

$$\begin{tikzcd}
S \arrow[rr] & & A^{\times} \\
R \arrow[rr, "\psi"] \arrow[dr, "\phi"'] & & A \\
& S^{-1}R \arrow[ur, "\widetilde{\psi}"'] &
\end{tikzcd}$$

Theorem 3.1.3.

$S^{-1}R$ exists and is unique.

As usual with universal property, the uniqueness is automatic.

To construct localization, let the set of fractions be

$$R \times S = \left\{ \frac{a}{s} := (a, s) \right\}.$$

Of course, we have to handle something like $\frac{1}{2} = \frac{3}{6}$. We thus define an equivalence relation $\frac{a}{s} \sim \frac{b}{t}$ if and only if $at - bs = 0$. However, this is not an equivalence relation (when R is not a domain).

To salvage this, we make a slightly different construction: We say that

$$\frac{a}{s} \sim \frac{b}{t} \iff u(at - bs) = 0 \text{ for some } u \in S,$$

and one can check that this is an equivalence relation, and we may let

$$S^{-1}R = \frac{S \times R}{\sim}.$$

We may define addition and multiplication by the usual high school fraction operations:

$$\begin{aligned} \frac{a}{s} + \frac{b}{t} &= \frac{at + bs}{st} \\ \frac{a}{s} \cdot \frac{b}{t} &= \frac{ab}{st}. \end{aligned}$$

When writing this, one needs to check that it behaves well with respect to addition and multiplication. This is very tedious and hence omitted. We can also define the inclusion $R \to A$ as $\phi(a) = \frac{a}{1}$.

Proposition 3.1.4.

The construction of $S^{-1}R$ above satisfies universal property.

▶ *Proof.* Given $\psi : R \to A$ such that $\psi(s)^{-1}$ exists for all $s \in S$, one can define the map

$$\begin{aligned} \widetilde{\psi} : S^{-1}R &\to A \\ \frac{a}{s} &\mapsto \psi(a)\psi(s)^{-1}. \end{aligned}$$

One can check that this map respects the equivalence relation: if $u(at - bs) = 0$, then $\psi(a)\psi(s)^{-1} = \psi(b)\psi(t)^{-1}$. To do so, note that

$$\psi(u)\Big(\psi(a)\psi(t) - \psi(b)\psi(s)\Big) = 0,$$

and since $\psi(u)$, $\psi(t)$, $\psi(s)$ are units, one can multiply by $\psi(u)^{-1}\psi(s)^{-1}\psi(t)^{-1}$ on both sides to get that $\widetilde{\psi}$ is well-defined.

Finally, it's obvious that $\widetilde{\psi}$ satisfies the universal property. ☐

§3.1.2 Examples

Example 3.1.5 (Fraction Field).

If R is a domain and $S = R \setminus \{0\}$, then

$$S^{-1}R =: \operatorname{Frac} R$$

is a field.

For example, if $R = \mathbb{Z}$ and $S = \mathbb{Z} \setminus \{0\}$, then $\operatorname{Frac} \mathbb{Z} = S^{-1}\mathbb{Z} = \mathbb{Q}$.

Example 3.1.6 (Localization at one element)**.**

Take $R = \mathbb{C}[x]$ and $S = \{(x-1)^k : k \geq 0\}$. Then,

$$S^{-1}\mathbb{C}[x] = \left\{ \frac{g(x)}{(x-1)^k} : g \in \mathbb{C}[x] \right\}.$$

Geometrically, this ring is a ring of function defined everywhere at $\mathbb{C} \setminus \{1\}$, thus allowed to have poles at 1.

Example 3.1.7 (Two common localizations, in $\mathbb{Z}$)**.**

Take $R = \mathbb{Z}$. There are two common localization about some prime, say 5.

- Take $S = \{5^k : k \geq 0\}$, we get $\mathbb{Z}\left[\frac{1}{5}\right] \in \mathbb{Q}$.
- Take $S = \{n : 5 \nmid n\}$ to get $S^{-1}\mathbb{Z} = \mathbb{Z}_{(5)} = \left\{\frac{a}{b} : 5 \nmid b\right\}$.

Example 3.1.8 (The two most important examples of localization)**.**

Let R be a ring. Then, there are two important examples.

(a) **Localization away from f.** For any $f \in R$, take $S = \{1, f, f^2, \ldots, \}$ to get

$$S^{-1}R = R_f = R[f^{-1}] = \frac{R[x]}{(xf-1)}.$$

(b) **Localization at prime ideal $\mathfrak{p}$.** For any prime ideal $\mathfrak{p}$, take $S = R \setminus \mathfrak{p}$ to get

$$S^{-1}R = R_{\mathfrak{p}}.$$

When R is a domain and $\mathfrak{p} = (0)$, we get the fraction field.

§3.1.3 Ideals of Localization

Let's discuss how ideals behave under localization. From the map $\phi : R \to S^{-1}R$, the ideal I extends to ideal

$$S^{-1}I := \left\{ \frac{i}{s} : i \in I \right\} \subseteq S^{-1}R.$$

It turns out that every ideal of $S^{-1}R$ is of this form.

Proposition 3.1.9 (Every ideal is extended ideal)**.**

For all ideal $J \subseteq S^{-1}R$, we have $S^{-1}(\phi^{-1}(J)) = J$.

In particular, every ideal in $S^{-1}R$ is of the form $S^{-1}I$ for some ideal $I \subseteq R$.

▶ *Proof.* For all $a \in R$ and $s \in S$, each of the following is equivalent to the next.

- $\frac{a}{s} \in J$
- $\frac{a}{1} \in J$. (Proof: s is a unit in $S^{-1}R$).
- $a \in \phi^{-1}(J)$.
- $\frac{a}{s} \in S^{-1}(\phi^{-1}(J))$. □

Theorem 3.1.10 (Prime ideals of localization)**.**

Let R be a ring, S multiplicatively closed, and $\phi : R \to S^{-1}R$ be the canonical map. There is a correspondence between

$$\begin{aligned}\{\text{prime ideals of } S^{-1}R\} &\leftrightarrow \{\text{prime ideal } \mathfrak{p} \subset R \text{ such that } \mathfrak{p} \cap S = \emptyset\} \\ \mathfrak{q} &\mapsto \phi^{-1}\mathfrak{q} \\ S^{-1}\mathfrak{p} &\leftarrow\!\shortmid \mathfrak{p}.\end{aligned}$$

▶ *Proof.* The proof is in several steps.

- **The first map is well-defined.** $\phi^{-1}\mathfrak{q}$ is prime because contraction of prime ideal is prime. Moreover, $\phi^{-1}\mathfrak{q}$ does not meet S because if $s \in S$ and $s \in \phi^{-1}\mathfrak{q}$, then $\phi(s) \in \mathfrak{q}$, but $\phi(s) = \frac{s}{1}$ is a unit in $S^{-1}R$, so $\mathfrak{q} = S^{-1}R$, a contradiction.
- **The second map is well-defined.** Let $\mathfrak{p}$ be a prime ideal that does not meet S. We first show that for all $a \in R$ and $s \in S$,

  $$\tfrac{a}{s} \in S^{-1}\mathfrak{p} \iff a \in \mathfrak{p}. \tag{3.1}$$

  The direction ($\Leftarrow$) is clear. For the direction ($\Rightarrow$), suppose that $\frac{a}{s} = \frac{b}{t}$ for some $b \in \mathfrak{p}$ and $t \in S$. Then, there exists $u \in S$ such that $u(at - bs) = 0$. Reducing modulo $\mathfrak{p}$ gives $uat \in \mathfrak{p}$. However, $u, t \in S$, so they are not in $\mathfrak{p}$, so $a \in \mathfrak{p}$.

  Finally, if $\frac{a}{s}$ and $\frac{b}{t}$ are in $S^{-1}R$ such that $\frac{a}{s} \cdot \frac{b}{t} \in S^{-1}\mathfrak{p}$, then by (3.1), $ab \in \mathfrak{p}$, and so either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Thus, either $\frac{a}{s} \in S^{-1}\mathfrak{p}$ or $\frac{b}{t} \in S^{-1}\mathfrak{p}$. Hence, $S^{-1}\mathfrak{p}$ is prime.
- **For all prime $\mathfrak{q} \subseteq S^{-1}R$, we have $S^{-1}(\phi^{-1}\mathfrak{q}) = \mathfrak{q}$.** Follows from Proposition 3.1.9.
- **For all prime $\mathfrak{p} \subseteq R$ that does not meet S, we have $\phi^{-1}(S^{-1}\mathfrak{p}) = \mathfrak{p}$.** Indeed, each of the following is equivalent to the next
  - $a \in \phi^{-1}(S^{-1}\mathfrak{p})$
  - $\frac{a}{1} \in S^{-1}\mathfrak{p}$
  - $a \in \mathfrak{p}$. (by (3.1)) ☐

Recall that spectrum of a ring is the topological space of prime ideals of a ring.

Corollary 3.1.11 (Spectrum of localization away from an element)**.**

For all $f \in R$, we have

$$\operatorname{Spec} R\,[1/f] \simeq D(f) = \{\mathfrak{p} : f \notin \mathfrak{p}\},$$

which is an open subset of $\operatorname{Spec} R$.

Corollary 3.1.12 (Spectrum of localization at a prime ideal)**.**

For all prime ideal $\mathfrak{p}$, we have

(a) $\operatorname{Spec} R_{\mathfrak{p}} \simeq \{\mathfrak{q} : \mathfrak{q} \subset \mathfrak{p}\}$.

(b) $R_{\mathfrak{p}}$ is a local ring with unique maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$.

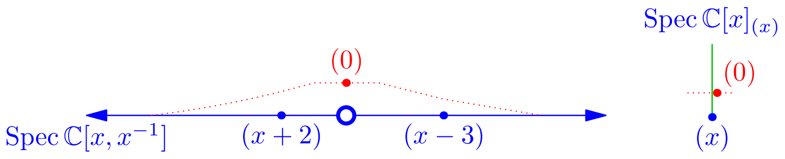
We now explain where the term localization comes from.

- $\operatorname{Spec} R[1/f]$ is the open subset $D(f)$ of $\operatorname{Spec} R$ of points where $\frac{1}{f}$ is defined. In other words, functions in $R[1/f]$ are rational functions defined on the open set $D(f)$. We are localizing **away from** points that f vanishes, and this explains why it gets the name “localization away from f”.

- In contrast, $\operatorname{Spec} R/(f)$ is $V(f)$, which is complement of $D(f)$.
- $\operatorname{Spec} R_{\mathfrak{p}}$ is the intersection of all open sets containing $\mathfrak{p}$. Thus, functions (read, elements) in $R_{\mathfrak{p}}$ corresponds to rational functions defined on some neighborhood of $\mathfrak{p}$. In particular, we are essentially zooming into just point $\mathfrak{p}$, and this is why it gets the name "localization at $\mathfrak{p}$".

To drive the point home, let us draw picture of $\operatorname{Spec} \mathbb{C}[x]_x = \operatorname{Spec} \mathbb{C}[x, x^{-1}]$ and $\operatorname{Spec} \mathbb{C}[x]_{(x)}$.

- All prime ideals of $\operatorname{Spec} \mathbb{C}[x, x^{-1}]$ are (0) and $(x - \alpha)$ for all $\alpha \in \mathbb{C} \setminus \{0\}$. Thus, it is an affine line minus point 0.
- All prime ideals of $\operatorname{Spec} \mathbb{C}[x]_{(x)}$ are (0) and (x). Thus, $\operatorname{Spec} \mathbb{C}[x]_{(x)}$ has only two points, and all closed sets are $\emptyset, \{(x)\}, \{(0), (x)\}$.


$\operatorname{Spec} \mathbb{C}[x]_{(x)}$
(0)
(0)
$\operatorname{Spec} \mathbb{C}[x, x^{-1}]$
$(x+2)$
$(x-3)$
(x)

§3.1.4 Localization Commutes with Everything

Localization commutes with everything you can ever imagine. In this subsection, we state various theorems of this sort. We omit all proofs because they are all routine. (In fact, you should be able to prove it yourself.)

As as setup, let R be a ring, S be a multiplicatively closed subset, and $\phi : R \to S^{-1}R$ be the canonical map $a \mapsto \frac{a}{1}$.

Proposition 3.1.13 (Localization Commutes with Quotient)**.**

Let I be an ideal of R and $\overline{S}$ be the image of S in R/I, then

$$\overline{S}^{-1}(R/I) = \frac{S^{-1}R}{(\phi(I))}.$$

Proposition 3.1.14 (Localization in Stages)**.**

Let T be another multiplicatively closed subset of A, and let U be the image of T in $S^{-1}R$. Then,

$$U^{-1}(S^{-1}R) = (ST)^{-1}R,$$

where $ST = \{st : s \in S, t \in T\}$.

Proposition 3.1.15 (Localization Commutes with Nilradical)**.**

We have $S^{-1}(\operatorname{Nil} R) = \operatorname{Nil}(S^{-1}R)$. In particular, if R is reduced (no nilpotent element), then so is $S^{-1}R$.

Proposition 3.1.16 (Properties Preserved by Localization)**.**

(a) If R is a domain, then $S^{-1}R$ is a domain.

(b) If R is a PID, then $S^{-1}R$ is a PID.

(c) If R is a UFD, then $S^{-1}R$ is a UFD.

§3.2 Localization of Modules

§3.2.1 Definition and Basic Properties

The easiest way to define localization of modules is to base change from R to $S^{-1}R$.

Definition 3.2.1.

Let R be a ring and S be multiplicatively closed. Then, $S^{-1}R$ is an R-algebra. Thus, one can define **localization of module** M as

$$S^{-1}M := S^{-1}R \otimes_R M.$$

This can be constructed explicitly as follows.

Proposition 3.2.2 (Explicit construction)**.**

We have

$$S^{-1}M = \frac{M \times S}{\sim},$$

where the equivalence relation $\sim$ is defined by

$$\frac{m}{s} \sim \frac{m'}{t} \quad \Longleftrightarrow \quad \text{there exists } u \in S \text{ such that } u(tm - sm') = 0.$$

▶ *Proof.* There is nothing difficult in this proof.

Let $M' = (M \times S)/\sim$ be the construction above. The map

$$\begin{aligned} S^{-1}R \times M &\to M' \\ \frac{a}{s} \times m &\mapsto \frac{am}{s} \end{aligned}$$

is bilinear, and hence descend down to the map $S^{-1}R \otimes_R M \to M'$. Clearly, this map is surjective. Now, we show that it is injective. First, we claim that every element in $S^{-1}R \otimes_R M$ can be written in form $\frac{1}{s} \otimes m$ where $s \in S$ and $m \in M$. To prove this, suppose we have one such element $x = \sum_{i=1}^{n} \frac{a_i}{s_i} \otimes m_i$. Let $s = s_1 \cdots s_n$, $t_i = \prod_{j \neq i} s_j$. Then, we can rewrite

$$x = \sum_{i=1}^{n} \frac{a_i}{s_i} \otimes m_i = \sum_{i=1}^{n} \frac{a_i t_i}{s} \otimes m_i = \sum_{i=1}^{n} \frac{1}{s} \otimes a_i t_i m_i = \frac{1}{s} \otimes \left(\sum_{i=1}^{n} a_i t_i m_i \right) = \frac{1}{s} \otimes m,$$

as claimed.

Now, suppose that $\frac{1}{s} \otimes m$ is mapped to 0. Then, $\frac{m}{s} = 0$ in M', so there exists $u \in S$ such that $um = 0$. Therefore,

$$\frac{1}{s} \otimes m = u \left(\frac{1}{us} \otimes m \right) = \frac{1}{us} \otimes um = 0,$$

implying that the map is injective. ☐

§3.2.2 Exactness

Having localized modules, one can think of localization as a functor between R-modules. This functor is automatically right-exact by Theorem 2.5.6 because it is tensoring with $S^{-1}R$. However, more is true.

Theorem 3.2.3 (Localization is exact).

The functor $S^{-1}\bullet$ defined by $M \mapsto S^{-1}M$ is exact. In other words, an exact sequence $0 \to L \to M \to N \to 0$ gives the exact sequence

$$0 \longrightarrow S^{-1}L \longrightarrow S^{-1}M \longrightarrow S^{-1}N \longrightarrow 0.$$

▶ *Proof.* From Theorem 2.5.6, it suffices to show that $S^{-1}\bullet$ preserves injectivity. Suppose $f : L \to M$ is injective. We need to show that $S^{-1}L \to S^{-1}M$ is injective. Suppose that there exist $l \in L$ and $s \in S$ such that $\frac{f(l)}{s} = 0$. This implies that there exists $t \in S$ such that $tf(l) = 0 \in M$. However, this implies that $f(tl) = 0$, so $tl = 0$, or $\frac{l}{s} = 0$, so we are done. ☐

Corollary 3.2.4 (Localization is flat).

For any ring R and any multiplicative set S, we have $S^{-1}R$ is a flat R-module.

(In particular, $\mathbb{Q}$ is a flat $\mathbb{Z}$-module.)

§3.2.3 Localization Commutes with Everything II

Let S be a multiplicative set of R.

Proposition 3.2.5 (Localization Commutes with Sum and Intersection).

If M is an R-module and N and P are submodules of M, then

(a) $S^{-1}(M/N) = S^{-1}M/S^{-1}N$.

(b) $S^{-1}(N + P) = S^{-1}N + S^{-1}P$.

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

Proposition 3.2.6 (Localization Commutes with Tensor Product and Hom).

Let M and N be R-modules, then

(a) $S^{-1}(M \otimes_R N) = S^{-1}M \otimes_{S^{-1}R} S^{-1}N$.

(b) $S^{-1}\operatorname{Hom}_R(M, N) = \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$.

§3.3 Local Properties of a Module

We will now discuss local properties, which is how properties of localization transfers to the global ring. The first one is being the zero module or not.

Proposition 3.3.1 (Being zero module is stalk-local).

Let M be an R-module. The following are equivalent.

(a) $M = 0$

(b) $M_{\mathfrak{p}} = 0$ for all prime ideal $\mathfrak{p}$.

(c) $M_{\mathfrak{m}} = 0$ for all maximal ideal $\mathfrak{m}$.

▶ *Proof.* Clearly (a) $\Rightarrow$ (b) and (b) $\Rightarrow$ (c). so we need to check that (c) $\Rightarrow$ (a).

If $M_{\mathfrak{m}} = 0$ for all maximal ideal $\mathfrak{m}$, then for each $y \in M$, we have $\frac{y}{1} = 0$ in $M_{\mathfrak{m}}$. Thus, there exists $a \notin \mathfrak{m}$ such that $ay = 0 \in M$. However, this means that $\operatorname{Ann}(y) \not\subset \mathfrak{m}$ for each $\mathfrak{m}$, so by Krull's theorem Theorem 1.3.7, $\operatorname{Ann}(y) = R$, so $y = 0$. ☐

We say that $M_{\mathfrak{p}}$ is a **stalk** of M at point $[\mathfrak{p}] \in \operatorname{Spec} R$. Thus, the previous proposition says that "$M = 0$ is a **stalk-local property**". We now discuss more stalk-local properties.

Corollary 3.3.2 (Injectivity and surjectivity is stalk-local)**.**

Let $\phi : M \to N$. Then, the following are equivalent.

(a) $\phi : M \to N$ is injective.

(b) $\phi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective for all prime ideal $\mathfrak{p}$

(c) $\phi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective for all maxmial ideal $\mathfrak{m}$.

The same statement holds when injective is replaced by surjective and isomorphism.

▶ *Proof.* Let $K = \operatorname{Ker} \phi$. Then, by exactness of localization Theorem 3.2.3, the exact sequence

$$0 \longrightarrow K \longrightarrow M \xrightarrow{\phi} N$$

gives the exact sequence

$$0 \longrightarrow K_{\mathfrak{p}} \longrightarrow M_{\mathfrak{p}} \xrightarrow{\phi_{\mathfrak{p}}} N_{\mathfrak{p}},$$

so $K_{\mathfrak{p}} = \operatorname{Ker} \phi_{\mathfrak{p}}$ for all prime ideal $\mathfrak{p}$. Therefore, (b) is equivalent to $K_{\mathfrak{p}} = 0$, while (c) is equivalent to $K_{\mathfrak{m}} = 0$. Apply Proposition 3.3.1 on K.

To prove a similar statement for surjectivity, we apply Proposition 3.3.1 on $\operatorname{Coker} \phi$ instead. ☐

The above proposition gives a good way to check whether $m_1, \dots, m_n$ generates M or not. Let $\phi : R^{\oplus n} \to M$ sending the i-th basis element to m_i. With knowledge of localization, we have that

$$\begin{aligned} m_1, \dots, m_n \text{ generates } M &\iff \phi \text{ is surjective} \\ &\iff \phi_{\mathfrak{m}} \text{ is surjective for all } \mathfrak{m} \\ &\iff \frac{m_1}{1}, \dots, \frac{m_n}{1} \text{ generate } M_{\mathfrak{m}} \\ &\iff \overline{m_1}, \dots, \overline{m_n} \text{ generate } M_{\mathfrak{m}}/\mathfrak{m}M_{\mathfrak{m}}, \end{aligned}$$

where the last step follows from Nakayama's lemma Corollary 2.2.5. This is a convenient procedure to check if something generates the module because the last thing is a vector space.

Now, let's discuss some more local properties.

Corollary 3.3.3 (Reduced is stalk-local)**.**

R is reduced if and only if $R_{\mathfrak{m}}$ is reduced for all maximal ideals $\mathfrak{m}$.

▶ *Proof.* Apply Proposition 3.3.1 to $\operatorname{Nil}(R)$, noting that localization commutes with nilradical Proposition 3.1.15 ☐

Proposition 3.3.4 (Flatness is stalk-local)**.**

For any module M, M is flat if and only if $M_{\mathfrak{m}}$ is flat for all maximal ideal $\mathfrak{m}$.

▶ *Proof.* The left-to-right direction is easy. We prove that the last implies the first. Given an injective map $L \to N$, then $L_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective. Thus, we get the injective map

$$M_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} L_{\mathfrak{m}} \to M_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} N_{\mathfrak{m}}.$$

However, from the lemma above, we have that both sides are isomorphic to

$$(M \otimes_R L)_{\mathfrak{m}} \to (M \otimes_R N)_{\mathfrak{m}}.$$

Then, since injectivity is local property, we get an injective map $M \otimes_R L \to M \otimes_R N$. All the maps are natural, so we get the same map as what we wanted. ☐

We have seen many stalk-local properties. However, not all properties are stalk-local.

Example 3.3.5 (Finitely-generated is not stalk-local)**.**

Being finitely-generated is not a stalk-local property. For example, let $R = \mathbb{Z}$ and

$$M = \tfrac{1}{2}\mathbb{Z} + \tfrac{1}{3}\mathbb{Z} + \tfrac{1}{5}\mathbb{Z} + \tfrac{1}{7}\mathbb{Z} + \dots \subseteq \mathbb{Q}$$

(the sum runs through primes). Then, for any prime p, $M_{(p)} = \frac{1}{p}\mathbb{Z}_{(p)}$. Thus, $M_{\mathfrak{m}}$ is finitely-generated for all maximal ideal $\mathfrak{m}$. However, one can check that M is not finitely-generated.

§3.4 Locally Free Modules

§3.4.1 Definition and Examples

Definition 3.4.1.

Let A be a ring. A module M is **locally free** if for every prime ideal $\mathfrak{p}$, the localization $M_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module.

A module M is locally free of **rank** r if for every prime ideal $\mathfrak{p}$, $M_{\mathfrak{p}} \simeq A_{\mathfrak{p}}^{\oplus r}$.

Locally free modules are interesting for two reasons.

- They are a natural setting to do multilinear algebra (e.g., tensor product, wedge product, dual, trace, determinant).
- They encompass a much larger class of examples than free modules. For example, if K is an algebraic extension of $\mathbb{Q}$ and $\mathcal{O}_K$ is the ring of integer, then any ideal of $\mathcal{O}_K$ is a locally free $\mathcal{O}_K$-module of rank 1. This will follow from results in Chapter 7.

Consequently, linear algebra over locally free modules are used in number theory to define norm, traces, discriminants, etc. For the rest of this section, we introduce how to do linear algebra over locally free module.

We do one example that we can simply calculate explicitly.

Example 3.4.2.

Let $A = \mathbb{Z}[\sqrt{-5}]$ and $I = (2, 1+\sqrt{-5})$. We show that I is locally free. To do this, we observe the following.

- If $f_1 = 2$, then I_{f_1} is locally free because 2 is a unit in A_{f_1}, so I_{f_1} is a unit ideal.
- If $f_2 = 3$, then I_{f_2} is locally free because $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, and since 3 is a unit, it follows that 2 is divisible by $1+\sqrt{-5}$ in R_{f_2}, so I_{f_2} is generated by $1+\sqrt{-5}$.

For every prime ideal $\mathfrak{p}$, either $2 \notin \mathfrak{p}$ or $3 \notin \mathfrak{p}$, so $I_{\mathfrak{p}} \simeq A_{\mathfrak{p}}$ for all prime ideal $\mathfrak{p}$.

§3.4.2 Linear Algebra on Locally Free Modules

Properties of Hom and tensor that carries over from vector spaces (or free modules) do carry over to locally free modules. An example is given below.

Theorem 3.4.3 (Linear algebra on locally free modules I).

Let P and Q be finitely-generated locally free A-modules.

(a) $P \otimes_A Q$ and $\operatorname{Hom}(P, Q)$ are finitely-generated locally free modules.

(b) If $R^\vee = \operatorname{Hom}(R, A)$ for all locally free module R, then $(P^\vee)^\vee \simeq P$.

(c) For any module M, $\operatorname{Hom}(P, M) \simeq P^\vee \otimes_A M$.

▶ *Proof.* (a) Note that for every prime ideal $\mathfrak{p}$, $(P \otimes_A Q)_{\mathfrak{p}} \simeq P_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} Q_{\mathfrak{p}}$ (by Proposition 3.2.6) is free because it is a tensor product of free modules. Similar reason goes for $\operatorname{Hom}(P, Q)$.

(b) We have a canonical map $P \to (P^\vee)^\vee$ given by

$$\begin{aligned} \phi : P &\to (P^\vee)^\vee \\ m &\mapsto (f \mapsto f(m)). \end{aligned}$$

By Corollary 3.3.2, to show that this is an isomorphism, it suffices to show that $\phi_{\mathfrak{p}} : (P_{\mathfrak{p}}^\vee)^\vee \to P_{\mathfrak{p}}$ is an isomorphism for all prime ideal $\mathfrak{p}$. Thus, it suffices to prove that ϕ is an isomorphism for all finitely-generated free modules P, i.e., $P \simeq A^{\oplus r}$.

To do this, let $e_1, \ldots, e_r$ be the basis. Then, observe that

- $f_1, \ldots, f_r$ is a basis of $P^\vee$, where $f_i(e_j)$ is equal to 1 if $i = j$ and 0 otherwise.
- $g_1, \ldots, g_r$ is a basis of $(P^\vee)^\vee$ where $g_i(f_j)$ is equal to 1 if $i = j$ and 0 otherwise.

It is then easy to see that $g_i = \phi(e_i)$, so ϕ is surjective, hence an isomorphism.

(c) Again, we have the canonical map in one direction

$$\begin{aligned} \phi : P^\vee \otimes_A M &\to \operatorname{Hom}(P, M) \\ f \otimes m &\mapsto (n \mapsto m f(n)). \end{aligned}$$

By the same argument as (b), it suffices to check that this is an isomorphism for the case when P is a finitely-generated free module. One can do this by computing the basis explicitly, similar to above. ☐

We can even define determinants on locally free module. First, let us recall the abstract definition of determinants.

Definition 3.4.4 (Exterior power).

Let A be a ring and M be an A-module. A bilinear pairing $\psi : M^n \to P$ is an **alternating pairing** if $\psi(x_1, \ldots, x_n) = 0$ whenever two of x_i and x_j are equal.

The n-th **exterior power** is the module $\bigwedge^n M$ with an alternating pairing $\phi : M^n \to \bigwedge^n M$ such that any alternating pairing $\psi : M^n \to P$ factor through ψ:

$$\begin{tikzcd}
M^n \arrow[rr, "\psi"] \arrow[dr, "\phi"'] & & P \\
& \bigwedge^n M \arrow[ur] &
\end{tikzcd}$$

The explicit construction of exterior power is as follows:

$$\bigwedge^n M = \frac{M^{\otimes n}}{\langle \cdots \otimes m \otimes \cdots \otimes m \otimes \cdots = 0 \text{ for all } m \in M \rangle},$$

and the image of $(m_1, \dots, m_n)$ under the inclusion is denoted $m_1 \wedge \cdots \wedge m_n$.

Observe that since $(x+y) \wedge (x+y) = x \wedge x = y \wedge y = 0$, we get by expanding $(x+y) \wedge (x+y)$ that

$$(x \wedge x) + (x \wedge y) + (y \wedge x) + (y \wedge y) = 0 \implies x \wedge y = -(y \wedge x).$$

(i.e., wedges anticommute).

$\bigwedge^n$ is a functor. Given a morphism of modules $\phi : M \to N$, we have the morphism

$$\begin{gathered}\bigwedge^n \phi : \bigwedge^n M \to \bigwedge^n N \\ (m_1 \wedge \cdots \wedge m_n) \mapsto (\phi(m_1) \wedge \cdots \wedge \phi(m_n)).\end{gathered}$$

Definition 3.4.5 (Determinant).

If P is a locally free module of rank r, then the **determinant** of P is the top exterior power $\det P := \bigwedge^r P$, which will be a locally free module of rank 1.

Example 3.4.6.

Suppose that $P = A^{\oplus 2}$, with basis e_1 and e_2. Let $\phi : P \to P$ such that $\phi(e_1) = ae_1 + be_2$ and $\phi(e_2) = ce_1 + de_2$. Then, the map $\bigwedge^2 \phi$ sends $e_1 \wedge e_2$ to

$$\begin{aligned}(ae_1 + be_2) \wedge (ce_1 + de_2) &= ac(e_1 \wedge e_1) + ad(e_1 \wedge e_2) + bc(e_2 \wedge e_1) + bd(e_2 \wedge e_2) \\ &= ad(e_1 \wedge e_2) + bc(e_2 \wedge e_1) \\ &= (ad - bc)(e_1 \wedge e_2).\end{aligned}$$

Thus, the map is multiplication by determinant $ad - bc$.

If P is a free A-module, then any linear map $\phi : P \to P$ will induce a scalar multiplication on $\det P \to \det P$, and this scalar is simply the determinant corresponding to matrix representing ϕ. However, if P is only locally free, then $\det P$ can be any locally free module of rank 1.

Many properties of determinants in linear algebra carry over and can be proven simply by reducing to free modules.

Theorem 3.4.7 (Linear algebra on locally free modules II).

Let A be a ring.

(a) If P and Q are locally free A-modules of rank r, then $\phi : P \to Q$ is an isomorphism if and only if $\bigwedge^r \phi : \det P \to \det Q$ is an isomorphism.

(This is an analogue of theorem of linear algebra that a matrix is invertible if and only if the determinant is nonzero.)

(b) If P and Q are locally free A-modules of rank p and q, then

$$\det(P \oplus Q) \simeq (\det P) \otimes (\det Q).$$

▶ *Proof.* One can quickly reduce to the case where P and Q are free. (For (b), one needs to provide the obvious map in one direction.) We leave this as an exercise to the reader. ☐

§3.5 Problems

Problem 3.A. Construct a ring $R \neq 0$ such that $R_\mathfrak{p}$ is a domain for all prime ideals $\mathfrak{p}$ but R is not a domain.

Problem 3.B. Let R be a ring and $\mathfrak{p}$ be a prime ideal of R that is minimal under inclusion. Prove that every element of $\mathfrak{p}$ is a zero divisor.

Problem 3.C. (a) Is the maximal ideal of the local ring $(\mathbb{C}[x,y]/(y^2 - x^3 - x))_{(x,y)}$ principal?

(b) Is the maximal ideal of the local ring $(\mathbb{C}[x,y]/(y^2 - x^3 - x^2))_{(x,y)}$ principal?

In both parts, we are localizing at maximal ideal (x, y).

(Hint: look at $\mathfrak{m}/\mathfrak{m}^2$.)

Problem 3.D. Let A be a domain and $K = \operatorname{Frac} A$. The **rank** of an A-module M is defined as $\operatorname{rank}_A(M) = \dim_K(M \otimes_A K)$.

(a) What is the rank of the $\mathbb{Z}$-module $\mathbb{Z}^3 \oplus \mathbb{Z}/12 \oplus \mathbb{Z}/4$?

(b) If there is an exact sequence of A-modules

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow \dots \longrightarrow M_n \longrightarrow 0,$$

prove that $\sum_{i=1}^n (-1)^i \operatorname{rank}_A(M_i) = 0$.

Problem 3.E. Let R be a ring, and let M be a **finitely-presented** module.

(a) Prove that if $\mathfrak{p}$ is a prime ideal such that $M_\mathfrak{p}$ is free, then there exists $f \notin \mathfrak{p}$ such that M_f is free.[1]

(b) Deduce that the following are equivalent.

- $M_\mathfrak{m}$ is free for all maximal ideals $\mathfrak{m}$.
- $M_\mathfrak{p}$ is free for all prime ideals $\mathfrak{p}$.
- There exists $f_1, \dots, f_n \in R$ generating a unit ideal such that M_{f_i} is free for all $i = 1, 2, \dots, n$.

Problem 3.F (Gluing)**.** Let A be a ring, and let $f_1, \dots, f_n \in A$ generating a unit ideal. For each i, let $g_i \in A_{f_i}$ such that for all $i, j \in 1, 2, \dots, n$, g_i and g_j map to the same element in $A_{f_i f_j}$. Prove that there exists an element $g \in A$ such that g maps to $g_i \in A_{f_i}$ for each $i \in 1, 2, \dots, n$.[2]

Hint: use the fact that $f_1^N, f_2^N, \dots, f_n^N$ generate the unit ideal.

Problem 3.G. Prove that locally free modules are projective (defined in Problem 2.F).

(Hint: check condition (ii). Use Problem 3.F.)

---

[1] Geometric interpretation: free over point $\mathfrak{p}$ implies free over open neighborhood $D(f) \ni \mathfrak{p}$.

[2] This is an algebraic analogue of the following topological fact: given an open cover $U_1, \dots, U_n$ of a topological space X and functions $f_i : U_i \to Y$ such that $f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U j}$ for all i, j, there exists a function $f : X \to Y$ such that $f|_{U_i} = f_i$.

4 Integral Extensions

In this chapter, we study a integral dependence (being a root of monic polynomial), which is a fundamental notion that unifies different meanings in number theory and algebraic geometry.

- In number theory, this is used to define algebraic integer, an analogue of $\mathbb{Z}$ when the fraction field $\mathbb{Q}$ is replaced with a finite extension.
- In algebraic geometry, this is related to (ramified) covering maps and resolving singularities of codimension 1.

We will explore various applications, especially in algebraic geometry.

- First, we will prove Hilbert Nullstellensatz (Theorem 4.4.5), which classifies all maximal ideals of $\mathbb{C}[x_1, \ldots, x_n]$ as promised in the first chapter.
- Second, in Section 4.5, we will explore how to define **dimension** of varieties and prove some basic properties using tools we have so far (although we will give a more robust treatment of dimension again in Chapter 9).

§4.1 Integral Elements

📋 **Definition 4.1.1** (Integral Elements)**.**

Let $A \subset B$ be ring. We say that an element $b \in B$ is **integral** over A if b is a root of monic polynomial

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

where $a_i \in A$.

If A and B are fields, then the above definition is equivalent to that b is algebraic over A.

In the number-theoretic world, if K is a number field (finite extension of $\mathbb{Q}$), then the integral elements in K form the **ring of integers** $\mathcal{O}_K$, which is an analogue of integers. For example, if $K = \mathbb{Q}(\sqrt{-3})$, we have $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.

We will now give a clean characterization of integrality. To do so, we give the following intermediate definition.

📋 **Definition 4.1.2.**

Given $b \in B$, define the subring generated by b by $A[b]$ being the smallest subring of B containing b.

Now, we state the theorem.

Theorem 4.1.3 (Characterization of Integral Elements)**.**

The following are equivalent.

(a) b is integral over A.

(b) $A[b]$ is finitely-generated A-module.

(c) There exists a ring C, which is a finitely-generated A-module, such that $A \subset C \subset B$ and $b \in C$.

As an example, $\frac{1}{3} \in \mathbb{Q}$, but $\mathbb{Z}\left[\frac{1}{3}\right]$ is not finitely-generated as $\mathbb{Z}$-module since $\frac{1}{3}$ is not integral.

▶ *Proof.* **(a) $\Rightarrow$ (b).** Let b is integral over a, meaning that for some $a_0, \ldots, a_{n-1} \in A$, we have $b^n + a_{n-1}b^{n-1} + \cdots + b_0 = 0$. This means that $b^n \in \operatorname{Span}(b^{n-1}, \ldots, b, 1)$. Now, notice that

$$b^k \in \operatorname{Span}(b^{n-1}, \ldots, b, 1) \implies b^{k+1} \in \operatorname{Span}(b^n, \ldots, b^2, b) \subset \operatorname{Span}(b^{n-1}, \ldots, b, 1),$$

so by induction, $b^k \in \operatorname{Span}(b^{n-1}, \ldots, b, 1)$, so $A[b]$ is generated by $b^{n-1}, \ldots, b, 1$, done.

(b) $\Rightarrow$ (c). Take $C = A[b]$.

(c) $\Rightarrow$ (a). The multiplication by b (in C) can be represented as a matrix $T \in \operatorname{Mat}_m(A)$. By Cayley-Hamilton theorem, $p_T = 0$, where p_T is a characteristic polynomial of T. Thus, we have $p_T(1) = 0$, so writing coefficients out gives $b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$, as desired. ☐

Corollary 4.1.4 (Integral elements form a subring)**.**

Let $A \subset B$ be rings. Then,

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

is a subring of B

▶ *Proof.* It suffices to show that A' is closed under addition and multiplication. Let $r, s \in A'$, so by condition (b) in Theorem 4.1.3, we get that $A[r]$ and $A[s]$ are finitely-generated. We have to show that $r + s$ and rs are integral over A.

To do this, we use condition (c) in Theorem 4.1.3. Since $A[r]$ and $A[s]$ are finitely-generated, we get that $A[r] \otimes_A A[s]$ is finitely-generated. However, there is a surjective map $A[r] \otimes_A A[s] \to A[r, s]$, so $A[r, s]$ is finitely-generated.

Since $r + s$ and rs are both in $A[r, s]$, condition (c) is satisfied, so both $r + s$ and rs are integral over A, and we are done. ☐

Remark 4.1.5.

It is tempting to argue the following: $A[r + s] \subseteq A[r, s]$, so $A[r + s]$ is finitely-generated, so condition (b) in Theorem 4.1.3 apply.

This is incorrect because submodule of finitely-generated modules is not necessarily finitely-generated (but this would work if we assume that A is Noetherian though). This is why we have to develop condition (c) in Theorem 4.1.3.

§4.2 Integral Extension and Closure

§4.2.1 Definition

Definition 4.2.1 (Integral extension).

Let A be a ring. We say that ring $B \supseteq A$ is an **integral extension** if every element $b \in B$ is integral over A.

Similarly (but less-frequently used), the map $\phi : A \to B$ is **integral** if $\phi(A) \subset B$ is an integral extension.

Example 4.2.2.

- $\mathbb{Z}[\sqrt{-3}]$ is an integral extension of $\mathbb{Z}$ because $\sqrt{-3}$ is integral in $\mathbb{Z}$ (it is a root of x^2+3).
- $\mathbb{C}[t]$ is an integral extension of $\mathbb{C}[t^2]$ because t is a root of polynomial $x^2 - t^2$.

Definition 4.2.3 (Integral closure and integrally closed).

Let $A \subset B$. Then, the ring $\overline{A}$ of all integral elements in B is called the **integral closure** of A inside B.

If $\overline{A} = A$, then A is **integrally closed** inside B.

In the definition above, when A is a domain and B is omitted, we mean $B = \operatorname{Frac} A$. In other words, a domain A is **integrally closed** (or **normal**) if and only if A is integrally closed inside $\operatorname{Frac} A$.

Let's do some example.

Example 4.2.4 ($\mathbb{Z}$ is integrally closed).

$\mathbb{Z}$ is integrally closed (over $\mathbb{Q}$). To see why, pick $\frac{r}{s} \in \mathbb{Q}$ integral over $\mathbb{Z}$ where , i.e.,

$$\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1\left(\frac{r}{s}\right) + a_0 = 0$$

for $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$. By dividing out common factor, assume $\gcd(r, s) = 1$. Multiplying by s^n both sides gives

$$r^n = -a_{n-1}r^{n-1}s + \cdots + a_1 r s^{n-1} + a_0 s^n$$

Then, s divides the right hand side, so $s \mid r^n$, so $s = \pm 1$, implying that $\frac{r}{s} \in \mathbb{Z}$.

The argument in the above example generalizes directly to the following.

Proposition 4.2.5.

UFD is integrally closed.

Thus, for example, $\mathbb{Z}[i]$ and $\mathbb{C}[x_1, \ldots, x_n]$ is integrally closed.

Let's see how integral closure can break in both number-theoretic and geometric world. First, let's do an NT example.

Example 4.2.6 (Non-example in NT)**.**

$\mathbb{Z}[\sqrt{-3}]$ is not integrally closed since $\frac{1+\sqrt{-3}}{2}$ is integral. Thus, by Proposition 4.2.5 $\mathbb{Z}[\sqrt{-3}]$ is not a UFD.

More generally, for any number field K, any UFD subring of K must consists of only integral elements, and so it must be contained in the ring of integral element $\mathcal{O}_K$. We will show later by Corollary 4.2.12 that $\mathcal{O}_K$ is integrally closed. This is one reason why $\mathcal{O}_K$ is of a special interest in algebraic number theory.

Now, let's see how integral closure breaks in geometric world.

Example 4.2.7 (Non-example in AG)**.**

We let

$$A = \frac{\mathbb{C}[x,y]}{(y^2 - x^3)},$$

the coordinate ring of a cuspidal curve. Let $u = \frac{y}{x} \in \operatorname{Frac} A$. We have $u^2 = \frac{y^2}{x^2} = \frac{x^3}{x^2} = x$, so u is in the integral closure.

Now, we consider the map

$$\begin{aligned} A &\to \mathbb{C}[u] \\ x &\mapsto u^2 \\ y &\mapsto u^3 \end{aligned}$$

This map is well-defined and is injective, so $A = \mathbb{C}[u^2, u^3]$. We then see that $\mathbb{C}[u]$ is an integral closure.

Geometrically, we have $A \hookrightarrow \mathbb{C}[u]$, inducing a map $\operatorname{Spec} \mathbb{C}[u] \to \operatorname{Spec} A$. We have $\operatorname{Spec} \mathbb{C}[u]$ is a line, but $\operatorname{Spec} A$ is a non-smooth curve with a cusp at $(0,0)$. Thus, essentially, integral closure is a process of making a ring smoother.

This process holds for not just $y^2 = x^3$, but for any "one-dimensional" complex varieties (i.e., curves). The coordinate ring of a variety is integrally closed if and only if the curve is a smooth manifold. If the curve is not smooth, then taking integral closure resolves singularity by *straightening* the curve. What's surprising is that this process is canonical, which is a special property of one-dimensional rings. In higher dimension, it is much more difficult to resolve singularities, and often there are choices involved. In Chapter 7, we will see how being integrally closed is connected to smoothness.

§4.2.2 Basic Properties

We now start to present properties of integral extension. Before that, we make a remark about finitely-generated algebras.

Definition 4.2.8 (Finitely-generated vs. finite)**.**

Given a ring homomorphism $\phi : A \to B$. We say that

- B is a **finitely-generated** (or **finite-type**) A-algebra if and only if there is a surjection from $A[t_1, \ldots, t_n] \to B$.
- B is a **finite** A-algebra if and only if B is finitely-generated as A-module.

Warning 4.2.9.

Don't confuse between finitely-generated and finite. For example, polynomial ring $A[x]$ is a finitely-generated A-algebra but not a finite A-algebra.

Corollary 4.2.10.

Let B be an A-algebra. Suppose that B is finitely-generated as A-algebra and is integral over A, then B is finitely-generated as an A-module.

▶ *Proof.* Follows directly from Theorem 4.1.3. ☐

▶ Tower of Integral Elements

Proposition 4.2.11 (Integrality is transitive)**.**

Let $A \subset B \subset C$. Suppose B is integral over A and C is integral over B, then C is integral over A.

▶ *Proof.* Let $\gamma \in C$. Then, for some $b_0, \ldots, b_{n-1} \in B$, we have $\gamma^n + b_{n-1}\gamma^{n-1} + \cdots + b_1\gamma + b_0 = 0$. Let $B' = A[b_0, \ldots, b_{n-1}]$, which is a finitely-generated A-algebra, so by Corollary 4.2.10, it is a finitely-generated A-module. Since $B'[\gamma]$ is a finitely-generated B'-module, it is a finitely-generated A-module, so by Theorem 4.1.3 ((c) implies (a)), γ is integral over A. ☐

Corollary 4.2.12 (Integral closure is integrally-closed)**.**

Let $A \subset B$ be rings. If $\overline{A}$ is an integral closure of A inside B, then $\overline{A}$ is integrally closed already.

▶ *Proof.* If $\gamma \in B$ is integral over $\overline{A}$, then by the proposition above, γ is integral over A, so $\gamma \in \overline{A}$. ☐

▶ Integral Closure vs. Quotient and Localization

Proposition 4.2.13 (Integral extension is preserved under quotient and localization)**.**

Let $A \subseteq B$ be rings such that B is integral over A.

(a) If J is an ideal of B and $I = J \cap A$, then B/J is integral over A/I.

(b) If $S \subset A$ be multiplicatively closed, then $S^{-1}B$ is integral over $S^{-1}A$.

▶ *Proof.* (a) Any $b \in B$ satisfies the relation $b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$ for some $a_0, a_1, \ldots, a_{n-1} \in A$. Now reduce this equation modulo J.

(b) Note that $\frac{b}{s} = \frac{1}{s} \cdot b$, and we have $\frac{1}{s}$ and $\frac{b}{1}$ are both integral over $S^{-1}A$. ☐

Proposition 4.2.14 (Localization preserves integral closure)**.**

Let $A \subseteq B$ be rings, and let C be the integral closure of A in B (so $A \subseteq C \subseteq B$). Then, $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.

▶ *Proof.* By Proposition 4.2.13 (b), we see that every element in $S^{-1}C$ is integral over $S^{-1}B$. Conversely, if $\frac{b}{s} \in S^{-1}B$ is integral in $S^{-1}A$, then we have the equation in form

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s_{n-1}}\left(\frac{b}{s}\right)^n + \cdots + \frac{a_1}{s_1}\left(\frac{b}{s}\right) + \frac{a_0}{s_0} = 0,$$

where $a_0, \ldots, a_{n-1} \in A$ and $s_0, \ldots, s_{n-1} \in S$. Let $t = s_0 \cdots s_{n-1}$. Then, multiplying this equation by $(ts)^n$ gives

$$(bt)^n + c_{n-1}(bt)^{n-1} + \cdots + c_1(bt) + c_0 = 0$$

for some $c_0, \ldots, c_{n-1} \in A$. This shows that $bt \in C$, so $b/s = bt/st \in S^{-1}C$. ☐

Finally, we note that being integrally closed is a stalk-local property.

Proposition 4.2.15 (Being integrally closed is stalk-local)**.**

If A is a **domain**, then the following are equivalent.

(a) A is integrally closed.

(b) $A_{\mathfrak{p}}$ is integrally closed for all prime ideal $\mathfrak{p}$.

(c) $A_{\mathfrak{m}}$ is integrally closed for all maximal ideal $\mathfrak{m}$.

▶ *Proof.* Proposition 4.2.14 gives that (a) implies (b), and clearly, (b) implies (c). Thus, it suffices to prove that (c) implies (a).

Assume (c). Let B be the integral closure of A, and let $\phi : A \to B$ be the inclusion map. Then, by Proposition 4.2.14, $B_{\mathfrak{m}}$ is the integral closure of $A_{\mathfrak{m}}$, so the map $\phi_{\mathfrak{m}} : A_{\mathfrak{m}} \to B_{\mathfrak{m}}$ is surjective for all maximal ideals $\mathfrak{m}$. Since being surjective is local (Corollary 3.3.2), we get that ϕ is surjective, so $A = B$. ☐

▶ **The Minimal Polynomial Test** Verifying that α is not integral over A would be difficult since we need to examine all possible monic polynomials vanishing at α. Fortunately, with favorable condition, we only need to examine the minimal polynomial.

Lemma 4.2.16 (Minimal Polynomial Test)**.**

Let A be an integrally-closed domain. Let $K = \mathrm{Frac}(A)$, and let L be a field extension of K. Let $\alpha \in L$, and let $f(x) \in K[x]$ be the monic minimal polynomial of α over K.

Then, α is integral over A if and only if $f(x) \in A[x]$.

▶ *Proof.* If $f(x) \in A[x]$, then α is clearly integral over A by definition.

In another direction, let $g(x) \in A[x]$ be a monic polynomial such that $g(\alpha) = 0$. Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ be roots of f in $\overline{K}$. Thus, since f divides g in $K[x]$, α_i must also be a root of g, and hence integral over A. Therefore, each coefficient of polynomial

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

is a sum of products of α_i, and hence integral over A. However, A is integrally closed, so all coefficients are in A, or $f \in A[x]$. ☐

Example 4.2.17.

Using the above Lemma 4.2.16 with $A = \mathbb{Z}$ and $K = \mathbb{Q}$, we can see that $\frac{1+\sqrt{3}}{2}$ is not integral over $\mathbb{Z}[\sqrt{3}]$ because the minimal polynomial $x^2 - x - \frac{1}{2}$ does not have integer coefficients.

Exercise 4.2.18. Let d be a squarefree integer. Prove that the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ is

$$\begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2,3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod 4). \end{cases}$$

§4.3 Cohen-Seidenberg Theory

Cohen-Seidenberg theory is a series of theorems that control prime ideals in an integral extensions, making them useful in algebraic geometry. In this section, we describe and prove those.

§4.3.1 Going-up Theorem

► **Lying Over** First, let us define a new terminology.

Definition 4.3.1 (Lies over).

Consider an integral extension $A \subset B$. A prime ideal $\mathfrak{q} \subset B$ **lies over** a prime ideal $\mathfrak{p} \subset A$ if and only if $\mathfrak{p} = \mathfrak{q} \cap A$.

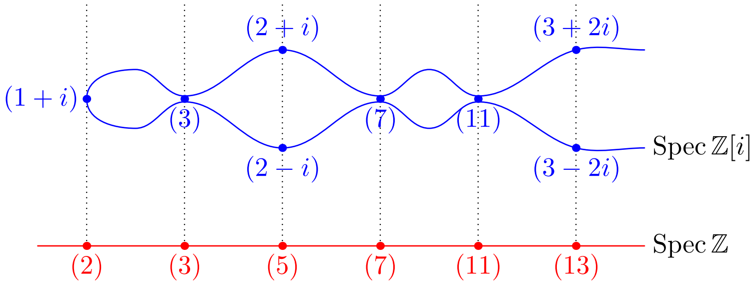
Another interpretation: the inclusion map $\phi : A \hookrightarrow B$ induces the map on spectrum $\phi^\# : \operatorname{Spec} B \to \operatorname{Spec} A$ taking $\mathfrak{q}$ to $\mathfrak{q} \cap A$. Thus, $\mathfrak{q}$ lies over $\mathfrak{p}$ if $\phi^\# \mathfrak{q} = \mathfrak{p}$.

Example 4.3.2 (Gaussian integers).

If $A = \mathbb{Z}$ and $B = \mathbb{Z}[i]$, then

- $(3) \subseteq \mathbb{Z}[i]$ is the only prime lying over $(3) \subseteq \mathbb{Z}$.
- $(2+i)$ and $(2-i)$ are two primes lying over $(5) \subseteq \mathbb{Z}$.

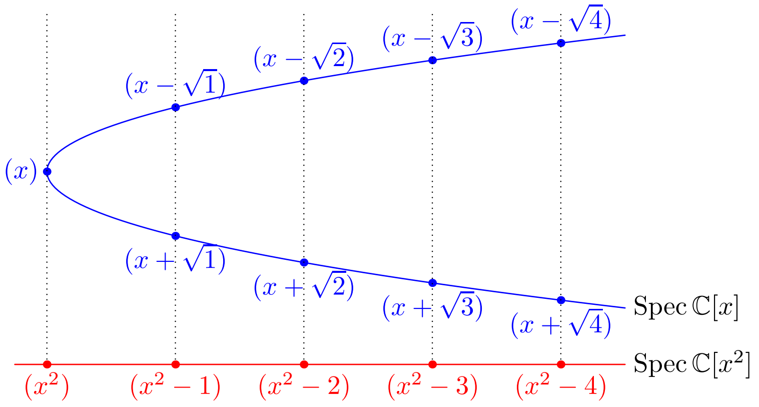
The map $\operatorname{Spec} \mathbb{Z}[i] \to \operatorname{Spec} \mathbb{Z}$ looks like a *double cover*, as in the following diagram



Example 4.3.3.

Suppose that $A = \mathbb{C}[t^2]$ and $B = \mathbb{C}[t]$. Then, the map $\operatorname{Spec} \mathbb{C}[t] \to \operatorname{Spec} \mathbb{C}[t^2]$ takes prime ideal $(t-a)$ to prime ideal $(t^2 - a^2)$. This map correspond to the morphism on affine line $\mathbb{C} \to \mathbb{C}$ that sends a to a^2.

Visually, the map $\operatorname{Spec} \mathbb{C}[t] \to \operatorname{Spec} \mathbb{C}[t^2]$ looks like a double cover map, ramified at 0, as in the following diagram.



Informally, if B is an integral extension of A, then the map Spec $B \to$ Spec A looks like a ramified covering map. The algebraic results that explain this are the following theorems.

▶ **Key Results** We will now state three imporant theorems.

Theorem 4.3.4 (Lying Over).

Let $A \subset B$ be an integral extension. For any prime $\mathfrak{p} \subset A$, there exists a prime ideal $\mathfrak{q} \subset B$ lying over $\mathfrak{p}$.

$$\begin{tikzcd}
\mathfrak{q} \arrow[d, dash, dashed] & \subset & B \arrow[d, dash] \\
\mathfrak{p} & \subset & A
\end{tikzcd}$$

(In other words, the map Spec $B \to$ Spec A is surjective.)

Theorem 4.3.5 (Incomparability).

Let $A \subseteq B$ be an integral extension, $\mathfrak{p} \subset A$ be a prime ideal. If $\mathfrak{q} \subseteq \mathfrak{q}'$ be two prime ideals lying over $\mathfrak{p}$, then $\mathfrak{q} = \mathfrak{q}'$.

Theorem 4.3.6 (Going-up).

Let $A \subseteq B$ such that B is an integral extension of A. Given two prime ideals $\mathfrak{p} \subset \mathfrak{p}' \subset A$, and another prime ideal $\mathfrak{q} \subset B$ such that $\mathfrak{q} \cap A = \mathfrak{p}$. Then, there is another prime ideal $\mathfrak{q}'$ such that $\mathfrak{q} \subset \mathfrak{q}' \subset B$ and $\mathfrak{q}' \cap A = \mathfrak{p}'$.

$$\begin{tikzcd}
\mathfrak{q} \arrow[d, dash] & \subset & \mathfrak{q}' \arrow[d, dash, dashed] & \subset & B \arrow[d, dash] \\
\mathfrak{p} & \subset & \mathfrak{p}' & \subset & A
\end{tikzcd}$$

Exercise 4.3.7 (Morphism version of the above theorems). Let $\phi : A \to B$ be an integral morphism. Using the above theorems, prove the following.

(a) For any prime ideal $\mathfrak{p} \subset A$, prove that there exists a prime ideal $\mathfrak{q} \subset B$ such that $\phi^{-1}\mathfrak{q} = \mathfrak{p}$.

(b) Given two primes ideal $\mathfrak{p} \subset \mathfrak{p}' \subset A$ and another prime ideal $\mathfrak{q} \subset B$ such that $\phi^{-1}\mathfrak{q} = \mathfrak{p}$, prove that there exists a prime ideal $\mathfrak{q}'$ such that $\mathfrak{q} \subset \mathfrak{q}' \subset B$ and $\phi^{-1}\mathfrak{q}' = \mathfrak{p}'$.

✍ **Exercise 4.3.8.** Deduce from going-up theorem that if $\phi : A \to B$ is integral map, then $\phi^{\#} : \operatorname{Spec} B \to \operatorname{Spec} A$ is a **closed map** (i.e., image of closed sets is closed).

▶ **Proof** The rest of this subsection is devoted to proving two theorems. To prove these theorems, we start with a very special case when B is a field.

Lemma 4.3.9 (The field case)**.**

Let $A \subseteq B$ such that A and B are domains and B is an integral extension of A. Then, A is a field if and only if B is a field.

▶ *Proof.* (⇒) Let $b \in B$. There exists $c_0, \ldots, c_{n-1} \in A$ such that

$$b^n + c_{n-1}b^{n-1} + \cdots + c_1 b + c_0 = 0.$$

We may assume $c_0 \neq 0$ because otherwise, one can divide out by b (this requires the fact that B is a domain). Since A is a field, there exists $d \in A$ such that $dc_0 = 1$. Then, we have

$$b \cdot -d(b^{n-1} + c_{n-1}b^{n-2} + \cdots + c_2 b + c_1) = 1,$$

giving the inverse of b.

(⇐) Let $a \in A$. Since B is a field, we have $a^{-1} \in B$. Thus, for some $c_0, \ldots, c_{n-1} \in A$, we have

$$(a^{-1})^n + c_{n-1}(a^{-1})^{n-1} + \cdots + c_1 a^{-1} + c_0 = 0$$

Multiplying by a^n both sides gives

$$\begin{aligned} 1 + c_{n-1}a + \cdots + c_1 a^{n-1} + c_0 a^n &= 0 \\ 1 - a \cdot (\text{fluff}) &= 0, \end{aligned}$$

and this fluff will be the inverse of a. ☐

Believe it or not, by solving a very specific case, we actually have half of the work done. The strategy is to use quotient and localization to reduce the theorem down to the above lemma.

Corollary 4.3.10 (The maximal ideal case)**.**

Let $A \subseteq B$ be integral, $\mathfrak{p} \subset A$ be a prime ideal, and $\mathfrak{q}$ lies over $\mathfrak{p}$. Then, $\mathfrak{q}$ is maximal if and only if $\mathfrak{p}$ is maximal.

▶ *Proof.* Since integral closure is preserved under quotient (Proposition 4.2.13 (a)), $B/\mathfrak{q}$ is an integral extension of $A/\mathfrak{p}$. Thus, by the field case (Lemma 4.3.9), $B/\mathfrak{q}$ is a field if and only if $A/\mathfrak{p}$ is a field. This implies the result. ☐

Now, we can prove the main theorems.

▶ *Proof of Lying Over Theorem 4.3.4.* We use localization. As above, let $S = A \setminus \mathfrak{p}$ and $B_{\mathfrak{p}} = S^{-1}B$ and $B_{\mathfrak{p}}$ is integral over $A_{\mathfrak{p}}$ by Proposition 4.2.13 (b). Then, let $\mathfrak{m}$ be maximal ideal in $B_{\mathfrak{p}}$. By the maximal ideal case Corollary 4.3.10, $\mathfrak{m} \cap A_{\mathfrak{p}}$ must be (the only) maximal ideal in $A_{\mathfrak{p}}$, which is be $\mathfrak{p}A_{\mathfrak{p}}$. Thus, $\mathfrak{m} \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$, so taking intersection to A both sides gives $\mathfrak{m} \cap A = \mathfrak{p}$. Hence, $\mathfrak{m} \cap B$ is our desired ideal $\mathfrak{q}$. ☐

▶ *Proof of Incomparability Theorem 4.3.5.* We use localization. Let $S = A \setminus \mathfrak{p}$ and let $B_{\mathfrak{p}} = S^{-1}B$. Then, by Proposition 4.2.13 (b), we get an integral extension $A_{\mathfrak{p}} \subset B_{\mathfrak{p}}$. Now, if $\mathfrak{q} \subset \mathfrak{q}'$, then we extend to $B_{\mathfrak{p}}$ to get $\mathfrak{q}B_{\mathfrak{p}} \subseteq \mathfrak{q}'B_{\mathfrak{p}}$.

Now, the magic happens, since $\mathfrak{p}A_{\mathfrak{p}}$ is a maximal ideal in $A_{\mathfrak{p}}$, we get by the maximal ideal case (Corollary 4.3.10) that $\mathfrak{q}B_{\mathfrak{p}}$ is a maximal ideal in $B_{\mathfrak{p}}$. This forces $\mathfrak{q}B_{\mathfrak{p}} = \mathfrak{q}'B_{\mathfrak{p}}$ or $\mathfrak{q} = \mathfrak{q}'$, done. ☐

▶ *Proof of Going Up Theorem 4.3.6.* We use quotient again. Since $\mathfrak{q}$ lies over $\mathfrak{p}$, we have by Proposition 4.2.13 (a) that $A/\mathfrak{p} \subset B/\mathfrak{q}$ is integral. Thus, by lying over Theorem 4.3.4, pick prime ideal $\overline{\mathfrak{q}'} \subset B/\mathfrak{q}$ lying over $\overline{\mathfrak{p}'} \subset A/\mathfrak{p}$. By correspondence theorem, we have $\mathfrak{p} \subset \mathfrak{p}'$ and $\mathfrak{q} \subset \mathfrak{q}'$. Moreover, the lying over condition $\overline{\mathfrak{q}'} \cap A = \overline{\mathfrak{p}'}$ directly translates to $\mathfrak{q}' \cap A = \mathfrak{p}'$, so we are done. ☐

§4.3.2 Going-down Theorem

We will now state a similar result. However, it will require additional assumption that

- B is a domain.
- A is integrally closed (any integral element in fraction is in A)

Theorem 4.3.11 (Going-down)**.**

Let $A \subset B$ be domains such that A integrally closed and B is integral over A. Given that $\mathfrak{p} \subset \mathfrak{p}' \subset A$ be prime ideals and $\mathfrak{q}'$ lies over $\mathfrak{p}'$, then there exists a prime ideal $\mathfrak{q} \subset \mathfrak{q}'$ lying over $\mathfrak{p}$.

$$\begin{tikzcd}
\mathfrak{q} \arrow[d, dash, dashed] \arrow[r, phantom, "\subset"] & \mathfrak{q}' \arrow[d, dash] \arrow[r, phantom, "\subset"] & B \arrow[d, dash] \\
\mathfrak{p} \arrow[r, phantom, "\subset"] & \mathfrak{p}' \arrow[r, phantom, "\subset"] & A
\end{tikzcd}$$

To prove this theorem, we begin with a small lemma that allows us to find ideals.

Lemma 4.3.12 (Lying Over Criterion)**.**

Let $R \subset R'$ be a ring extension (not necessarily integral!). For any prime ideal $\mathfrak{p} \subset R$ the following are equivalent:

(a) There exists a prime ideal $\mathfrak{p}' \subset R'$ such that $\mathfrak{p}' \cap R = \mathfrak{p}$.

(b) $\mathfrak{p}R' \cap R = \mathfrak{p}$.

▶ *Proof.* We first prove that (a) implies (b). To do this, we note that $\mathfrak{p}R' \subseteq \mathfrak{p}'$, so

$$\mathfrak{p} \subseteq \mathfrak{p}R' \cap R \subseteq \mathfrak{p}' \cap R = \mathfrak{p},$$

so all equalities occur, implying that $\mathfrak{p}R' \cap R = \mathfrak{p}$.

Next, we prove that (b) implies (a). The strategy is that we want prime ideal that does not meet $R \setminus \mathfrak{p}$, so we invert that set. Localize R' with multiplicative set $S = R \setminus \mathfrak{p}$ to get $R_{\mathfrak{p}}$. Then, $\mathfrak{p}R' \cap S = (\mathfrak{p}R' \cap R) \setminus \mathfrak{p} = \emptyset$ (by assumption (b)). Thus, $\mathfrak{p}R'_{\mathfrak{p}}$ is a proper ideal of $R'_{\mathfrak{p}}$, and hence contained in a maximal ideal $\mathfrak{m} \subseteq R'_{\mathfrak{p}}$. By Theorem 3.1.10, $\mathfrak{m}$ must be in form $\mathfrak{p}'R'_{\mathfrak{p}}$ for some prime ideal $\mathfrak{p}' \subset R'$ such that $\mathfrak{p}' \cap (R \setminus \mathfrak{p}) \neq \emptyset$. Since $\mathfrak{p}R'_{\mathfrak{p}} \subset \mathfrak{m}$, it follows that $\mathfrak{p} \subset \mathfrak{p}'$. Combining previous two sentences gives $\mathfrak{p}' \cap R = \mathfrak{p}$. ☐

▶ *Proof of Going Down Theorem 4.3.11.* First, we claim that it suffices to show

$$\mathfrak{p}B_{\mathfrak{q}'} \cap A = \mathfrak{p}.$$

Indeed, assume that this is true, then by Lemma 4.3.12 we there is a prime ideal of $B_{\mathfrak{q}'}$ lying above $\mathfrak{p}A_{\mathfrak{p}}$, which must be of the form $\mathfrak{q}B_{\mathfrak{q}'}$ for some prime ideal $\mathfrak{q} \subseteq \mathfrak{q}'$ by Theorem 3.1.10. Since $\mathfrak{q}B_{\mathfrak{q}'}$ contracts to $\mathfrak{p} \subset A$, it follows that $\mathfrak{q} \subset B$ contracts to $\mathfrak{p} \subset A$.

Now, we prove that $\mathfrak{p}B_{\mathfrak{q}'} \cap A = \mathfrak{p}$. One containment $\mathfrak{p} \subset \mathfrak{p}B_{\mathfrak{q}'} \cap A$ is automatic. Thus, suppose $a = \mathfrak{p}B_{\mathfrak{q}'} \cap A$ but $a \notin \mathfrak{p}$. Then, $a = \frac{b}{s}$, where $b \in \mathfrak{p}B$ and $s \notin \mathfrak{q}'$. The proof proceeds in four steps.

1. **There exists polynomial $F(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0$ such that $c_0, \ldots, c_{n-1} \in \mathfrak{p}$ and $F(b) = 0$.** The fact that $b \in \mathfrak{p}B$ means that b can be written as a linear combination $b = \sum_{i=1}^m x_i p_i$, where $x_i \in B$ and $p_i \in \mathfrak{p}$.

   Set $A' = A\langle x_1, \ldots, x_m\rangle \subset B$ to be a finitely-generated submodule of B. We have $bA' \subset \mathfrak{p}A'$, so by Cayley-Hamilton theorem Corollary 2.2.2, there exists polynomial

   $$F(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0, \quad c_i \in \mathfrak{p}$$

   such that $F(b) = 0$.

2. **The minimal polynomial $G(X) = X^m + d_{m-1}X^{m-1} + \cdots + d_1X + d_0$ of b satisfies $d_0, \ldots, d_{m-1} \in \mathfrak{p}$.** Let G be such minimal polynomial, so by the minimal polynomial test (Lemma 4.2.16), we get that $G(X) \in A[x]$. Since $G(X)$ divides $F(X)$ in $K[X]$ and both polynoimals are monic, we get that the quotient must be in $A[x]$, so $F(X) = G(X)H(X)$ for some $H(X) \in A[X]$.

   Now, we reduce modulo $\mathfrak{p}$. We get $X^n = \overline{G}(X)\overline{H}(X)$ in $A/\mathfrak{p}[x]$. Thus, $\overline{G}(X) = X^m$, so all other coefficients in G vanish modulo $\mathfrak{p}$.

3. **$d_i/a^{n-i} \in A$ for all $i = 0, 1, \ldots, n-1$.** The minimal polynomial F of b can be translated to minimal polynomial of $s = \frac{b}{a}$ by

   $$\left(\frac{b}{a}\right)^n + \frac{d_{n-1}}{a}\left(\frac{b}{a}\right)^{n-1} + \cdots + \frac{d_0}{a^n} = 0. \tag{4.1}$$

   Thus, by the minimal polynomal test (Lemma 4.2.16), we get that all coefficients of this polynomial must be in A, or $d_i/a^{n-i} \in A$ for all $i = 0, 1, \ldots, n-1$.

4. **Conclusion.** Let $e_i = d_i/a^{n-i}$. We have $d_i \in \mathfrak{p}$ from Step 2. However, $a \notin \mathfrak{p}$, so we have $e_i \in \mathfrak{p}$.

   Finally, we note that $\mathfrak{p} \subset \mathfrak{q}'$, so $e_i \in \mathfrak{q}'$ for all i. Thus, $e_i s^i \in \mathfrak{q}'$ for all i. However, from (4.1), we have $s^n + e_{n-1}s^{n-1} + \cdots + e_1 s + e_0 = 0$. All terms except s^n are in $\mathfrak{q}'$, so $s^n \in \mathfrak{q}'$, and so $s \in \mathfrak{q}'$, a contradiction. ☐

§4.4 Noether Normalization and Nullstellensatz

In this section, we discuss Noether Normalization Lemma, an important source of integral extension that can be obtained from any ring in form $k[x_1, \ldots, x_n]/\mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal. We will then use it to prove Hilbert's Nullstellensatz.

§4.4.1 Noether Normalization

Theorem 4.4.1 (Noether Normalization Lemma)**.**

Let k be a field, and let B be a finitely-generated k-algebra. In other words, $B = k[y_1, \ldots, y_n]/I$ for some ideal I. Then, there exists $x_1, \ldots, x_m \in B$ such that

- The subring $A \subset B$ generated by $x_1, \ldots, x_m$ is isomorphic to the polynomial ring $k[x_1, \ldots, x_m]$ (i.e., $x_1, \ldots, x_m$ are algebraically independent).
- B is an integral extension of A.

In particular, the theorem states that "any finitely-generated k-algebra is an integral extension of polynomial ring $k[T_1, \ldots, T_m]$." Geometrically, this means that any variety is a finite cover of the affine space k^m.

Before proving this theorem, we provide some example of why this theorem is intuitive, but not completely obvious.

Example 4.4.2.

Consider

$$B = \frac{k[x, y]}{(xy - 1)}.$$

Let's randomly take $A = k[x]$, but this doesn't work. In particular, recall that by Lying Over Theorem 4.3.4 that if B is an integral extension of A, then $\operatorname{Spec} B \to \operatorname{Spec} A$ is a surjection, but this map clearly misses zero (i.e., ideal (x)).

Thus, to fix this, we want to perturb A a little bit. In this case, we see that $A = k[x+\delta y]$ for any $\delta \neq 0 \in k$ works. To see why, if $z = x+\delta y$, then we have the relation $(z-\delta y)y = 0$, which gives a monic polynomial that y is a root. Similarly, $(z - x)x = 0$, giving a monic polynomial that x is a root.

The following proof of this theorem is due to Nagata.

▶ *Proof.* We use induction on n. The base case $n = 0$ is obvious. Thus, assume that the statement is true for $n - 1$. If $I = (0)$, then we are immediately done.

The strategy is that we will find $z_1, \ldots, z_{n-1} \in B$ such that $y_1, \ldots, y_n$ are all integral over ring $k[z_1, \ldots, z_{n-1}]/J$, which is the subring of B generated by $z_1, \ldots, z_{n-1}$ with relations being ideal J. If we managed to do that, then we would have a chain of ring extension

$$A = k[x_1, \ldots, x_m] \overset{\text{integral}}{\subset} \frac{k[z_1, \ldots, z_{n-1}]}{J} \overset{\text{integral}}{\subset} \frac{k[y_1, \ldots, y_n]}{I} = B,$$

where the first inclusion is integral extension by applying induction hypothesis on $k[z_1, \ldots, z_{m-1}]/J$. Thus, by Proposition 4.2.11, we get B is an integral extension of A as desired.

We now establish such $z_1, \ldots, z_{n-1}$. Select any nonzero $f \in I$. We pick $z_i = y_i - y_n^{r_i}$ where $r_1 \gg r_2 \gg \cdots \gg r_{m-1} \gg 0$ (large enough so that $r_i \gg (\deg f) r_{i-1}$).

$$f(z_1 + y_n^{r_1}, z_2 + y_n^{r_2}, \ldots, z_{n-1} + y_n^{r_{n-1}}, y_n) = 0.$$

Imagine expanding this relation. All the y_n's will be distinct, and so the largest one will be y_n^N for some N (and other terms, which include some factors of z_i, have smaller exponent of y_n). Thus, there exists $\lambda \in k$ such that $\lambda f(z_1 + y_n^{r_1} \ldots, z_{n-1} + y_n^{r_{n-1}}, y_n)$ is monic in y_n. Thus, we establish an integral dependence of y_n in the ring $k[z_1, \ldots, z_{n-1}]/\mathfrak{q}$, implying that y_n is integral. Consequently, $y_i = z_i + y_n^{r_i}$ is integral, so we are done. ☐

Remark 4.4.3.

If k is infinite, then picking $z_i = y_i - a_i y_n$ for some $a_1, \ldots, a_{n-1} \in k$ also works. This is more intuitive because we are doing linear perturbation. However, in order to make the proof works for k finite, one needs to consider higher-degree perturbation as well.

§4.4.2 Nullstellensatz

We use Noether normalization to prove Hilbert Nullstellensatz, a theorem that we stated very early in Chapter 1. We first do the weak version.

Theorem 4.4.4 (Weak Nullstellensatz)**.**

Let k be a field and K be a field extension such that K is finitely-generated as a k-algebra. Then, $[K : k]$ is a finite extension.

▶ *Proof.* By Noether normalization, there exists m such that

$$\underbrace{k[z_1, \dots, z_m]}_{=A} \overset{\text{integral}}{\subset} K$$

such that K is an integral extension of A. However, since K is a field, we get by Lemma 4.3.9 that A is a field, so $m = 0$ and $A = k$. Thus, K is finitely-generated as k-modules. ☐

Theorem 4.4.5 (Hilbert's Nullstellensatz)**.**

Let k be an algebraically-closed field and let $A = k[X_1, \dots, X_n]$. If $\mathfrak{m} \subset A$ is maximal, then there exists $a_1, \dots, a_n \in k$ such that $\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n)$.

▶ *Proof.* We have the map from $k \to A/\mathfrak{m}$ by quotient projection. By Theorem 4.4.4, $A/\mathfrak{m}$ is a finite field extension of k. Since k is algebraically closed, we actually get that $A/\mathfrak{m} = k$. Thus, setting $a_i \in k$ be the image of x_i in the isomorphism $A/\mathfrak{m} \to k$, we get that $x_i - a_i$ maps to zero, so $x_i - a_i \in \mathfrak{m}$. Collating this for all i, we get that $(x_1 - a_1, \dots, x_n - a_n) \subset \mathfrak{m}$, but this ideal is maximal already, so the equality is forced. ☐

Definition 4.4.6.

Given an ideal $J \subset k[X_1, \dots, X_n]$, we define the **vanishing locus**

$$V_m(J) = \{\vec{a} \in k^n : f(\vec{a}) = 0 \text{ for all } f \in J\},$$

which is a closed set (under both Zariski topology and classical topology) of k^n.

Conversely, given a subset $Z \subseteq k^n$, define the ideal

$$I(Z) = \{f : f(\vec{a}) = 0 \text{ for all } \vec{a} \in Z\}.$$

Then, we have the following.

Proposition 4.4.7.

If k is algebraically closed, then the maximal ideals of $k[X_1, \dots, X_n]/I$ corresponds in bijection to $V_m(I)$.

▶ *Proof.* By correspondence theorem, maximal ideals of $k[X_1, \dots, X_n]/I$ correspond to maximal ideals of $k[X_1, \dots, X_n]$ containing I, which then correspond to points in k^n that vanish at every polynomials in I. ☐

In particular, by taking maximal ideals, we can recover the set of points from ring of function.

Now we investigate the other direction: given set of points $V_m(I)$, can we recover the corresponding ideal I? In other words, we ask of the correspondence

$$\begin{aligned} \{\text{ideals of } k[x_1, \dots, x_n]\} &\leftrightarrow \{\text{closed set of } k^n\} \\ J &\mapsto V_m(J) \\ I(Z) &\leftarrow\!\shortmid Z. \end{aligned}$$

is a bijection or not. The answer is not quite, because ideals (x^2) and (x) have the same vanishing locus. The fix is that we have to take radical, and this is strong nullstellensatz.

Theorem 4.4.8 (Strong Hilbert's Nullstellensatz)**.**

Let k be an algebraically-closed field and $A = k[X_1, \dots, X_n]$. Given an ideal $J \subset A$, we have

$$I(V_m(J)) = \sqrt{J}.$$

To spell out in words, if $f(\vec{a}) = 0$ for all $\vec{a} \in V_m(J)$, then $f^n \in J$ for some n.

▶ *Proof.* The following proof is known as **Rabinowitsch's trick**. Let J and f as in the statement.

We are going to add a variable Y and consider an ideal

$$J' := (J, Yf - 1) \subseteq k[X_1, \dots, X_n, Y].$$

If $J' \neq k[X_1, \dots, X_n, Y]$, then by Krull's theorem Theorem 1.3.7, J' is contained in a maximal ideal of $k[X_1 \dots, X_n, Y]$, which (by Theorem 4.4.5) must be of the form $(X_1 - a_1, \dots, X_n - a_n, b)$ for some $a_1, \dots, a_n, b \in k$. The fact that $\mathfrak{m}$ contains J gives $(a_1, \dots, a_n) \in V_m(J)$, so $f(a_1, \dots, a_n) = 0$. Moreover, the fact that $\mathfrak{m}$ contais $Yf - 1$ gives $f(\vec{a})b - 1 = 0$, which is a contradiction.

Thus, $J = k[X_1, \dots, X_n, Y]$. Therefore, there exists $g_i \in k[X_1, \dots, X_n, Y]$ and $h_i \in J$ such that

$$1 = g_0(fY - 1) + \sum_{i=1}^{r} g_i h_i.$$

We will now plug in $Y = \frac{1}{f}$, working in the localization $k[X_1, \dots, X_n][1/f]$ to be rigorous. The term outside the summation goes away, and we obtain that

$$1 = \sum_{i=1}^{r} g_i \left(X_1, \dots, X_n, \frac{1}{f} \right) h_i(X_1, \dots, X_n).$$

Finally, we clear the denominator to get

$$f^N = \sum_{i=1}^{r} G_i(X_1, \dots, X_n) h_i(X_1, \dots, X_n) \in J,$$

where $G_i(X_1, \dots, X_n) = f^N g_i(X_1, \dots, X_n, 1/f)$ and $N \gg \deg g_i$ for all i, so G_i is actually a polynomial. Hence, $f \in \sqrt{J}$, and we are done. ☐

Remark 4.4.9.

What if k is not algebraically-closed?

If one follows the proof above, one gets that $A/\mathfrak{m}$ is a finite extension of k, and it is possible to continue and classify all maximal ideals of $k[x_1, \dots, x_n]$. The result is that there is a correspondence between

$$\{\text{maximal ideals of } k[x_1, \dots, x_n]\} \longleftrightarrow \frac{\{(a_1, \dots, a_n) \in \overline{k}^n\}}{\mathrm{Gal}(\overline{k}/k)\text{-action}}.$$

In other words, closed points of $k[x_1, \dots, x_n]$ corresponds to Galois orbits of $\overline{k}^n$.

If you take algebraic geometry, you will see that a lot of definitions (e.g., morphisms, and when they are the same) on varieties over k are usually defined by the behavior over $\overline{k}$. In the world of affine schemes (i.e., Spec R), this is completely natural because we naturally have $\overline{k}$-points in $\operatorname{Spec} k[x_1, \dots, x_n]$.

§4.5 First Steps in Dimension Theory

We now use tools developed in this chapter to study dimension of a variety. Let us first define dimension.

Definition 4.5.1 (Krull dimension).

Given any ring A, the **Krull dimension** (or just **dimension**) of A, denoted $\dim A$, is the maximum value of n for which there exists a chain of prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subset A$$

or length n.

This definition is not too horrible to make because of the following two reasons.

- For any vector space V, the dimension of V can be defined as the maximal value of n for which there exists a chain of subspaces

  $$V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_n \subset V$$

  of length n. In particular, V_i is an i-dimensional subspace. This resembles the chain definition given above, except that subspaces are replaced by prime ideals.

- The chain of prime ideal correspond to a descending chain of (closed) subvarieties

  $$\operatorname{Spec} A/\mathfrak{p}_0 \supsetneq \operatorname{Spec} A/\mathfrak{p}_1 \supsetneq \cdots \supsetneq \operatorname{Spec} A/\mathfrak{p}_n.$$

  Intuitively, $\operatorname{Spec} A/\mathfrak{p}_n$ would correspond to a point, $\operatorname{Spec} A/\mathfrak{p}_{n-1}$ would correspond to a curve, $\operatorname{Spec} A/\mathfrak{p}_{n-2}$ would correspond to a surface, and so on. We make $\mathfrak{p}_i$ prime so that one cannot write $\{\text{a line}\} \subsetneq \{\text{union of two lines}\}$ as an inclusion of a chain, forcing us to increase a dimension.

Example 4.5.2.

- For any field k, we have $\dim k = 0$.
- We claim that $\dim \mathbb{Z} = 1$ because the prime ideals of $\mathbb{Z}$ are (0), which is contained in $(2), (3), (5), \ldots$.
- More generally, if R is a PID that is not a field, we claim that $\dim R = 1$. The ideal (0) is contained in (a) for any non-unit $a \neq 0$. Meanwhile, if (a) is prime where $a \neq 0$, then a is irreducible, so (a) is maximal, so any nonzero prime ideal is maximal.

  In particular, $\dim k[x] = 1$ for any field k.
- If k is a field, then we can easily show that $\dim k[x_1, \ldots, x_n] \geq n$ by exhibiting a chain of prime ideals

  $$(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, \ldots, x_n).$$

  On the other hand, showing that $\dim k[x_1, \ldots, x_n] \leq n$ is considerably more difficult because one needs to consider any chain of prime ideals. We will do this in the course of proving Theorem 4.5.4.

Going-up theorem (Theorem 4.3.6) controls dimension.

Theorem 4.5.3 (Integral extension has equal dimension).

Let A be a ring and let B be an integral extension of A (so $A \subset B$). Then, $\dim A = \dim B$.

▶ *Proof.* First, we show $\dim A \geq \dim B$. Given any prime ideal chain $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_n$ of B, one let $\mathfrak{p}_i = \mathfrak{q}_i \cap S$, forming a chain of prime ideal $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ of A. The equality cannot occur because if $\mathfrak{p}_i = \mathfrak{p}_{i+1}$, then $\mathfrak{q}_i \subsetneq \mathfrak{q}_{i+1}$ both lie over $\mathfrak{p}_i$, violating incomparability Theorem 4.3.5.

Next, we show $\dim B \geq \dim A$. Given any prime ideal chain $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ of A, let $\mathfrak{q}_0$ be a prime lying over $\mathfrak{p}_0$ (exists by Theorem 4.3.4), and then by Going Up Theorem (Theorem 4.3.6), construct the chain $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_n$ such that $\mathfrak{p}_i = \mathfrak{q}_i \cap R$. Clearly, $\mathfrak{q}_i \neq \mathfrak{q}_{i+1}$.

Hence, we conclude that $\dim A = \dim B$. ☐

Now, we use Noether normalization lemma (Theorem 4.4.1) to give a neat characterization of dimension of a variety.

We first recall that given a field extension K/k, the **transcendence degree** $\operatorname{tr deg} K/k$ is the size of maximal set $S \subset K$ whose elements are k-algebraically independent. For example,

$$\operatorname{tr deg} k(x_1, \ldots, x_n)/k = n$$

because $x_1, \ldots, x_n$ are algebraically independent in $k(x_1, \ldots, x_n)$.

Theorem 4.5.4 (Dimension equals transcendence degree)**.**

If k is a field, B is a finitely-generated k-algebra that is a domain (i.e., $B = k[x_1, \ldots, x_n]/\mathfrak{p}$ for some prime ideal $\mathfrak{p}$), and $K = \operatorname{Frac} B$, then

$$\dim B = \operatorname{tr deg} K/k.$$

▶ *Proof.* We use induction on the transcendence degree $\operatorname{tr deg} K/k = n$. Assume that the result is known for transcendence degree less than n.

By Noether normalization lemma (Theorem 4.4.1), there exists $A = k[y_1, \ldots, y_m]$ such that B is an integral extension of A, which means $\dim A = \dim B$ by Theorem 4.5.3. Furthermore, $\operatorname{Frac} B$ is a finite extension of $\operatorname{Frac} A$, so $m = \operatorname{tr deg}(\operatorname{Frac}(A)/k) = \operatorname{tr deg}(\operatorname{Frac}(B)/k) = n$.

Thus, it suffices to show that $\dim k[y_1, \ldots, y_n] = n$. We have shown in Example 4.5.2 above that the dimension is at least n. To show that it is at most n, suppose for contradiction that there is a chain of length $n+1$:

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{n+1}.$$

Replace $\mathfrak{p}_0$ with (0). Choose an element $g \in \mathfrak{p}_1$, let f be an irreducible factor of g lying in $\mathfrak{p}_1$, and replace $\mathfrak{p}_1$ with (f). (Here, we use the fact that $k[x_1, \ldots, x_n]$ is a UFD to see that (f) is prime.) Thus, the above chain simplifies to

$$(0) \subsetneq (f) \subsetneq \mathfrak{p}_2 \subsetneq \cdots \subsetneq \mathfrak{p}_{n+1},$$

which induces the chain of prime ideal of length n on ring $C = k[x_1, \ldots, x_n]/(f)$.

However, note that $\operatorname{Frac} C = k(x_1, \ldots, x_n)/(f)$, which has transcendence degree $n-1$. Therefore, by induction hypothesis, $\dim C = n - 1$, contradicting the above paragraph. ☐

Example 4.5.5.

If f is any irreducible polynomial in $k[x_1, \ldots, x_n]$, then $\dim k[x_1, \ldots, x_n]/(f) = n - 1$.

This covers dimension theory in the case of finitely-generated algebra over k. However, we still don't know how to prove, for example, that $\dim \mathbb{Z}[x_1, \ldots, x_n] = n + 1$. We will develop a more robust dimension theory in Chapter 9 that will allow us to prove that.

§4.6 Problems

Problem 4.A. Decide whether each of the following ring is an integral extension of $\mathbb{C}[x]$.

(a) $\mathbb{C}[x, y]/(x^2 - y^2)$.

(b) $\mathbb{C}[x, y]/(xy)$.

(c) $\mathbb{C}[x, y]/(xy - 1)$.

Problem 4.B. If B is an integral extension of A and $\mathfrak{q} \subset B$ is a prime ideal lying above $\mathfrak{p} \subset A$, is it necessarily true that $B_{\mathfrak{q}}$ is integral over $A_{\mathfrak{p}}$? Compare with Proposition 4.2.13 (b).

Problem 4.C. Prove that $\mathbb{C}[x, y, z]/(x^2 - yz)$ is integrally closed.[1]

(Hint: minimal polynomial test.)

Problem 4.D. Let K be a finite, Galois extension of $\mathbb{Q}$. Let $\mathcal{O}_K$ be the ring of integer of K. Let p be a rational prime, and $\mathfrak{p}$ and $\mathfrak{q}$ are two prime ideals of $\mathcal{O}_K$ lying above (p). Prove that there exists $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma\mathfrak{p} = \mathfrak{q}$.

(Hint: use prime avoidance, Problem 1.E.)

Problem 4.E. Find a Noether normalization and the dimension of the ring

$$R = \frac{\mathbb{C}[x, y, z]}{(x^2 - y^3 - 1, xyz - 1)}.$$

Problem 4.F. Let $\mathfrak{n}$ be a maximal ideal of $R = \mathbb{R}[x_1, \dots, x_n]$.

(a) Prove that there exists $a = (a_1, \dots, a_n) \in \mathbb{C}^n$ such that if $\mathfrak{m}_a = (x_1 - a_1, \dots, x_n - a_n) \subset \mathbb{C}[x_1, \dots, x_n]$, then $\mathfrak{m}_a \cap R = \mathfrak{n}$.

(b) Let $a, b \in \mathbb{C}^n$. Prove that $\mathfrak{m}_a \cap R = \mathfrak{m}_b \cap R$ if and only if $a = b$ or $a = \overline{b}$ (where $\overline{b}$ is the complex conjugate of b.)

Thus, we establish a bijection between maximal ideals of $\mathbb{R}[x_1, \dots, x_n]$ and tuples in $\mathbb{C}^n$ modulo conjugation. You can generalize this result by replacing $\mathbb{R}$ and $\mathbb{C}$ to k and $\overline{k}$, respectively.

Problem 4.G. Let k be a field and A and B are finitely-generated k-algebra.

(a) Assume that k is algebraically closed. Prove that there exists a bijection between

$$\{\text{maximal ideals of } A \otimes_k B\} \leftrightarrow \{\text{maximal ideals of } A\} \times \{\text{maximal ideals of } B\}.$$

Geometric interpretation: $A \otimes_k B$ is the ring corresponding to product of varieties.

(b) Prove that $\dim(A \otimes_k B) = \dim A + \dim B$, where dim in both sides are dimension as rings.

Problem 4.H. Let k be a field, and let A be a finitely-generated k-algebra that is a domain.

(a) Let B be an integral extension of A that is a domain. Suppose that $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \mathfrak{p}_3 \subset A$ is a chain of prime ideals in A. Let $\mathfrak{q}_1 \subsetneq \mathfrak{q}_3 \subset B$ be prime ideals above $\mathfrak{p}_1$ and $\mathfrak{p}_3$, respectively. Prove that there exists a prime ideal $\mathfrak{q}_2$ such that $\mathfrak{q}_1 \subsetneq \mathfrak{q}_2 \subsetneq \mathfrak{q}_3$. Note that $\mathfrak{q}_2$ need not lie over $\mathfrak{p}_2$.

Hint: WLOG, assume $\mathfrak{p}_1 = (0)$ and $\mathfrak{q}_1 = (0)$. Why?

(b) Prove that all maximal chains of prime ideals in A have length exactly $\dim A$. (Here, maximal is in the sense that one cannot insert another prime ideal at the boundary or between any two consecutive ideals in the chain.)

(c) Prove that for all prime ideals $\mathfrak{p} \subsetneq \mathfrak{q}$ of A, the length of all maximal chains of prime ideals starting at $\mathfrak{p}$ and ending at $\mathfrak{q}$ are the same. (Rings with this property are called **catenary**.)

---

[1] Note that the surface $x^2 - yz = 0$ has a singularity at $(0, 0, 0)$.

5 Chain Conditions

In this chapter, we are going to talk about chain conditions, which are conditions on rings / modules that makes various objects finite. There are two similar conditions, Noetherian, which is about ascending chain, and Artinian, which is about descending chain. We first discuss these two conditions for modules in Section 5.1. Later, we will specialize to Noetherian rings (Section 5.2) and Artinian rings (Section 5.3). It will turns out that while Noetherian rings is a fundamental finiteness condition that makes rings reasonable, Artinian rings much more specialize and looks like "points" (i.e., has dimension 0).

§5.1 Noetherian and Artinian Modules

§5.1.1 Definitions and Basic Examples

There are two main types of chain condition that we will discuss.

Definition 5.1.1 (Noetherian and Artininan modules)**.**

Let R be a ring, and M be an R-module.

- M is a **Noetherian module** if it satisfies the **ascending chain condition (ACC)**: there does not exist a chain of submodules

$$M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq \cdots \subset M.$$

  (i.e., any ascending chain stops).

- M is a **Artinian module** if it satisfies the **descending chain condition (DCC)**: there does not exist a chain of submodules

$$M \supset M_1 \supsetneq M_2 \supsetneq M_3 \supsetneq \dots$$

We say that R is a **Noetherian ring** (resp. **Artinian ring**) if R is Noetherian (resp. Artinian) as an R-module.

Now, let's do a basic example.

Example 5.1.2.

We have the following examples.

- Finite abelian groups (as a $\mathbb{Z}$-module) are both Noetherian and Artinian because they are finite.
- $R = \mathbb{Z}/(n)$ is both Noetherian and Artinian for the same reason.
- PID's are Noetherian rings: if there is a chain $(a_1) \subsetneq (a_2) \subsetneq \dots$, then $(a_1) \cup (a_2) \cup \dots$ is an ideal generated by element (a). Then, $a \in (a_i)$ for some i, forcing $(a_i) = (a_{i+1}) = \cdots = (a)$, so the chain is eventually constant.

Consequently, $\mathbb{Z}$ and $\mathbb{C}[x]$ are Noetherian.

- $\mathbb{Z}$ is not Artinian ring: $\mathbb{Z} \supset (2) \supset (4) \supset (8) \supset \dots$.
- $R = \mathbb{Z}$ and $M = \mathbb{Z}[1/p]/\mathbb{Z}$ is Artinian but not Noetherian. Any submodule of M is in form $M_n = \frac{1}{p^n}\mathbb{Z}/\mathbb{Z}$, so $0 = M_0 \subset M_1 \subset M_2 \subset \dots$. Therefore, this module is not Noetherian. It is Artinian because any descending chain must start somewhere, hence finite.
- $\mathbb{C}[x_1, x_2, \dots]$ is neither Noetherian nor Artinian ring.

We will see later that Noetherian rings is a more fundamental concept of commutative algebra: almost all examples you would care about is Noetherian. On the other hand, Artinian ring is an extremely special kind of rings that we will describe later.

§5.1.2 Properties of Noetherian and Artinian Modules

Proposition 5.1.3.

An R-module M is Noetherian if and only if every submodule is finitely-generated.

▶ *Proof.* (⇒) If $N \subset M$ is not finitely generated, pick $x_1 \in N$, $x_2 \notin \operatorname{Span}(x_1)$, $x_3 \notin \operatorname{Span}(x_1, x_2)$, $\dots$. Then, one has

$$Rx_1 \subsetneq Rx_1 + Rx_2 \subsetneq Rx_1 + Rx_2 + Rx_3 \subsetneq \dots,$$

a contradiction.

(⇐) Suppose that we have a chain

$$M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq \dots,$$

then $N = \bigcup_{i=1}^{\infty} M_i$ is finitely-generated. Pick generators $x_1, \dots, x_r \in N$. Clearly x_i has to be in some M_j's, so one can pick n such that $x_1, \dots, x_r \in M_n$, so $N = M_n$, and the chain terminates. ☐

Now, we start giving how to generate Noetherian modules.

Proposition 5.1.4 (Exact Sequence Property).

Consider an exact sequence of R-modules

$$0 \longrightarrow M_1 \xrightarrow{\phi} M_2 \xrightarrow{\pi} M_3 \longrightarrow 0.$$

Then,

(a) M_2 Noetherian if and only if M_1 and M_3 are Noetherian.

(b) M_2 Artinian if and only if M_1 and M_3 are Artinian.

▶ *Proof.* (a) (⇒) An infinite chain of submodules of M_1

$$P_1 \subsetneq P_2 \subsetneq \dots \subsetneq M_1$$

turns to an infinite chain of submodules in M_2:

$$\phi(P_1) \subsetneq \phi(P_2) \subsetneq \dots \subsetneq M_2$$

(they are distinct since ϕ is injective). Thus, if M_1 is not Noetherian, then M_2 is not Noetherian.

Similarly, an infinite chain of submodules of M_3

$$Q_1 \subsetneq Q_2 \subsetneq \cdots \subsetneq M_3$$

turns to an infinite chain of submodules in M_2:

$$\pi^{-1}(Q_1) \subsetneq \pi^{-1}(Q_2) \subsetneq \cdots \subsetneq M_2$$

(they are distinct since π is injective). Thus, if M_3 is not Noetherian, then M_2 is not Noetherian. Hence, we are done.

($\Leftarrow$) Given $N_1 \subset N_2 \subset N_3 \subset \dots$ is a chain in M_2. Then, if $\pi : M_2 \to M_3$ again, then we have two chains

$$\begin{aligned} \phi^{-1}(N_1) \subset \phi^{-1}(N_2) \subset \phi^{-1}(N_3) \subset \dots \\ \pi(N_1) \quad \subset \quad \pi(N_2) \quad \subset \quad \pi(N_3) \quad \subset \dots . \end{aligned}$$

Since M_1 and M_3 are Noetherian, both chains stabilizes, so for some sufficiently large k, we have $\phi^{-1}(N_k) = \phi^{-1}(N_{k+1})$ and $\pi(N_k) = \pi(N_{k+1})$. We claim that this implies $N_k = N_{k+1}$.

To see this, suppose $x \in N_{k+1}$, then $\pi(x) \in \pi(N_{k+1}) = \pi(N_k)$, so for some $y \in N_k$, we have $\pi(x - y) = 0$, which means $x - y \in \operatorname{Im}\phi$. Thus, there exists $z \in M_1$ such that $x = y + \phi(z)$. Now, $\phi(z) \in N_{k+1}$, so $z \in \phi^{-1}(N_{k+1})$, which implies $z \in \phi^{-1}(N_k)$, so $\phi(z) \in N_k$. Hence, $x = y + \phi(z) \in N_k$.

(b) is similar to (a). ☐

Corollary 5.1.5.

If $M_1, \dots, M_n$ are all Noetherian (resp. Artinian), then $M_1 \oplus \cdots \oplus M_n$ is Noetherian (resp. Artinian).

If R is Noetherian ring, checking if a module is Noetherian is even more convenient.

Proposition 5.1.6 (Noetherian iff finitely-generated)**.**

If R is Noetherian ring, then M is Noetherian if and only if M is finitely-generated as an R-module.

▶ *Proof.* ($\Rightarrow$) is clear from Proposition 5.1.3. For ($\Leftarrow$), consider an exact sequence $R^{\oplus n} \to M \to 0$. We know that $R^{\oplus n}$ is Noetherian, so M is Noetherian by the exact sequence property Proposition 5.1.4 (a). ☐

Exercise 5.1.7. If R is an Artinian ring, prove that M is Artinian module if and only if M is finitely-generated as an R-module.

§5.2 Noetherian Rings

§5.2.1 Properties of Noetherian Rings

We now restrict our attention to Noetherian rings. First, from Proposition 5.1.3, we have

Corollary 5.2.1.

R is Noetherian if and only if every ideal of I is finitely-generated.

Now, we begin stating properties.

Proposition 5.2.2 (Quotient, localization, product of Noetherian ring is Noetherian)**.**

Let R be a Noetherian ring.

(a) R/I is Noetherian for all ideal I;

(b) $S^{-1}R$ is Noetherian for any multiplicative set S;

(c) $R \times S$ is Noetherian for any Noetherian rings R and S.

▶ *Proof.* (a) Let $\pi : R \to R/I$ be the quotient map. By correspondence theorem Theorem 1.1.8, all ideals of R/I must be in form $\pi(J)$ for some ideal $J \subseteq R$. If $J = (x_1, \ldots, x_n)$, then $\pi(J) = (\pi(x_1), \ldots, \pi(x_n))$ is finitely-generated.

(b) By Proposition 3.1.9, any ideal $J \subset S^{-1}R$ is an extension of some ideal $I \subset R$. If $I = (x_1, \ldots, x_n)$, then $J = \left(\frac{x_1}{1}, \ldots, \frac{x_n}{1}\right)$.

(c) Let $\pi_1 : R \times S \to R$ and $\pi_2 : R \times S \to S$ be the projection maps. Given an ideal $J \subset R \times S$, let $J_R = \pi_1(J)$ and $J_S = \pi_2(J)$.

We claim that $J = J_R \times J_S$. To do so, given $(a, b) \in J_R \times J_S$. We have $(a, c) \in J$ for some c and $(d, b) \in J$ for some d, then

$$(a, b) = (a, c) \cdot (1, 0) + (d, b) \cdot (0, 1) \in J.$$

Thus, J is finitely-generated. ☐

Theorem 5.2.3 (Hilbert's Basis Theorem)**.**

If R is Noetherian, then so is $R[x]$ (and hence $R[x_1, \ldots, x_n]$).

This allows us to deduce, for example, that $\mathbb{C}[x_1, \ldots, x_n]$ and $\mathbb{Z}[x_1, \ldots, x_n]$ are Noetherian. This is a nontrivial result, since ideals $\mathbb{C}[x_1, \ldots, x_n]$ can be quite arbitrary, but it is still finitely-generated. It is also interesting to find an algorithm finding these finitely-many generators. However, typical proofs (e.g., the one below) is not algorithmic in nature. The set of generators you get is exponential.

▶ *Proof.* Let $I \subset R[x]$ be an ideal. We want to show that I is finitely-generated. We want to use the fact that R is Noetherian. The key idea is to look at the leading coefficients. Define an ideal

$$J_n = \{a \in R : \text{there exists } f \in I \text{ with degree } n \text{ and leading coefficient } a\} \cup \{0\}.$$

Clearly, J_n is an ideal. Moreover, $J_n \subset J_{n+1}$ because if $f \in I$ of degree n, then $xf \in I$ of degree $n+1$. Therefore, since R is Noetherian, we have $J_n = J_{n+1} = \ldots$ for all n. Even further, for each $m \leq n$, we have J_m is finitely generated, say by $(a_{m,i})$. We let $a_{m,i}$ be the leading coefficient of $f_{m,i}$.

We now claim that $I = (f_{m,i} : m \leq n)$ (and henceforth finitely-generated). To prove this, we prove by induction on $r = \deg f$ that f is generated by $f_{m,i}$'s. The base case $r = 0$ is clear. We have two cases.

- If $r \geq n$, let $f(x) = cx^r + \cdots$. Then, $c \in J_r = J_n$, so c is generated by $(a_{n,i})$. This means there exists $b_i \in R$ such that $c = \sum b_i a_{n,i}$. Then, we have
$$\sum b_i f_{n,i}(x) \cdot x^{r-n} = cx^r + \text{lower-order terms}.$$
The left-hand-side is generated by $f_{n,i}$, so one can use the induction hypothesis.
- If $r \neq n$, the same thing happen: just change $f_{n,i}$ to $f_{r,i}$. ☐

To summarize, any quotient and localization of Noetherian ring is Noetherian. Adjoining finitely many elements into Noetherian ring is also Noetherian. This pretty much covers everything you will care about in Algebraic Geometry.

We end with some warning.

⚠ **Warning 5.2.4.**

- If R is a Noetherian ring, then subring $S \subseteq R$ is not necessarily Noetherian. Example: $S = k[x_1, x_2, \dots]$ and $R = \operatorname{Frac} S$.
- If R and S are T-algebra, and R, S, T are all Noetherian, then $R \otimes_T S$ is not necessarily Noetherian. The counterexample is $\mathbb{Q}(x_1, x_2, \dots) \otimes_{\mathbb{Q}} \mathbb{Q}(x_1, x_2, \dots)$ is not Noetherian; see [Vám78, Theorem 11]

Non-Noetherian rings show up in number theory (specifically, class field theory): for example, the adele ring $\mathbb{A}_{\mathbb{Q}}$ is not Noetherian.

§5.2.2 Zariski Topology of Noetherian Rings

We have discussed a lot on properties on Noetherian rings. Now, we try to interpret this in terms of spectrum.

Definition 5.2.5 (Noetherian Space).

A topological space X is **Noetherian** if the closed subsets satisfy the Descending Chain Condition (DCC). In particular, there is no infinite chain of closed sets

$$X \supset Z_1 \supsetneq Z_2 \supsetneq Z_3 \supsetneq \dots.$$

Most topological spaces are not Noetherian though. For example, the real line $\mathbb{R}$ is obviously not Noetherian because one can take infinitely nested intervals.

There is no surprising that this definition is rigged so that it is equivalent to Noetherian rings.

Proposition 5.2.6.

If R is Noetherian, then $\operatorname{Spec} R$ is a Noetherian space.

▶ *Proof.* There exists a correspondence between

$$\begin{aligned} \{\text{closed sets of } \operatorname{Spec} R\} &\leftrightarrow \{\text{radical ideals of } R\} \\ Z &\mapsto I(Z) = \bigcap_{\mathfrak{p} \in Z} \mathfrak{p} \\ V(J) &\leftarrow J \end{aligned}$$

Observe that $I(V(J)) = \sqrt{J}$ by definition of radical, so these correspondence are inverses.

Thus, given a chain of closed sets $Z_1 \supsetneq Z_2 \supsetneq Z_3 \supsetneq \dots$, we get an ascending chain

$$I(Z_1) \subsetneq I(Z_2) \subsetneq \dots,$$

which violates the Noetherian condition. □

§5.2.3 Irreducible Components

We now give a way to decompose $\operatorname{Spec} R$.

Definition 5.2.7 (Reducible topological spaces).

A topological space X is **reducible** if $X = Y_1 \cup Y_2$ (not necessarily disjoint) such that Y_i is closed and $Y_i \neq X$.

If X is not reducible and $X \neq \emptyset$, we say that X is **irreducible**.

Let us make some examples for the spectrum.

Example 5.2.8.

- $\operatorname{Spec} \mathbb{Z}$ is irreducible because closed set is finite, so no two closed sets union to X.
- More generally, if R is a domain, then $\operatorname{Spec} R$ is irreducible, because if $\operatorname{Spec} R = Y_1 \cup Y_2$, then (0) must be in at least one of Y_i's, but closure of (0) is the entire $\operatorname{Spec} R$.
- On the other hand, $\operatorname{Spec} \mathbb{C}[x, y]/(xy)$ is reducible because $\mathbb{C}[x, y]/(xy)$ is the union of x-axis and y-axis. In particular,
$$\operatorname{Spec} \mathbb{C}[x, y]/(xy) = V(x) \cup V(y).$$

If X is a topological space, then a closed subset $W \subseteq X$ is irreducible if and only if the induced topology on W makes W irreducible. By plugging in the definition of induced topology, we find that W is irreducible if and only if "for all closed subsets Y, Z such that $W \subseteq Y \cup Z$, we have either $W \subseteq Y$ or $W \subseteq Z$". An irreducible closed set is **maximal** if it is not contained in another irreducible closed set.

Every Noetherian topological space can be decomposed to a finite union of irreducible closed sets. The Noetherian condition will guarantee finiteness.

Proposition 5.2.9 (Irreducible decomposition)**.**

Let X be a Noetherian topological space. Then,
$$X = \bigcup_{i=1}^{n} Z_i,$$
where Z_i is a maximal irreducible closed set.

Moreover, this decomposition is unique. Consequently, there are finitely many maximal irreducible closed sets.

▶ *Proof.* The proof is in two parts.

Existence. If X is irreducible, we are done. Otherwise, $X = Y_1 \cup Y_2$ where $Y_i \subsetneq X$ closed. If both Y_1 and Y_2 are irreducible, we are done. Otherwise, take $Y_1 = Y_3 \cup Y_4$, where $Y_3, Y_4 \subsetneq Y_1$. This process continues. It must terminate in finitely many steps because X is noetherian. Thus, we have $X = Z_1 \cup \cdots \cup Z_n$ for some irreducible closed sets $Z_1, \ldots, Z_n$.

We now check that Z_i is maximal. Assume that $Z_i \subseteq Y$ for some irreducible closed set Y. Then, note that $Y \subseteq Z_1 \cup \cdots \cup Z_n$, so $Y \subseteq Z_j$ for some j. Thus, $Z_i \subseteq Z_j$ for some j, and we can throw Z_i out of the decomposition.

Uniqueness. If $X = Y_1 \cup \cdots \cup Y_m$ is another decomposition, then $Y_1 \subseteq Z_1 \cup \cdots \cup Z_n$, so $Y_1 \subseteq Z_i$ for some i, so by maximality, $Y_1 = Z_i$. Thus, every set in Y_i is equal to set in Z_j for some j. Conversely, every set in Z_j is equal to Y_i for some i. Therefore, $\{Y_i\}$ and $\{Z_j\}$ are the same set. ☐

We now interpret this result algebraically. First, we can characterize when $\operatorname{Spec} R$ is irreducible.

Proposition 5.2.10.

The following are equivalent.

(a) $\operatorname{Spec} R$ is irreducible.

(b) $\operatorname{Nil}(R)$ is a prime ideal.

▶ *Proof.* This is a straightforward definition-chasing. For completeness, we provide a complete proof below.

(a) implies (b). If $a, b \notin \operatorname{Nil}(R)$ such that $ab \in \operatorname{Nil}(R)$, so $(ab)^n = 0$ for some n. We claim that $\operatorname{Spec} R = V(a) \cup V(b)$. To see this, given any prime ideal $\mathfrak{p}$, $(ab)^n = 0$, so $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, so $\mathfrak{p} \in V(a)$ or $\mathfrak{p} \in V(b)$. Finally, note that $V(a) \neq \operatorname{Spec} R$ because $a \notin \operatorname{Nil}(R)$, so by Proposition 1.4.1, there exists a prime ideal not in $V(a)$. Similarly, $V(b) \neq \operatorname{Spec} R$. Thus, $\operatorname{Spec} R$ is not irreducible.

(b) implies (a). We claim that the closure of $\operatorname{Nil}(R)$ is $\operatorname{Spec} R$. To see why, consider a closed set $V(I)$ containing $\operatorname{Nil}(R)$, so $I \subseteq \operatorname{Nil}(R)$, which in turn contains $\mathfrak{p}$ for all prime ideal $\mathfrak{p}$. Thus, every prime $\mathfrak{p} \in \operatorname{Spec} R$ is in $V(I)$.

Hence, if any irreducible closed set contains $\operatorname{Nil}(R)$, it must be entire $\operatorname{Spec} R$. This shows that $\operatorname{Spec} R$ is irreducible. ☐

Corollary 5.2.11.

(a) There exists a bijective correspondance

$$\begin{aligned} \{\text{prime ideals of } R\} &\leftrightarrow \{\text{irreducible closed sets of } R\} \\ \mathfrak{p} &\mapsto V(\mathfrak{p}). \end{aligned}$$

(b) The correspondence above takes minimal prime ideals to maximal irreducible closed sets of R.

▶ *Proof.* (a) If I is a radical ideal, the following are equivalent:

- $V(I) = \operatorname{Spec} R/I$ is irreducible.
- R/I is a domain (proof: R/I is reduced).
- I is a prime ideal.

(b) Follows from that V is inclusion reversing, so it takes minimal prime ideals to maximal irreducible closed sets. ☐

Thus, we have deduce the following corollaries.

Corollary 5.2.12.

If R is Noetherian ring, then there are finitely many minimal primes.

▶ *Proof.* Combine Proposition 5.2.9 (on $X = \operatorname{Spec} R$) and Corollary 5.2.11. ☐

Corollary 5.2.13.

If R is Noetherian ring, then for every ideal $I \subset R$, there are finitely prime ideals minimal among those containing I.

▶ *Proof.* Apply the previous corollary to R/I. ☐

Let us now interpret these results. Let R be a Noetherian ring and I be a radical ideal. Then, $V(I) \simeq \operatorname{Spec}(R/I)$ can be written as union of $V(\mathfrak{p})$, where $\mathfrak{p}$ is a prime ideal minimal among those containing I. This means

$$V(I) = \bigcup_{i=1}^{n} V(\mathfrak{p}_i) = V\left(\bigcap_{i=1}^{n} \mathfrak{p}_i\right).$$

Therefore, we have

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

where $\mathfrak{p}_i$ prime ideals minimal among those containing I. Thus, any radical ideal can be written as intersection of prime ideals minimal among those containing I. Moreover, this decomposition is unique!

In the next Chapter, Section 6.2, we will generalize this to non-radical ideals.

§5.3 Artinian Rings

§5.3.1 Preliminary: Product Rings

The following lemma tells us that spectrum of a product ring is disjoint union.

Lemma 5.3.1 (Product Rings).

(a) Let A and B be rings. Then, $\operatorname{Spec}(A \times B)$ is homeomorphic to the disjoint union of $\operatorname{Spec} A$ and $\operatorname{Spec} B$.

(b) Conversely, if R is a ring such that $\operatorname{Spec} R = Y_1 \sqcup Y_2$, where Y_1 and Y_2 are both open and closed, then $R = A \times B$ for rings A and B such that $\operatorname{Spec} A = Y_1$ and $\operatorname{Spec} B = Y_2$.

▶ *Proof.* (a) Let P be a prime ideal of $A \times B$. We claim that either $P = \mathfrak{p} \times B$ for some prime ideal $\mathfrak{p} \subseteq A$ or $P = A \times \mathfrak{q}$ for some prime ideal $\mathfrak{q} \subseteq B$.

To prove this, note that $(1,0)(0,1) = (0,0)$, so either $(1,0) \in P$ or $(0,1) \in P$. Without loss of generality, assume the former. Then, $(a,0) \in P$ for all $a \in A$. This shows that $P = A \times \mathfrak{q}$ for some ideal $\mathfrak{q} \subseteq B$, and one can see that P is prime implies $\mathfrak{q}$ must be prime.

Thus, we have a bijective correspondence

$$\begin{aligned} \operatorname{Spec} A \sqcup \operatorname{Spec} B &\to \operatorname{Spec}(A \times B) \\ \mathfrak{p} \in \operatorname{Spec} A &\mapsto \mathfrak{p} \times B \\ \mathfrak{q} \in \operatorname{Spec} B &\mapsto A \times \mathfrak{q} \end{aligned}$$

and one can check that this is a homeomorphism.

(b) Since Y_1 and Y_2 are closed, let $Y_1 = V(I)$ and $Y_2 = V(J)$ for ideals I and J. Then, the disjointness of Y_1 and Y_2 implies $I + J = (1)$, while union condition implies that $IJ \subseteq \operatorname{Nil}(R)$. Therefore, there exists $i \in I$ and $j \in J$ such that $i + j = 1$. Since $IJ \subseteq \operatorname{Nil}(R)$, we get that $(ij)^n = 0$ for some integer n.

Now, observe that (i) and (j) are coprime. Thus, (i^n) and (j^n) are coprime. Moreover, $(i^n)(j^n) = (0)$. Therefore, applying Chinese Remainder Theorem (Theorem 1.2.11) gives

$$R \simeq R/(i^n) \times R/(j^n),$$

where the map is quotient projection to each component. Next, we note that

$$V(i) \cup V(j) \supseteq V(I) \cup V(J) = R,$$

and $V(i)$ and $V(j)$ are disjoint because $i+j = 1$. Hence, $V(i^n) = V(i) = V(I)$, so $\operatorname{Spec} R/(i^n) \simeq Y_1$. Similarly, $\operatorname{Spec} R/(j^n) \simeq Y_2$. ☐

§5.3.2 Structure Theorem for Artinian Rings

Recall that Artinian rings satisfy the Descending Chain Condition: there is no chain

$$I_1 \supsetneq I_2 \supsetneq I_3 \supsetneq \dots.$$

We will now give the main structure theorem for Artinian rings.

First, we study Artinian local rings. Recall that a ring has dimension 0 if and only if every prime ideal is maximal.

Theorem 5.3.2 (Artinian local rings).

Let R be a local ring with maximal ideal $\mathfrak{m}$. The following are equivalent.

(a) R is Artinian.

(b) R is Noetherian and has dimension 0 (i.e., has $\mathfrak{m}$ as the only prime ideal).

(c) R is Noetherian and $\mathfrak{m} = \operatorname{Nil}(R)$.

(d) R is Noetherian and $\mathfrak{m}^N = 0$ for some integer $N \geq 0$.

This theorem tells us that a local ring R is Artinian if and only if $\operatorname{Spec} R$ has one point.

▶ *Proof.* We first do the easy part of showing that (b), (c), and (d) are all equivalent.

- **(b) ⇔ (c).** Follows immediately from the fact that $\operatorname{Nil}(R)$ is intersection of prime ideals (Proposition 1.4.1).
- **(c) ⇒ (d).** Let $\mathfrak{m}$ be generated by $x_1, \dots, x_n$. Since $\mathfrak{m} = \operatorname{Nil}(R)$, all elements $x_1, \dots, x_n$ are nilpotent, so there exists e such that $x_1^e = x_2^e = \dots = x_n^e = 0$. Now, we claim that $\mathfrak{m}^{ne} = 0$. To see this, note that each term in $\mathfrak{m}^{ne}$ is a multiple of monomials $x_1^{f_1} \cdots x_n^{f_n}$ where $f_1 + \dots + f_n \geq ne$. This monomial is zero because $f_i \geq e$ for some i.
- **(d) ⇒ (c).** From $\mathfrak{m}^N = 0$, taking radical both sides gives $\mathfrak{m} = \operatorname{Nil}(R)$.

Finally, we move on to the difficult part of showing that (a) and (d) are equivalent. This is done in two steps.

1. **If R is Artinian, then $\mathfrak{m}^N = 0$ for some N.** Consider a descending chain $\mathfrak{m} \supset \mathfrak{m}^2 \supset \dots$. Since R is Artinian, we have $\mathfrak{m}^N = \mathfrak{m}^{N+1}$ for some N.

   It's so tempting to apply Nakayama's Lemma (Corollary 2.2.5), and conclude that $\mathfrak{m}^N = 0$. However, this **doesn't work**, as Nakayama requires that $\mathfrak{m}^N$ is finitely-generated.

   Let us find a way to salvage this. Assume $\mathfrak{m}^N \neq 0$. Let

   $$\Sigma = \{\text{ideals } J \text{ such that } \mathfrak{m}^N J \neq (0)\}.$$

   We have $\Sigma \neq \emptyset$ since $(1) \in \Sigma$. We then find $J \in \Sigma$ that is minimal (this is a finite process because R is Artinian). Then, there exists $x \in J$ such that $\mathfrak{m}^N x \neq 0$. However, $\mathfrak{m}^N \cdot (x) \neq 0$, so since J is minimal, we have that $J = (x)$!

   Furthermore, we note that

   $$\mathfrak{m}^N(\mathfrak{m}J) = \mathfrak{m}^{N+1}J = \mathfrak{m}^N J \neq 0 \implies \mathfrak{m}J \in \Sigma,$$

   so by minimality of J again, we get $\mathfrak{m}J = J$. However, J is finitely generated because it is principal! Thus, we may use Nakayama's lemma (Corollary 2.2.5) to get that $J = (0)$, and this is a contradiction.

2. **If $\mathfrak{m}^N = 0$ for some N, then R is Artinian if and only if R is Noetherian.**

   We consider the filtration

$$R \supset \mathfrak{m} \supset \mathfrak{m}^2 \supset \dots \mathfrak{m}^{N-1} \supset \mathfrak{m}^N = 0.$$

   Then, the following are equivalent.

   - R is Noetherian as R-module.
   - $\mathfrak{m}^{i-1}/\mathfrak{m}^i$ is Noetherian as R-modules for all $i = 1, 2, \dots, N$. (Use Proposition 5.1.4.)
   - $\mathfrak{m}^{i-1}/\mathfrak{m}^i$ is Noetherian as $R/\mathfrak{m}$-modules for all $i = 1, 2, \dots, N$.
   - $\dim_{R/\mathfrak{m}}(\mathfrak{m}^{i-1}/\mathfrak{m}^i) < \infty$ for all $i = 1, 2, \dots, N$.
   - $\mathfrak{m}^{i-1}/\mathfrak{m}^i$ is Artinian as $R/\mathfrak{m}$-modules for all $i = 1, 2, \dots, N$ (as an $R/\mathfrak{m}$-module).
   - $\mathfrak{m}^{i-1}/\mathfrak{m}^i$ is Artinian as R-modules for all $i = 1, 2, \dots, N$ (as an R-module).
   - R is Artinian (as R-module). (Use Proposition 5.1.4 again.) ☐

Now, we can prove the main result for general Artinian ring.

Theorem 5.3.3 (Artinian rings).

Let R be a ring. The following are equivalent.

(a) R is Artinian.

(b) R is Noetherian of dimension 0.

(c) $\operatorname{Spec} R$ is finite and has discrete topology.

(d) R is a finite product of Artinian local rings.

▶ *Proof.* We first show that (b), (c), and (d) are equivalent.

- **(b) ⇒ (c).** Corollary 5.2.12 gives that there are finitely minimal primes, and from R has dimension 0, every prime ideal is a minimal prime, so there are finitely many prime ideals.

- **(c) ⇒ (d).** By Lemma 5.3.1 (b), if $\operatorname{Spec} R$ has discrete topology, it is a product ring $R_1 \times \cdots \times R_n$ where $\operatorname{Spec} R_i$ is a single point, hence an Artinian local ring.

- **(d) ⇒ (b).** Clear from Lemma 5.3.1 (a).

Next, we show that (d) implies (a). To do this, it suffices to show that product of two Artinian rings is Artinian (hence by induction, finite product of Artinian ring is Artinian). Let A and B be Artinian. Then, we have an exact sequence of $(A \times B)$-module

$$0 \longrightarrow A \longrightarrow A \times B \longrightarrow B \longrightarrow 0.$$

Note that A is Artinian as A-module, so A is Artinian as $(A \times B)$-module. Simiarly, B is Artinian as $(A \times B)$-module, so by exact sequence property, Proposition 5.1.4 $A \times B$ is Artinian.

Finally, we show the hardest implication that (a) implies (c). This is in two steps.

1. **Every prime ideal of R is maximal (i.e., R has dimension 0).** Let $\mathfrak{p} \subset R$ be prime but not maximal. Then, $A = R/\mathfrak{p}$ is a domain but not a field. Thus, there exist $0 \neq f \in A$ such that f is not a unit, producing an infinite descending chain

$$A \supsetneq (f) \supsetneq (f^2) \supsetneq (f^3) \supsetneq \dots,$$

   which contradicts that fact that A is Artinian.

2. **R has finitely many maximal ideals.** Suppose $\mathfrak{m}_1, \mathfrak{m}_2, \dots$ are distinct maximal ideals of R. Then, we product a chain

$$\mathfrak{m}_1 \supsetneq \mathfrak{m}_1\mathfrak{m}_2 \supsetneq \mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3 \supsetneq \dots$$

   Note that equality cannot occur: if $\mathfrak{m}_1 \cdots \mathfrak{m}_n = \mathfrak{m}_1 \cdots \mathfrak{m}_{n+1}$, then $\mathfrak{m}_1 \cdots \mathfrak{m}_n \subseteq \mathfrak{m}_{n+1}$, so the primeness of $\mathfrak{m}_{n+1}$ implies $\mathfrak{m}_i \subseteq \mathfrak{m}_{n+1}$ for some i, which is a contradiction. Thus, we have an infinite descending chain. ☐

Example 5.3.4.

Let $R = \mathbb{C}[x_1, \dots, x_n]/I$, and suppose that the only point in $\operatorname{Spec} R$ is $\vec{0}$. Thus, $(x_1, \dots, x_n)$ is going to be the unique maximal ideal, and $\mathfrak{m}^k = 0$ in R for some k. Therefore, if I is an ideal satisfying

$$(x_1, \dots, x_n)^k \subset I \subset (x_1, \dots, x_n),$$

then $\mathbb{C}[x_1, \dots, x_n]/I$ is Artinian. For example, the ring

$$\mathbb{C}[x]/(x^3, x^2y, xy, xy^5)$$

is Artinian.

§5.4 Problems

Problem 5.A. Let A be a Noetherian ring. Prove that an A-module is finitely-generated if and only if it is finitely-presented.

Problem 5.B. (a) Let A be a Noetherian ring and $\phi : A \to A$ be a surjective ring morphism. Prove that ϕ is an isomorphism.

(Hint: consider $\operatorname{Ker} \phi^n$.)

(b) Let A be a ring, and let M be a Noetherian module. Prove that every surjective module morphism $\phi : M \to M$ is an isomorphism. (Notice that this is a special case of Problem 2.E. You are asked to come up with a different proof.)

(c) Prove that (a) and (b) holds when "Noetherian" is replaced with "Artinian" and "surjecitve" is replaced with "injective".

Problem 5.C. Is the ring of algebraic integer (i.e., the integral closure of $\mathbb{Z}$ in $\overline{\mathbb{Q}}$) Noetherian?

Problem 5.D. Let A be a Noetherian ring. Prove that the formal series ring

$$A[[x]] := \{a_0 + a_1x + a_2x^2 + \dots : a_0, a_1, \dots, \in A\}$$

is Noetherian.

Problem 5.E. Let A be a ring such that A is Noetherian, $\operatorname{Spec} A$ is connected, and $A_{\mathfrak{p}}$ is a domain for all prime ideal $\mathfrak{p}$. Prove that A is a domain.

Problem 5.F. Let k be a field and A be a finitely-generated k-algebra. Prove that A is Artinian if and only if $\dim_k A$ is finite. (There is a very short solution.)

6 Associated Primes and Primary Decomposition

In this chapter, we will discuss primary decomposition, which is a theory that tries to decompose a general ring into a simpler set of ideals, called **primary ideals**.

Many theorems in this chapter requires Noetherian assumption. We will try to be careful about which part requires Noetherian hypothesis, but for most part, you should assume that all rings are Noetherian.

§6.1 Associated Primes

§6.1.1 Definition

Definition 6.1.1 (Associated primes)**.**

Let M be an A-module. A prime ideal $\mathfrak{p} \subset A$ is an **associated prime** M if there exists $x \in M$ for which $\operatorname{Ann}(x) = \mathfrak{p}$.

The set of associated primes is (unfortunately) denoted $\operatorname{Ass}(M)$ (or $\operatorname{Ass}_A(M)$ if the ground ring is not clear).

Equivalent definitions: $\mathfrak{p} \in \operatorname{Ass}(M)$ iff the following (equivalent) conditions hold:

- there exists $x \in M$ such that the map $A \xrightarrow{\cdot x} M$ has kernel $\mathfrak{p}$.
- there exists an injective map $A/\mathfrak{p} \to M$.

Let's do some examples.

Example 6.1.2.

We have some examples for $\mathbb{Z}$ module.

- If $M = \mathbb{Z}/(p^a q^b)$, then $\operatorname{Ass}(M) = \{(p), (q)\}$, where $(p) = \operatorname{Ann}(p^{a-1}q^b)$, $(q) = \operatorname{Ann}(p^a q^{b-1})$.
- If $M = \mathbb{Z} \oplus \mathbb{Z}/2$, then $\operatorname{Ass}(M) = \{(0), (2)\}$.
- More generally, it is easy to show that $\operatorname{Ass}(M \oplus N) = \operatorname{Ass} M \cup \operatorname{Ass} N$.

§6.1.2 Basic Properties

Proposition 6.1.3.

We have the following.

(a) If $x \in M$ and $\operatorname{Ann}(x) = \mathfrak{p}$. Suppose that $0 \neq y \in Ax$, then $\operatorname{Ann}(y) = \mathfrak{p}$ also.

(b) $\operatorname{Ass}(A/\mathfrak{p}) = \{\mathfrak{p}\}$.

▶ *Proof.* (a) We have $Ax \simeq A/\mathfrak{p} \subset M$, and since $A/\mathfrak{p}$ is a domain and $y \neq 0$, we have $\operatorname{Ann}_{A/\mathfrak{p}} y = (0)$. Thus, $\operatorname{Ann}_A y = \mathfrak{p}$.

(b) Follows directly from (a). ☐

We now prove that there exists at least one associated prime.

Theorem 6.1.4 (Existence).

If A is Noetherian and $y \neq 0 \in M$, then there exists a prime $\mathfrak{p} \in \operatorname{Ass}(M)$ such that $\mathfrak{p} \supseteq \operatorname{Ann}(y)$.

In particular, if $M \neq 0$, then $\operatorname{Ass}(M) \neq \emptyset$.

▶ *Proof.* Make a poset

$$\Sigma = \{\operatorname{Ann}(x) : x \neq 0 \in M\}$$

ordered by inclusion.

We claim that every maximal element must be in $\operatorname{Ass}(M)$. To show this, suppose $I \in \Sigma$ is maximal element, so $I = \operatorname{Ann}(x)$ for some $x \in M$. It suffices to that I is prime. To that end, given $f, g \in A$ and $fg \in I$. Then, $(fg)x = 0$.

Assume that $g \notin I$. Thus, $gx \neq 0$. Then, we have that $(I, f) \subset \operatorname{Ann}(gx) \in \Sigma$, but I is maximal in Σ, so the only way this could happen is $\operatorname{Ann}(gx) = I$ and $f \in I$.

Finally, if $\operatorname{Ann}(y)$ is not maximal in Σ, we keep climbing up the poset, forming an infinite ascending chain that must stabilize because A is Noetherian. The poset must stabilize at a maximal element of Σ, which is in $\operatorname{Ass}(M)$ by the above claim. ☐

Remark 6.1.5.

Theorem 6.1.4 does not hold when A is not Noetherian. Example: $R = M = C(\mathbb{R}, \mathbb{R})$, the ring of continuous functions on a real line.

Corollary 6.1.6.

We have

$$\bigcup_{\mathfrak{p} \in \operatorname{Ass}(M)} \mathfrak{p} = \bigcup_{y \neq 0 \in M} \operatorname{Ann}(y) = \{\text{zero divisors of } M\}.$$

We now show that for a Noetherian module, there are finitely many associated primes.

Theorem 6.1.7 (Finiteness).

(a) If we have a short exact sequence of A-modules

$$0 \longrightarrow L \xrightarrow{\phi} M \xrightarrow{\pi} N \longrightarrow 0,$$

then

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

(b) If M is a Noetherian A-module, then $\operatorname{Ass}(M)$ is finite.

▶ *Proof.* (a) For the first containment, we have the composition $0 \to A/\mathfrak{p} \to L \xrightarrow{\phi} M$ of injective maps, therefore, $\mathfrak{p} \in \operatorname{Ass}(M)$ also.

We now prove the second containment. Let $\mathfrak{p} \in \operatorname{Ass}(M)$, so there exists injective map $\alpha : A/\mathfrak{p} \to M$. By viewing L as a submodule of M, we assume that $L = \operatorname{Ker} \pi$. We have two cases.

- **If $\operatorname{Im}(\alpha) \cap L = 0$**, then $\pi \circ \alpha$ is an injective from $A/\mathfrak{p} \to N$, and so $\mathfrak{p} \in \operatorname{Ass}(N)$.
- **Otherwise**, there exists $y \in \operatorname{Im}(\alpha) \cap L$. By Proposition 6.1.3 (a), we have that $\operatorname{Ann}(y) = \mathfrak{p}$, so $\mathfrak{p} \in \operatorname{Ass}(L)$.

(b) It suffices to make a chain of submodules

$$0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M$$

such that $M_i/M_{i-1} = A/\mathfrak{p}_i$ for prime ideal $\mathfrak{p}_i$. If we have this, then (a) gives $\operatorname{Ass}(M) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

To prove this, by Theorem 6.1.4, pick $\mathfrak{p}_1 \in \operatorname{Ass}(M)$, so there exists element $x_1 \in M$ such that $\operatorname{Ann}_M(x_1) = \mathfrak{p}_1$. Thus, we let $M_1 = Ax_1 \simeq A/\mathfrak{p}_1$.

If $M_1 = M$, then we are done. Otherwise, by Theorem 6.1.4, pick $\mathfrak{p}_2 \in \operatorname{Ass}(M/M_1)$, so there exists element $x_2 \in M$ such that $\operatorname{Ann}_{M/M_1}(x_2) = \mathfrak{p}_2$. Therefore, $M_2 = Ax_2$ satisfies $M_2/M_1 = A/\mathfrak{p}_2$. Continue this process forever, and it must terminate because M is a Noetherian A-module. ☐

Example 6.1.8.

Consider the exact sequence

$$0 \to \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \to \mathbb{Z}/2 \to 0.$$

Then, we have $\operatorname{Ass} M = \{(0)\} \neq \operatorname{Ass}(L) \cup \operatorname{Ass}(N) = \{(0), (2)\}$.

Theorem 6.1.9.

(a) For any multiplicative set $S \subseteq A$, we have

$$\operatorname{Ass}_{S^{-1}A}(S^{-1}M) = \{S^{-1}\mathfrak{p} : \mathfrak{p} \in \operatorname{Ass}_A(M) \text{ such that } \mathfrak{p} \cap S = \emptyset\}.$$

(b) If A is Noetherian, M is finitely-generated, and $\mathfrak{p}$ is a prime ideal minimal among those containing $\operatorname{Ann}(M)$, then $\mathfrak{p} \in \operatorname{Ass}(M)$.

▶ *Proof.* (a) Mostly definition-chasing.

If $\mathfrak{p} \in \operatorname{Ass}_A(M)$ and $\mathfrak{p} \cap S = \emptyset$, then there is an injective map $R/\mathfrak{p} \hookrightarrow M$, which turns to $S^{-1}(A/\mathfrak{p}) = S^{-1}A/S^{-1}\mathfrak{p} \hookrightarrow S^{-1}M$, where we used Theorem 3.2.3 to commute localization inside quotient and see that it preserves injectivity. This gives $S^{-1}\mathfrak{p} \in \operatorname{Ass}_{S^{-1}A}(S^{-1}M)$.

Conversely, by Theorem 3.1.10, suppose that $S^{-1}\mathfrak{p} \in \operatorname{Ass}_{S^{-1}A}(S^{-1}M)$, where $\mathfrak{p} \cap S = \emptyset$, then we have an injective map $S^{-1}(A/\mathfrak{p}) \hookrightarrow S^{-1}M$. Suppose that this map takes 1 to x/s for some $x \in M$ and $s \in S$. We claim that $\operatorname{Ann}(x) = \mathfrak{p}$. To see this, suppose that $rx = 0$ for some $r \in A$. Then, $r\frac{x}{s} = 0$, so $r = 0$ in $S^{-1}(A/\mathfrak{p})$. Therefore, $ur = 0 \pmod{\mathfrak{p}}$ for some $u \in S$, and since $S \cap \mathfrak{p} \neq \emptyset$, we have $u \notin \mathfrak{p}$, so $r \in \mathfrak{p}$.

(b) First, we show that $M_\mathfrak{p} \neq 0$. Suppose $M_\mathfrak{p} = 0$. Suppose $x_1, x_2, \ldots, x_n$ generates M. Then, since the image of x_i in $M_\mathfrak{p}$ is 0, there exists $a_i \notin \mathfrak{p}$ such that $a_i x_i = 0$. Now, note that the product $a_1 \cdots a_n$ annihilates $x_1, \ldots, x_n$, and hence annihilates M, so $a_1 \cdots a_n \in \operatorname{Ann}(M)$, but $a_1 \cdots a_n \notin \mathfrak{p}$, a contradiction.

By Theorem 6.1.4, we have $\operatorname{Ass}_{A_\mathfrak{p}}(M_\mathfrak{p}) \neq \emptyset$. However, from (a), this set correspond to $\mathfrak{q} \in \operatorname{Ass}(M)$ such that $\mathfrak{q} \subseteq \mathfrak{p}$. Note that $\mathfrak{q}$ contains $\operatorname{Ann}(M)$, so by minimality, $\mathfrak{q} = \mathfrak{p}$. Hence $\mathfrak{p} \in \operatorname{Ass}(M)$. ☐

§6.1.3 Local Property and Associated Primes

Corollary 6.1.10 (Local Property and Associated Primes).

Let A be Noetherian ring, M be an A-module. Suppose that $x \in M$ such that for all $\mathfrak{p} \in \operatorname{Ass}(M)$, the image of x in $M_\mathfrak{p}$ is 0. Then, $x = 0$.

▶ *Proof.* Assume $x \neq 0$. By Theorem 6.1.4, $\operatorname{Ann}(x)$ is contained in some associated prime $\mathfrak{p}$. Then, if the image of x in $M_\mathfrak{p}$ is 0, then $ax = 0$ for some $a \notin \mathfrak{p}$. This contradicts $\operatorname{Ann}(x) \subseteq \mathfrak{p}$. ☐

This gives the following two corollaries.

Corollary 6.1.11.

Let A be Noetherian and M be an A-module. Then,

(a) If K is a submodule of M, then $K = 0$ if and only if $K_\mathfrak{p} = 0$ for all $\mathfrak{p} \in \operatorname{Ass}(M)$.

(b) If $\phi : M \to N$, then ϕ is injective if and only if $\phi_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ is injective for $\mathfrak{p} \in \operatorname{Ass}(M)$.

▶ *Proof.* (a) Clear from Corollary 6.1.10.

(b) Apply (a) with $K = \operatorname{Ker}\phi \subseteq M$. ☐

§6.2 Primary Decomposition

For this entire section, let A be a a Noetherian ring.

The goal of this section is to develop the theory that decompose ideals of A into simpler ideals. We have seen two special cases of this.

- If A is a PID (hence UFD), then an ideal $I = (f)$ can be written in form
$$I = (p_1)^{a_1} \cdots (p_k)^{a_k} = \bigcap_{i=1}^{k} (p_i)^{a_i},$$
where $p_1, \ldots, p_k$ are prime elements of A. In order words, any ideal is an intersection of prime powers. Special cases of this include $A = \mathbb{Z}$ and $A = k[x]$.
- From Section 5.2.2, any radical ideal I is an intersection of prime ideals minimal among those containing I.

Our theorem will be that for any Noetherian ring A, any ideal I can be written as the intersection of a special kind of ideas called primary ideals. When A is a PID, primary ideals coincide with prime powers. However, the notion of primary ideals is more general.

§6.2.1 Primary Ideals

Definition 6.2.1.

An ideal $Q \subsetneq A$ is

- **primary** if whenever $fg \in Q$, either $f \in Q$ or $g^n \in Q$ for some $n \geq 1$.
- **$\mathfrak{p}$-primary** (where $\mathfrak{p}$ is a prime ideal) if Q is primary and $\sqrt{Q} = \mathfrak{p}$.

In other words, Q is primary if and only if every zero divisor in A/Q is nilpotent. For example, prime powers in $\mathbb{Z}$ are primary.

Lemma 6.2.2.

If Q is primary, then $\sqrt{Q}$ is prime.

▶ *Proof.* Note that

$$fg \in \sqrt{Q} \implies f^n g^n \in Q \implies f^n \in Q \text{ or } g^{mn} \in Q.$$

Either way, this implies that $f \in \sqrt{Q}$ or $g \in \sqrt{Q}$. ☐

In the definition above, since we assumed that A is Noetherian, $\mathfrak{p}$ is finitely generated, so there exists $m > 0$ such that $\mathfrak{p}^m \subset Q \subset \mathfrak{p}$.

Warning 6.2.3.

- **If $\sqrt{Q}$ is prime, then Q is not necessarily primary.** For example,

  $$I = (x^2, xy) \subset \mathbb{C}[x, y] \implies \sqrt{I} = (x).$$

  We have $(x^2) \subset I \subset (x)$, but I is not primary. We have $xy \in I$ but $x \notin I$ and $y \notin \sqrt{I}$.

- **Prime powers are not necessarily primary**. To see an example, take

  $$A = \frac{\mathbb{C}[x, y, z]}{(xz - y^2)}, \ \mathfrak{p} = (x, y).$$

  Then, we claim that $\mathfrak{p}^2 = (x^2, xy, y^2)$ is not primary. To see why, note that $xz = y^2$, but $x \notin \mathfrak{p}^2$ and $z \notin \mathfrak{p}$.

Proposition 6.2.4.

Given an ideal $Q \subset A$ such that $\sqrt{Q} = \mathfrak{m}$ is maximal, then Q is $\mathfrak{m}$-primary.

▶ *Proof.* Suppose that $f \notin Q$, then the ideal $I = \{g \in A : fg \in Q\}$ is a proper ideal of A, so it is contained in a maximal ideal $\mathfrak{m}'$. In particular, we have $Q \subset I \subset \mathfrak{m}'$. Thus, we have $\sqrt{Q} \subset \sqrt{\mathfrak{m}'} \implies \mathfrak{m} \subset \mathfrak{m}'$, and so $\mathfrak{m} = \mathfrak{m}'$. Thus, $I \subset \mathfrak{m}$. Therefore, if $fg \in Q$, we must have $g \in I$, so $g \in \mathfrak{m}$ or $g^n \in Q$ for some I. ☐

We now connect primary ideal to associated primes we studied earlier in the previous section.

Theorem 6.2.5 (Primary if and only if one associated prime)**.**

Q is $\mathfrak{p}$-primary if and only if $\operatorname{Ass}(A/Q) = \{\mathfrak{p}\}$.

▶ *Proof.* (⇒). Pick $x \in A$ such that the image $\overline{x} \in A/Q$ is nonzero and such that $\operatorname{Ann}_{A/Q}(\overline{x})$ is a prime ideal. Then, we observe that

$$\begin{aligned} Q \subseteq \operatorname{Ann}_{A/Q}(\overline{x}) &= \{y \in A : xy \in Q\} \\ &\subseteq \{y : y^n \in Q \text{ for some } n \geq 0\} && \text{(def. of primary ideal)} \\ &\subseteq \sqrt{Q} = \mathfrak{p}. \end{aligned}$$

Since $\operatorname{Ann}_{A/Q}(\overline{x})$ is prime ideal, taking radical both sides gives $\mathfrak{p} \subseteq \operatorname{Ann}_{A/Q}(\overline{x}) \subseteq \mathfrak{p}$, so $\operatorname{Ann}_{A/Q}(\overline{x}) = \mathfrak{p}$, so any associated prime must be $\mathfrak{p}$. Since $\operatorname{Ass}(A/Q) \neq \emptyset$ (Theorem 6.1.4), it follows that $\operatorname{Ass}(A/Q) = \{\mathfrak{p}\}$.

(⇐) If $\operatorname{Ass}(A/Q) = \{\mathfrak{p}\}$, then any nonzero submodule of A/Q also has only $\mathfrak{p}$ as associated prime. Given $0 \neq M \subset A/Q$, we note by definition of radical that

$$\sqrt{\operatorname{Ann} M} = \bigcap_{\mathfrak{q} \supseteq \operatorname{Ann}(M)} \mathfrak{q} = \bigcap_{\mathfrak{q} \in \operatorname{Ass}(M)} \mathfrak{q} = \mathfrak{p} \tag{6.1}$$

(where we used Theorem 6.1.9 in the middle equality). In particular, plugging $M = A/Q$ into (6.1) gives $\sqrt{Q} = \mathfrak{p}$.

Now, given f, g such that $fg \in Q$. If $f \notin Q$, then we reduce $0 \neq \overline{f} \in A/Q$, giving a submodule $M = A\overline{f} \subset A/Q$ generated by single element $\overline{f}$ We have $g \in \operatorname{Ann}(M)$, so using (6.1) with this choice of M, we have $g \in \sqrt{\operatorname{Ann}(M)} = \mathfrak{p}$, so $g^n \in \mathfrak{p}$ for some n. Hence, Q is primary. ☐

Remark 6.2.6.

All the theory above generalizes by replacing A with arbitrary modules M. In that case, a submodule $N \subseteq M$ is $\mathfrak{p}$-primary if $\operatorname{Ass}(M/N) = \{\mathfrak{p}\}$. The theorem then says that any submodule of M can be expressed as an intersection of $\mathfrak{p}$-primary submodules. Moreover, the set of primes that appear is precisely $\operatorname{Ass}(M)$.

§6.2.2 Primary Decomposition

We are now ready to state primary decomposition theorem.

Definition 6.2.7 (Primary decoposition)**.**

Given $I \subset A$, a **primary decomposition** of I is an expression

$$I = \bigcap_{i=1}^{n} Q_i$$

such that

- Q_i is $\mathfrak{p}_i$-primary for all i.
- $I \not\subset \bigcap_{i \neq j} Q_i$ for each j.
- $\mathfrak{p}_i \neq \mathfrak{p}_j$ for all i, j.

The second one is to clean out redundant elements. For the third one, if $\mathfrak{p}_i = \mathfrak{p}_j$ for some i and j, then the following lemma tells us that we can combine Q_i and Q_j into a single ideal.

Lemma 6.2.8.

If Q_1 and Q_2 are both $\mathfrak{p}$-primary, then so is $Q_1 \cap Q_2$.

▶ *Proof.* The map $A/(Q_1 \cap Q_2) \longrightarrow A/Q_1 \oplus A/Q_2$ is injective. Thus, by Theorem 6.1.7 (a),

$$\operatorname{Ass}(A/(Q_1 \cap Q_2)) \subseteq \operatorname{Ass}(A/Q_1) \cup \operatorname{Ass}(A/Q_2) = \{\mathfrak{p}\},$$

so since $\operatorname{Ass}(A/(Q_1 \cap Q_2)) \neq \emptyset$ (Theorem 6.1.4), it follows that $\operatorname{Ass}(A/(Q_1 \cap Q_2)) = \{\mathfrak{p}\}$, so the result follows from Theorem 6.2.5. ☐

Thus, to prove that primary decomposition exists, we must show that any ideal can be written as intersection of primary ideals; there is no need to care about the second and third condition.

Let us demonstrate some examples of what primary decomposition look like.

Example 6.2.9.

Consider

$$I = (x^2, xy) \subset \mathbb{C}[x, y].$$

This ideal is contained in the maximal ideal (x, y), and in fact, we have

$$(x^2, xy) = (x) \cap (x, y)^2,$$

which is one primary decomposition. However, there are also other decompositions. For example,

$$\begin{aligned} I &= (x) \cap (x^2, y) \\ &= (x) \cap (x^2 y - \alpha x). \end{aligned}$$

Example 6.2.10.

Consider

$$A = \frac{\mathbb{C}[x, y, z]}{(xz - y^2)}, \quad \mathfrak{p} = (x, y).$$

We have seen in Warning 6.2.3 that $\mathfrak{p}^2$ is not primary. Its primary decomposition looks like

$$\mathfrak{p}^2 = (x) \cap (x, y, z)^2.$$

We now prove that primary decomposition exists.

Theorem 6.2.11.

If A is Noetherian, then primary decomposition always exists.

To prove this theorem, we first make the definition.

Definition 6.2.12.

An ideal $I \subset A$ is **indecomposable** if whenever $I = J \cap K$ for ideals J and K, then $I = J$ or $I = K$.

Thus, by repeatedly breaking down decomposable ideals, any ideal I must be written as $J_1 \cap J_2 \cap \cdots \cap J_n$, where J_i indecomposable. Since A is Noetherian, the process must stop.

Thus, to prove that primary decomposition exists, it suffices to show the following.

Proposition 6.2.13.

If Q is indecomposable ideal of a Noetherian ring A, then Q is primary.

▶ *Proof.* By replacing A with A/Q, we may assume that $Q = (0)$.

If $xy = 0$, then we have

$$y \in \operatorname{Ann}(x) \subset \operatorname{Ann}(x^2) \subset \operatorname{Ann}(x^3) \subset \dots$$

This chain must stabilize, so for some k, we have $\operatorname{Ann}(x^k) = \operatorname{Ann}(x^{k+1})$.

Now, we claim $(x^k) \cap (y) = (0)$. To see why, if $a \in (x^k) \cap (y)$, then $ax = 0$ and $a = bx^k$. Thus, $bx^{k+1} = 0 \implies b \in \operatorname{Ann}(x^{k+1}) = \operatorname{Ann}(x^k)$. Thus, $a = bx^k = 0$ as claimed.

Since (0) is indecomposable, we must have either $(x^k) = (0)$ or $(y) = (0)$. Thus, $x^k = 0$ or $y = 0$, as desired. □

§6.2.3 Quasi-uniqueness of Primary Decomposition

Unfortunately, as seen above, primary decompositions are not unique. However, we can say something about uniqueness.

Theorem 6.2.14 (Quasi-uniqueness).

Let A be a Noetherian ring. If an ideal I has a primary decomposition $I = \bigcap Q_i$ such that Q_i is $\mathfrak{p}_i$-primary, then $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\} = \operatorname{Ass}(A/I)$.

In particular, the set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ is unique.

▶ *Proof.* Consider the direct sum of projection

$$f : A \to \bigoplus_{i=1}^{n} A/Q_i.$$

We have $\ker f = I$. Thus, A/I is a subring of these direct sums. In particular,

$$\operatorname{Ass}(A/I) \subseteq \operatorname{Ass}\left(\bigoplus_{i=1}^{n} A/Q_i\right) = \bigcup_{i=1}^{n} \operatorname{Ass}(A/Q_i) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}.$$

We now show that for each i, we have $\mathfrak{p}_i \in \operatorname{Ass}(A/I)$. Let

$$N = \frac{\bigcap_{j \neq i} Q_j}{I} \subset A/I.$$

By irredundant condition, $N \neq 0$. Moreover, we have the composition $N \to A/I \to \bigoplus_{j=1}^{n} A/Q_j$ is zero on each factor $j \neq i$, and it is injective onto A/Q_i. Thus, $\operatorname{Ass}(N) \subset \operatorname{Ass}(A/Q_i) = \{\mathfrak{p}_i\}$, so $\operatorname{Ass}(N) = \{\mathfrak{p}_i\}$ (because it must not be empty), and so $\mathfrak{p}_i \in \operatorname{Ass}(A/I)$. □

§6.3 Problems

Problem 6.A. Let M and N be two R-modules. Prove that $\operatorname{Ass}(M \oplus N) = \operatorname{Ass}(M) \cup \operatorname{Ass}(N)$.

Problem 6.B. Let $R = \mathbb{C}[x, y]/(xy)$-module and let M be an R-module with generators a and b and a single relation $xa + yb = 0$ (the same module as in Problem 2.A). Determine $\operatorname{Ass} M$.

Problem 6.C. Let A be a Noetherian ring and M be a finitely-generated module. Suppose that I is an ideal of A with property that for every $a \in I$, there exists $0 \neq m_a \in M$ such that $am_a = 0$. Prove that there exists $0 \neq m \in M$ such that $I \cdot m = 0$.

Hint: prime avoidance, Problem 1.E.

Problem 6.D. Let R be a Noetherian ring and I be an ideal.

(a) Explain why every prime ideal minimal over I (i.e., minimal among those containing I) must be an associated prime of R/I.

(b) If R/I is reduced (i.e., I is a radical ideal), prove that every associated prime of R/I is minimal over I.

Problem 6.E. Let A be a Noetherian domain and $r \in \operatorname{Frac} A$. Suppose that for every $f \in A$ and $\mathfrak{p} \in \operatorname{Ass}(A/(f))$, we have $r \in A_{\mathfrak{p}}$. Prove that $r \in A$.

(Hint: suppose that $r = a/b$. Let M be a submodule of $A/(b)$ generated by a and consider $\mathfrak{p} \in \operatorname{Ass} M$.)

Problem 6.F. Let R be a ring and Q be a primary ideal. Prove that $S^{-1}Q$ is either equal to $S^{-1}R$ or a primary ideal in $S^{-1}R$.

Problem 6.G. Find a primary decomposition of the following ideals.

(a) Ideal $(x+y, xy)$ of $\mathbb{C}[x,y]$.

(b) Ideal $(xy, x-yz)$ of $\mathbb{C}[x,y,z]$.

(c) Ideal (x^2, xy^2, y^2z, xz) of $\mathbb{C}[x,y,z]$.

7 Discrete Valuation Rings and Dedekind Domains

In this chapter, we are going to talk about a special kind of local rings, discrete valuation rings, and its non-local analogue, Dedekind domain.

Recall that the (Krull) **dimension** of a ring is the longest chain of prime ideals in a ring $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \dots \mathfrak{p}_d$. Rings of dimension 0 are Artininan rings. The next level of complexity is studying domains of dimension 1. In this case, every *nonzero* prime ideal is maximal. The two main examples to keep in mind are

- ring of integers $\mathcal{O}_K$ in a number field;
- $\operatorname{Spec} R$ of an algebraic curve.

§7.1 Discrete Valuation Ring

§7.1.1 Definition and Basic Properties

Definition 7.1.1 (Discrete valuation and DVR)**.**

Let K be a field. A **discrete valuation** on K a surjective function $v : K \to \mathbb{Z} \cup \{\infty\}$ satisfying the following:

- $v(xy) = v(x) + v(y)$.
- $v(x + y) \geq \min(v(x), v(y))$.
- $v(x) = \infty$ if and only if $x = 0$.

For any discrete valuation, one defines the ring

$$V = \{x \in K : v(x) \geq 0\}$$

(it's easy to check that it forms a ring). Every ring arises from discrete valuation this way is called a **discrete valuation ring (DVR)**.

Example 7.1.2.

Here are two examples from both Number Theory and Algebraic geometry that looks similar.

- For any prime p, the ring
$$\mathbb{Z}_{(p)} = \left\{\tfrac{a}{b} \in \mathbb{Q} : p \nmid b\right\}$$
is a DVR because it comes with the p-adic valuation $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$, where $v_p(r)$ is the exponent of p in the prime factorization of r.

- For any field k, the ring

$$k[x]_{(x)} = \left\{\tfrac{f(x)}{g(x)} \in k(x) : g(0) \neq 0\right\}$$

is a DVR. The valuation is define by for each $f \in k[x]$, $v(f)$ is the exponent of x in factorization of f, and then extend it by $v(f/g) = v(f) - v(g)$.

Proposition 7.1.3 (Properties of DVR)**.**

Let V be a DVR with corresponding valuation $v : K \to \mathbb{Z} \cup \{\infty\}$, where $K = \operatorname{Frac} V$.

Fix an element $\pi \in V$ with $v(\pi) = 1$, then every nonzero ideal of V is generated by (π^k) for some integer k.

Consequence of this facts include

- V is a PID (hence Noetherian, UFD, and integrally closed).
- V is local ring with unique maximal ideal (π).
- The only prime ideals of V are (0) or (π).
- V has Krull dimension 1.

▶ *Proof.* Let I be a nonzero ideal of V. Let $m = \min\{v(x) : x \in I\}$, and take an element x such that $v(x) = m$. We claim that $I = (\pi^m)$.

In one direction, we have to show that $\pi^m \in I$. Observe that, $v(\pi^m x^{-1}) = mv(\pi) - v(x) = 0$, so $\pi^m x^{-1} \in V$, implying that $x \cdot \pi^m x^{-1} = \pi^m \in I$.

In another direction, given $y \in I$, then by minimality, we have $v(y) \geq m$. Thus, $v(y \cdot \pi^{-m}) \geq 0$, so $y \cdot \pi^{-m} \in V$, so $y \in (\pi^m)$. □

§7.1.2 Characterization of DVRs

We have the following big theorem.

Theorem 7.1.4 (Characterization of DVR)**.**

Let $(R, \mathfrak{m})$ be a local Noetherian domain with dimension 1 (i.e., $\mathfrak{m}$ is the only nonzero prime ideal). Let $k = R/\mathfrak{m}$ be the residue field and $K = \operatorname{Frac} R$. Then, the following are equivalent.

(a) R is a DVR.

(b) R is integrally closed in K.

(c) $\mathfrak{m}$ is principal.

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

(e) Every nonzero ideal is a power of $\mathfrak{m}$.

(f) There exists $\pi \in R$ such that all ideals are in form (0) or (π^n).

Remark 7.1.5 (DVR, integrally closed, and smoothness)**.**

If R is the ring obtained by localizing $k[x, y]/(f)$ at the maximal ideal $(x - a, y - b)$, then $\dim R = 1$ (by Theorem 4.5.4). Moreover, condition (d) $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$ is the easiest to check whether R is a DVR. Roughly speaking $\mathfrak{m}^2$ mods out the quadratic or higher term, so $\mathfrak{m}/\mathfrak{m}^2$

> only cares about linear approximation of f near point (a,b). Working out the details, it turns out that
>
> $$R \text{ is a DVR} \iff \text{at least one of } \left.\frac{\partial f}{\partial x}\right|_{(a,b)} \text{ and } \left.\frac{\partial f}{\partial y}\right|_{(a,b)} \text{ is nonzero,}$$
>
> and this is equivalent to that the curve $f(x,y)=0$ is smooth at (a,b). Thus, you should think of DVR as a spectrum of smooth object of dimension 1.
>
> Owing to Proposition 4.2.15, condition (b) gives an easy condition to check whether $k[x,y]/(f)$ is a integrally closed when k is algebraically closed; one simply needs to evaluate partial derivative of f and show that at no point do both $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ vanish.

► *Proof.* **(a) ⇒ (b).** True because R is a PID, hence UFD, and integrally closed (Proposition 4.2.5).

(b) ⇒ (c). This is the hardest implication. Let $a \neq 0 \in \mathfrak{m}$. We first claim that there exists n such that $\mathfrak{m}^n \subset (a)$. To prove this, $\operatorname{Spec} R/(a)$ has only one point, so $R/(a)$ is Artinian. Thus, in $R/(a)$, we have from Theorem 5.3.2 that $\overline{\mathfrak{m}}^n = 0$, so $\mathfrak{m}^n \subseteq (a)$[1]. We pick n minimal so that $\mathfrak{m}^{n-1} \subsetneq (a)$, so there exists $b \in \mathfrak{m}^{n-1} \setminus (a)$.

Let $x = \frac{a}{b} \in K$. Then, since $b \notin (a)$, we have $\frac{b}{a} \notin R$, so it is not integral.

- If $\frac{b}{a}\mathfrak{m} \subseteq \mathfrak{m}$, then by Cayley-Hamilton's theorem (Theorem 2.2.1) on module $\mathfrak{m}$ and the map of multiplication by $\frac{b}{a}$, we get that $\frac{b}{a}$ is integral, a contradiction.
- If $\frac{b}{a}\mathfrak{m} \subsetneq \mathfrak{m}$, then, we note that $b\mathfrak{m} \subseteq \mathfrak{m}^n \subseteq (a)$, so $b\mathfrak{m} \subseteq (a)$. Dividing by a both sides gives $\frac{b}{a}\mathfrak{m} \subseteq R$. Therefore, $\frac{b}{a}\mathfrak{m}$ is an ideal, but it is not contained in *the* maximal ideal $\mathfrak{m}$, so $\frac{b}{a}\mathfrak{m} = R$. Hence, $\mathfrak{m} = (a/b)$.

(c) ⇒ (d). Let $\mathfrak{m} = (\pi)$. Then, $\mathfrak{m}/\mathfrak{m}^2 = \operatorname{Span}(\overline{\pi})$, so $\dim_k \mathfrak{m}/\mathfrak{m}^2 \leq 1$. However, $\mathfrak{m}/\mathfrak{m}^2 \neq 0$ because if $\mathfrak{m} = \mathfrak{m}^2$, then by Nakayama (Corollary 2.2.5), $\mathfrak{m} = (0)$, contradiction. Thus, $\dim(\mathfrak{m}/\mathfrak{m}^2) = 1$.

(d) ⇒ (c). We have $\mathfrak{m}/\mathfrak{m}^2 = k\overline{\pi}$. Pick $\pi \in \mathfrak{m}$ lifting $\overline{\pi}$. Then, by Nakayama on lifting generators (Corollary 2.2.6), we have $\mathfrak{m} = (\pi)$.

(c) ⇒ (e). Suppose $\mathfrak{m} = (\pi)$. Now, given $I \subset R$, we claim that we can find k such that $I \subset (\pi^k)$ but $I \subsetneq (\pi^{k+1})$. If such k does not exist, then $I \subseteq (\pi^k)$ for all k, which means that we have an infinite ascending chain of ideals

$$I \subsetneq \pi^{-1}I \subsetneq \pi^{-2}I \subsetneq \dots,$$

contradicting the fact that R is Noetherian.

Having found such k, we pick $f \in I \setminus (\pi^{k+1})$, so $f = \pi^k g$ where $g \notin (\pi)$. Thus, g is a unit and so $(f) = (\pi^k) \subset I \subset (\pi^k)$, forcing equality, so $I = (\pi^k) = \mathfrak{m}^k$.

(e) ⇒ (f). If $\mathfrak{m} = \mathfrak{m}^2$, then Nakayama (Corollary 2.2.5) gives $\mathfrak{m} = (0)$, a contradiction. Thus, there exists $\pi \in \mathfrak{m}$ but $\pi \notin \mathfrak{m}^2$. Let $(\pi) = \mathfrak{m}^r$. Since $\pi \notin \mathfrak{m}^2$, it follows that $r = 1$. Thus, every ideal is of the form $\mathfrak{m}^n = (\pi^n)$.

(f) ⇒ (a). We define $v : R \to \mathbb{Z} \cup \{\infty\}$ as follows: for each $a \in R$, by (e), the ideal (a) must be in form (π^e) for some integer $e \geq 0$. We set $e = v(a)$. This v clearly satisfies

- $v(a+b) \geq \min(v(a), v(b))$; and
- $v(ab) = v(a)v(b)$ for all $a, b \in R$.

Now, extend v to K by $v(x/y) = v(x) - v(y)$. One can see that the above two properties still hold. Finally, we have to show that $a \in R$ if and only if $v(a) \geq 0$. The (⇒) direction is clear. For the (⇐) direction, suppose that $a, b \in R$ such that $v(a/b) \geq 0$, or $v(a) \geq v(b)$. Then, $(b) \subseteq (a)$, so b divides a, so $a/b \in R$. Hence, we conclude that v is a discrete valuation with valuation ring R. ☐

---

[1] Note that we are using the easy implication (b) implies (d) in Theorem 5.3.2. Thus, it is possible to avoid using this theorem.

§7.2 Dedekind Domain

§7.2.1 Definition and Unique Factorization

The definition of Dedekind Domain is in the proposition.

Proposition 7.2.1 (Dedekind Domain)**.**

Let R be a domain, Noetherian, and one-dimensional (every nonzero prime ideal is maximal). Then, the following are equivalent.

(a) R is integrally closed.

(b) Every localization of nonzero prime $R_\mathfrak{p}$ is a DVR.

(c) Every primary ideal is a power of a prime ideal.

We say that R is **Dedekind Domain** if it meets the (equivalent) conditions of the proposition.

▶ *Proof.* **(a) ⇔ (b).** Since being integrally closed is local (Proposition 4.2.14), we get that R is integrally closed if and only if $R_\mathfrak{p}$ is integrally closed for all nonzero prime ideal $\mathfrak{p}$. By Theorem 7.1.4 ((b) implies (a)), this is equivalent to $R_\mathfrak{p}$ being DVR for all nonzero prime ideal $\mathfrak{p}$.

(b) ⇒ (c). The (0)-primary ideal is clearly just (0). Thus, it suffices to consider only $\mathfrak{p}$-primary for all nonzero prime $\mathfrak{p}$. If Q is $\mathfrak{p}$-primary, then $Q_\mathfrak{p}$ sits inside a DVR $R_\mathfrak{p}$, so $Q_\mathfrak{p} = \mathfrak{p}^k R_\mathfrak{p}$, and so by contracting to R, we get that $Q = \mathfrak{p}^k$.

(c) ⇒ (b). Now, suppose (c) holds: every primary is a prime power. Let $\mathfrak{p}$ be any nonzero prime ideal of R, and consider any ideal $I \subset R_\mathfrak{p}$. Note that the only prime ideals of I and $R_\mathfrak{p}$ are (0) and $\mathfrak{p}$, so $\operatorname{Ass}(R_\mathfrak{p}/I) = \{\mathfrak{p}\}$ (it cannot be empty), so I is $\mathfrak{p}$-primary.

Thus, the contraction of I to R is $\mathfrak{p}$-primary, and so it must be a power of $\mathfrak{p}$. This means that $I = \mathfrak{p}^k$ for some k, and Theorem 7.1.4 ((e) implies (a)) concludes that $R_\mathfrak{p}$ is a DVR. ☐

Corollary 7.2.2.

In a Dedekind Domain, any ideal I can be factored uniquely to

$$I = \prod_{i=1}^{n} \mathfrak{p}_i^{a_i},$$

where $\mathfrak{p}_i$ are maximal ideals and $a_i \geq 0$.

▶ *Proof.* By primary decomposition, we have $I = \bigcap_{i=1}^n \mathfrak{p}_i^{a_i}$. By Chinese Remainder Theorem, it suffices to prove that $\mathfrak{p}_i^{a_i}$ and $\mathfrak{p}_j^{a_j}$ are coprime. But this follows from that $\mathfrak{p}_i$ and $\mathfrak{p}_j$ are coprime. ☐

We now give some examples of Dedekind Domain.

Example 7.2.3.

- PID's are Dedekind Domain because the localization at any nonzero prime ideal is PID, hence a DVR.
- The next theorem (Theorem 7.2.4) will show that the ring of integers $\mathcal{O}_K$ of any number field K is a Dedekind domain. This is a key example in number theory.

§7.2.2 Key Example: Extensions of Dedekind Domain

We will now discuss a way to construct a Dedekind Domain.

Theorem 7.2.4 (Extension of Dedekind domain is Dedekind domain)**.**

Let $A \subset K = \operatorname{Frac} A$ be a Dedekind Domain. Let $K \subset L$ be a finite, **separable** extension. Let B be an integral closure of A inside L. Then, B is a Dedekind domain.

To prove that B is a Dedekind domain, we need to show that B is

- **integrally closed**: obvious;
- **one-dimension:** follows from Theorem 4.5.3;
- **Noetherian:** that is (surprisingly) the hard part.

The hard part is to prove that B is Noetherian. This will require the fact that $L \supset K$ is separable.

First, let us recall what separable means.

Definition 7.2.5 (Separable extension)**.**

A field extension L/K is **separable** if and only if for any $\alpha \in L$, the minimal polynomial of α over K has distinct roots in $\overline{K} \supset K$.

Example 7.2.6 (Non-seperable extension)**.**

Let $K = \mathbb{F}_p(t)$ and $L = K[x]/(x^p - t)$. Then, if α is the image of x in $K[x]/(x^p - t)$, then the minimal polynomial of α is $x^p - t = (x - \alpha)^p$.

We use the following fact from basic field theory: "L/K is separable if and only if there exists $[L : K] = n$ distinct embeddings $\sigma_1, \dots, \sigma_n : L \to \overline{K}$". If we base change a separable extension to algebraic closure, we have

$$\overline{K} \otimes_K L = \overline{K} \otimes_K \frac{K[x]}{(f)} = \frac{\overline{K}[x]}{(f)} = \frac{\overline{K}[x]}{\prod_{i=1}^n (x - \alpha_i)} \simeq \prod_{i=1}^n \overline{K}.$$

Then, we have the map

$$\begin{aligned} L &\to \overline{K} \otimes_K L \to \textstyle\prod_{i=1}^n \overline{K} \\ y &\mapsto \quad 1 \otimes y \quad \mapsto (\sigma_1(y), \dots, \sigma_n(y)). \end{aligned}$$

Now, let's go back to Theorem 7.2.4. Recall that the tricky part is to prove that B is Noetherian. This is hard because

Remark 7.2.7.

If A is Noetherian, then the integral closure of A inside $\operatorname{Frac} A$ need not be Noetherian.

However, we have the following result.

Theorem 7.2.8.

Let A be Noetherian and integrally closed inside fraction field $A \subset K$. Let L be a finite, separable extension of K. Let B be the integral closure of A in L. Then, B is finitely-generated A-module.

This theorem immediately proves Theorem 7.2.4.

▶ *Proof of Theorem 7.2.8.* To prove this theorem, we need the notion of trace. Define the trace map

$$\begin{aligned} \mathrm{Tr}_{L/K} : L &\to K \\ y &\mapsto \mathrm{Tr}(\underbrace{z \mapsto yz}_{M_y}). \end{aligned}$$

For separable case, one can calculate trace using the basis of $\overline{K} \otimes L = \prod \overline{K}$. In particular, we have $\mathrm{Tr}(M_y) = \mathrm{Tr}(M_{1\otimes y})$. However, if we write this in a basis of $\prod \overline{K}$, we have

$$M_{1\otimes y} = M_{(\sigma_1(y),\dots,\sigma_n(y))} = \begin{pmatrix} \sigma_1(y) & \dots & 0 \\ & \ddots & \\ 0 & \dots & \sigma_n(y) \end{pmatrix},$$

and so we have $\mathrm{Tr}_{L/K}(y) = \sigma_1(y) + \cdots + \sigma_n(y)$.

We now have the following observations.

1. If $b \in B$, then $\mathrm{Tr}_{L/K}(b) \in A$.

   Proof. We have $\mathrm{Tr}_{L/K}(b) = \sum_{i=1}^n \sigma_i(b) \in K$. Since b is integral, we have $\sigma_i(b)$ integral, so $\mathrm{Tr}_{L/K}(b)$ is integral over A, so $\mathrm{Tr}_{L/K}(b) \in A$.

2. The trace pairing $\langle \bullet, \bullet \rangle : L \times L \to K$ by $\langle y_1, y_2 \rangle = \mathrm{Tr}_{L/K}(y_1 y_2)$ is nondegenerate. (i.e., if $y \neq 0$, there exists $z \in L$ for which $\mathrm{Tr}_{L/K}(yz) \neq 0$).

   Proof. We need to check this after tensoring with $\overline{K}$, in which get $\prod K$. The pairing then is

   $$\langle (z_1, \dots, z_n), (w_1, \dots, w_n) \rangle = z_1 w_1 + \cdots + z_n w_n,$$

   and it's easy to see that this is non-degenerate.

We now prove the theorem. Pick a basis $x_1, \dots, x_n$ of L over K. By scaling x_i by $a \in A$, one can assume $x_i \in B$ (just let a be the product of all denominators).

The next step is to define the trace dual. Pick $y_1, \dots, y_n \in L$ such that

$$\mathrm{Tr}(x_i y_j) = \begin{cases} 1 & i = j \\ 0 & i \neq j. \end{cases}$$

Then, we are almost one. We claim

$$B \subset \bigoplus_{i=1}^n A y_i.$$

Why? If $b \in B$, write $b = \sum c_i y_i$, then by taking trace pairing both sides, we get that $\mathrm{Tr}_{L/K}(x_i b) = c_i \in A$, so we are done. That equation is enough to deduce the theorem. ☐

Let's give some example applications of this theorem.

Example 7.2.9.

- The most obvious application is in number theory. When $A = \mathbb{Z}$, $K = \mathbb{Q}$, and L is a finite extension of $\mathbb{Q}$, we get that the ring of integers $B = \mathcal{O}_L$ is a Dedekind domain.
- Let $A = \mathbb{C}[x]$, $K = \mathbb{C}(x)$, and $L = \mathbb{C}(x, y)/(y^2 - x^3 - x)$. Then, one can show that $\mathbb{C}[x, y]/(y^2 - x^3 - x)$ is integrally closed (which is true, but require some work), then $B = \mathbb{C}[x, y]/(y^2 - x^3 - x)$ is a Dedekind domain.

  In general, smooth curves over $\mathbb{C}$ correspond to integral closure of a finite extension of $\mathbb{C}(x)$. Then, the integral closure gives a Dedekind domain.

§7.3 Fractional Ideals

§7.3.1 Fractional Ideals and Invertible Ideals

We will first discuss these notions for a general domain (not necessarily Dedekind Domain).

Definition 7.3.1 (Fractional ideals).

Let A be a domain and $K = \operatorname{Frac} A$. An A-submodule $I \subset K$ is a **fractional ideal** if there exists $x \in A$ such that $xI \subseteq A$.

Equivalently, a submodule $I \subset K$ is a fractional ideal if and only if it is in form xJ for some $x \in K$ and regular ideal $J \subset A$.

Definition 7.3.2 (Invertible and principal fractional ideal).

A fractional ideal $I \subset K$ is

- **invertible** if and only if there exists a fractional ideal $J \subset K$ such that $IJ = A$.
- **principal** if and only if $I = (x)$ for some $x \in K$.

Proposition 7.3.3.

If I is invertible, then I is finitely-generated.

▶ *Proof.* Suppose that $IJ = A$. Then, there exists $i_1, \dots, i_n \in I$ and $j_1, \dots, j_n \in J$ such that $i_1 j_1 + \cdots + i_n j_n = 1$. For any $x \in I$, note that $xj_i \in IJ = A$ and we have $x = i_1(xj_1) + \dots i_n(xj_n)$, so I is generated by $i_1, \dots, i_n$. ☐

The following theorem shows that invertible fractional ideals are "locally principal". In other words, they are locally free modules of rank 1.

Theorem 7.3.4 (Characterization of invertible fractional ideals).

Let I be a fractional ideal over domain A. Suppose that I is finitely-generated. Then, the following are equivalent.

(a) I is invertible.

(b) $(A : I)I = A$, where $(A : I) = \{x \in K : xI \subset A\}$.

(c) $I_{\mathfrak{p}}$ is an invertible fractional $A_{\mathfrak{p}}$-ideal for all prime ideal $\mathfrak{p}$.

(d) $I_{\mathfrak{m}}$ is an invertible fractional $A_{\mathfrak{m}}$-ideal for all maximal ideal $\mathfrak{m}$.

(e) $I_{\mathfrak{p}}$ is a principal ideal for all prime ideal $\mathfrak{p}$.

(f) $I_{\mathfrak{m}}$ is a principal ideal for all maximal ideal $\mathfrak{m}$.

▶ *Proof.* We have the following clear implications:

- (b) implies (a) because $(A : I)$ is the inverse.
- Localizing $IJ = A$ gives $I_{\mathfrak{p}} J_{\mathfrak{p}} = A_{\mathfrak{p}}$, so (a) implies (c), and (c) implies (d).
- Principal ideals are invertible, so (e) implies (c) and (f) implies (d).

We first show (a) implies (b). (Thus, (a) and (b) are now equivalent.) Suppose $IJ = A$. Then, for any $j \in J$, we have $jI \subseteq IJ = A$, so $j \in (A : I)$. Thus, $J \subset (A : I)$. In the other direction, note that

$$(A : I) = (A : I)A = (A : I)IJ \subseteq AJ = J,$$

so $(A : I) \subseteq J$, forcing $J = (A : I)$.

Now, we show that (a), (b), (c), and (d) are equivalent. To do this, it suffices to show that (d) implies (a). Assume (d) is true. First, we leave to the reader to check that $(A : I)_\mathfrak{m} = (A_\mathfrak{m} : I_\mathfrak{m})$ for all maximal ideals $\mathfrak{m}$. (This uses I is finitely-generated.) Note that $(A : I)I \subset A$, so we have the inclusion map $\phi : (A : I)I \to A$. Localizing this map gives $\phi_\mathfrak{m} : (A_\mathfrak{m} : I_\mathfrak{m})I_\mathfrak{m} \to A_\mathfrak{m}$, which we know from (b) (applied on $A_\mathfrak{m}$) that it is surjective. Thus, by Corollary 3.3.2, we get that ϕ is an isomorphism, so $(A : I)I = A$.

Finally, we show that (c) implies (e) and (d) implies (f). To show both of these, it suffices to show that "if A is a local ring and I is an invertible fractional ideal, then I is principal."

To prove this claim, let $\mathfrak{m}$ be the (unique) maximal ideal of A, and let $IJ = A$. Then, there exists $i_1, \dots, i_n \in I$ and $j_1, \dots, j_n \in J$ such that $i_1 j_1 + \cdots + i_n j_n = 1$. Thus, at least one of the terms, say $i_1 j_1$, is in $A \setminus \mathfrak{m}$, hence a unit. Now, let $I' = i_1$. Then,

$$(1) \subseteq (i_1)(j_1) \subseteq (i_1)J \subseteq IJ = (1),$$

forcing all equalities. Thus, $(i_1)J = IJ$. Multiplying by I both sides gives $(i_1) = I$. ☐

Example 7.3.5.

The ideal $I = (x, y) \subset \mathbb{C}[x, y]$ is not invertible. We check this in two ways.

- First, we show that (b) does not hold. We claim that $(\mathbb{C}[x, y] : I) = \mathbb{C}[x, y]$. Indeed, if $f \in \mathbb{C}(x, y)$ such that $xf \in \mathbb{C}[x, y]$ and $yf \in \mathbb{C}[x, y]$, then we would have $f \in \mathbb{C}[x, y]$.
- We show that (e) does not hold. To do this, we localize at maximal ideal $\mathfrak{m} = (x, y)$. Then, $I_\mathfrak{m} = \mathfrak{m}(\mathbb{C}[x, y]_\mathfrak{m}) =: \overline{\mathfrak{m}}$, the maximal ideal of $\mathbb{C}[x, y]_\mathfrak{m}$. Then, $\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2$ is spanned by x and y, so it is definitely not generated by one element, so $\overline{\mathfrak{m}}$ is not principal.

Now, we specialize to Dedekind domain.

Theorem 7.3.6.

If A is a Dedekind domain, then every fractional ideal is invertible.

▶ *Proof.* Let I be a fractional ideal of A. Then, since $A_\mathfrak{p}$ is a DVR, hence PID (Theorem 7.1.4), we get that $I_\mathfrak{p}$ is principal for all nonzero prime ideal $\mathfrak{p}$. Hence, I is invertible (by Theorem 7.3.4 (d) implies (a)). ☐

§7.3.2 Class Group

Definition 7.3.7 (Class group)**.**

Let A be a Dedekind domain. Then, the invertible fractional ideals forms the group $\mathcal{I}_A$ (the inverse exist because of Theorem 7.3.6). Then, the **class group** is defined as

$$\operatorname{Cl} A := \frac{\mathcal{I}_A}{\{\text{principal fractional ideals of } A\}}.$$

Example 7.3.8.

- Any PID has a trivial class group.
- When $\mathcal{O}_K$ is an integral closure of $\mathbb{Z}$ inside some field extension of $\mathbb{Q}$, the key result in algebraic number theory is that $\operatorname{Cl} \mathcal{O}_K$ is finite. Proving this require understanding the lattice structure of $\mathcal{O}_K$, which is beyond the scope of these notes.

  The **class number** $\# \operatorname{Cl} \mathcal{O}_K$ measures how far away $\mathcal{O}_K$ is from a UFD.
- If A be an integral closure of $\mathbb{C}[x]$ in a finite extension of $\mathbb{C}(x)$ (thus getting a ring corresponding to a smooth curve), then there exists a number g, called the **genus** of the curve $\operatorname{Spec} A$, such that
$$\operatorname{Cl} A \simeq \mathbb{C}^g/\Lambda,$$
  where $\Lambda \simeq \mathbb{Z}^{2g}$ is a lattice embedded in $\mathbb{C}^g$. The proof of this is far beyond the scope of these notes.

Let's sketch how class group works in a specific case of **elliptic curves**. (We will not fully justify everything). Consider the ring
$$A = \frac{\mathbb{C}[x,y]}{(y^2 - x^3 - ax - b)},$$
where $x^3 + ax + b$ is a cubic polynomial with distinct roots (i.e., $4a^3 + 27b^2 \neq 0$). This ring corresponds to elliptic curve $y^2 = x^3 + ax + b$. Note that $\dim A = 1$ by Theorem 4.5.4. By using the condition $\dim(\mathfrak{m}/\mathfrak{m}^2) = 1$ (in Theorem 7.1.4 (d)), one can check that localization $A_{\mathfrak{m}}$ at any maximal ideal is a DVR, so A is a Dedekind domain.

Now, let us investigate class group. Suppose that $\mathfrak{m}_{(p,q)} = (x-p, y-q)$ is the maximal ideal corresponding to point (p,q). We observe the following.

- Function $x - p$ vanishes at two points (p,q) and $(p,-q)$. Checking valuation reveals that
$$(x-p) = \mathfrak{m}_{(p,q)}\mathfrak{m}_{(p,-q)}.$$
- If points (p_1,q_1), (p_2,q_2), and (p_3,q_3) lie on a line $ux + vy + w = 0$. Then, because elliptic curve is a cubic equation, this line must intersect the curve at only these three points. Then, checking valuations reveal that
$$(ux + vy + w) = \mathfrak{m}_{(p_1,q_1)}\mathfrak{m}_{(p_2,q_2)}\mathfrak{m}_{(p_3,q_3)}.$$

Thus, if we consider the map
$$\begin{aligned} \phi : \{\text{points on elliptic curve}\} \sqcup \{O\} &\to \operatorname{Cl} A \\ P &\mapsto \mathfrak{m}_P \\ O &\mapsto (1) \end{aligned}$$

Then, we get the following observations:

- If $-P$ is the reflection of P across the x-axis, then $\phi(P) + \phi(-P) = 0$.
- If point P, Q, R are collinear, then $\phi(P) + \phi(Q) + \phi(R) = 0$.
- In particular, $\phi(P) + \phi(Q)$ is ϕ of the reflection of R across the x-axis.

Since $\operatorname{Cl} A$ is generated by maximal ideals, we have shown that ϕ is surjective already. It turns out that **ϕ is injective**. This fact is equivalent to $\mathfrak{m}_P$ is not principal for all point P, and proving that requires a nontrivial algebraic geometry that we will not take time to develop. (The rough idea is that if $\mathfrak{m}_P$ is generated by (f), then f vanishes at only point P, and we can show that it induces an isomorphism from $\mathbb{C}[z]$ to A).

The important consequence of this is that by simply writing $\phi(P)$ as P, we get the group structure on points on elliptic curve (plus O). In particular, if P, Q, R are collinear, then $P + Q$ is the reflection of

R across the x-axis. This is the **elliptic curve group law**, and notice that we have immediately shown associativity of this addition process (which would require checking identities with hundreds of terms if bashing it out directly).

This also gives hint on how to generalize to other curves. The idea is that by considering the set of point where a polynomial in variables x and y intersect the curve, one can show that each element in $\operatorname{Cl} A$ is represented by the product of at most g maximal ideals. This number g is called the **genus** of a curve. Thus, instead of adding points (like elliptic curve), we can define a group law on g-tuple of points instead. This group law is known as the **Jacobian** of a curve.

§7.4 Problems

Problem 7.A. Let A be the localization of $\mathbb{C}[x,y]/(y^3 - x^5 - x)$ at maximal ideal (x,y).

(a) Prove that A is a DVR.

(b) What is the valuation of x in this DVR?

Problem 7.B. Let $\mathbb{Z}_{(2)} = \{\frac{a}{b} : a, b \in \mathbb{Z}, 2 \nmid b\} \subseteq \mathbb{Q}$. Let $R = \mathbb{Z}_{(2)}[x]/(x^5 + 2x + 2)$, which is an integral extension of $\mathbb{Z}_{(2)}$.

(a) Prove that R is a DVR. (In particular, you have to show that R is a local ring first.)

(b) What is the valuation of 2 in R?

Problem 7.C. Let $f \in \mathbb{C}[x]$ be a polynomial. Prove that $\mathbb{C}[x,y]/(y^2 - f(x))$ is a Dedekind domain if and only if all roots of f are distinct.

Problem 7.D. Let A be a Dedekind domain and I and J be fractional ideals. Prove that

(a) $I \oplus J \simeq A \oplus IJ$

(b) $I \otimes_A J \simeq IJ$.

This generalizes Problem 2.B. (Hint: localize. See Section 3.4.)

Problem 7.E. Let A be a Dedekind domain and I be a nonzero ideal.

(a) Prove that every ideal of A/I is principal.

(b) Prove that I is generated by two elements.

Problem 7.F (2-torsion points of elliptic curves)**.** Let $\alpha_1, \alpha_2, \alpha_3$ be distinct complex numbers, and let

$$A = \frac{\mathbb{C}[x,y]}{(y^2 - (x-\alpha_1)(x-\alpha_2)(x-\alpha_3))},$$

which is a Dedekind domain by Problem 7.C. Prove that the maximal ideal $\mathfrak{m}_j = (y, x - \alpha_j)$ for $j = 1, 2, 3$ all have order two in the class group $\operatorname{Cl} A$.

(Hint: to show that $\mathfrak{m}_j$ is not principal, begin by assuming $\mathfrak{m}_j = (f(x,y))$ and notice that $f(x,-y)$ is also a generator of $\mathfrak{m}_j$.)

8 Completion

This chapter discusses completion, which is a construction that attach a power series to a ring. Roughly speaking, if A is a ring and $A_{\mathfrak{p}}$ is a local ring at prime ideal $\mathfrak{p}$, then the completion $\widehat{A_{\mathfrak{p}}}$ is a ring that zooms in closer at $\mathfrak{p}$.

As a motivating example, consider

$$R = \frac{\mathbb{C}[x, y]}{(y^2 - x^2 - x^3)} \qquad S = \frac{\mathbb{C}[x, y]}{(y^2 - x^2)}.$$

These rings correspond to nodal curves $y^2 = x^3+x^2$ and $y^2 = x^2$. In particular, the open neighborhoods around $(0, 0)$ of both curves look like segments with slope 1 and -1.

Localization carries a lot more detail than the slope of these two lines. For example, the localization of R and S at maximal ideal (x, y) (the one corresponding to point $(0, 0)$) are not the same. In particular, since R is a domain, the localization of R at $(0, 0)$ is still a domain. In contrast, localization of S at $(0, 0)$ is not a domain. A geometric intuition for this is localization of R still carries the whole curve.

In contrast, completion is a more brutal version of localization that only keeps information in a very close range. We will later see that the completion of R and S at maximal ideal $(0, 0)$ are isomorphic! Completion thus loses some information. However, it also allows us to make sense of the notion that two rings are *analytically* the same. This allows us to also simplify the study of rings by first studying its completion first.

§8.1 Construction

§8.1.1 Inverse Limit

For simplicity, we define inverse limit on a sequence of group, which is sufficient for us. (Similar to direct limit, it's possible to generalize this to index by direct sets, or even small category.)

Definition 8.1.1 (Inverse limit).

An **inverse system** is a sequence of groups $(A_n)_{n\geq 0}$ with homomorphisms $\theta_{n+1} : A_{n+1} \to A_n$. For any inverse system, we can define an **inverse limit**

$$\varprojlim A_n := \{(a_n)_{n\geq 0} : a_n \in A_n, \theta_{n+1}(a_{n+1}) = a_n\}.$$

The sequences (a_n) above are called **coherent sequences**.

Example 8.1.2 (Formal series ring).

Let A be a ring and ideal $\mathfrak{a} \subset A$. Then, we have an inverse system

$$A \supset \mathfrak{a} \supset \mathfrak{a}^2 \supset \mathfrak{a}^3 \supset \dots.$$

A special case of this is the inverse system

$$\mathbb{C}[t] \supset (t) \supset (t^2) \supset (t^3) \supset \dots.$$

In this case, we have

$$\varprojlim(t^n) = \{(b_n) : b_n \in \mathbb{C}[t]/(t^n), b_{n+1} \equiv b_n \pmod{t^{n+1}}\} \simeq \mathbb{C}[[t]].$$

In particular, $c_0 + c_1t + c_2t^2 + \dots$ maps to

$$(c_0, c_0 + c_1t, c_0 + c_1t + c_2t^2, \dots).$$

One needs to check that this respect ring structure, but it is indeed correct.

Example 8.1.3 (p-adic number).

Consider an inverse system

$$\mathbb{Z} \supset (p) \supset (p^2) \supset (p^3) \supset \dots.$$

Then, the inverse limit is

$$\varprojlim(p^n) = \mathbb{Z}_p = \{c_0 + c_1p + c_2p^2 + \dots, c_i \in \{0, 1, \dots, p-1\}\}.$$

The ring structure of this is different from $\mathbb{Z}[[t]]$: there is a carry in modulo p.

The above two examples are a special case of the following construction.

Definition 8.1.4 (I-adic completion).

For any ring A and ideal I, the ***I*-adic completion** is

$$\widehat{A} = \varprojlim_{n \geq 0} A/I^n$$

(so each element is a sequence of $(x \bmod I, x \bmod I^2, \dots)$). Often, I is a maximal ideal.

It's natural to ask whether inverse limit preserves exactness or not. The following lemma gives the answer.

Lemma 8.1.5 (Inverse limit preserves exactness).

Suppose that we have a short exact sequence of inverse systems

$$0 \longrightarrow (A_n)_{n\geq 0} \xrightarrow{f} (B_n)_{n\geq 0} \xrightarrow{g} (C_n)_{n\geq 0} \longrightarrow 0,$$

i.e., the commutative diagram with exact rows

$$\begin{tikzcd}
 & \dots \arrow[d] & \dots \arrow[d] & \dots \arrow[d] & \\
0 \arrow[r] & A_n \arrow[r, "f_n"] \arrow[d, "\theta_n^A"] & B_n \arrow[r, "g_n"] \arrow[d, "\theta_n^B"] & C_n \arrow[r] \arrow[d, "\theta_n^C"] & 0 \\
0 \arrow[r] & A_{n-1} \arrow[r, "f_{n-1}"] \arrow[d] & B_{n-1} \arrow[r, "g_{n-1}"] \arrow[d] & C_{n-1} \arrow[r] \arrow[d] & 0 \\
 & \dots & \dots & \dots &
\end{tikzcd}.$$

(a) We have the left exact sequence

$$0 \longrightarrow \varprojlim_n A_n \longrightarrow \varprojlim_n B_n \longrightarrow \varprojlim_n C_n.$$

(b) If $\theta_n^A : A_n \to A_{n-1}$ is surjective for all n, then we have the exact sequence

$$0 \longrightarrow \varprojlim_n A_n \longrightarrow \varprojlim_n B_n \longrightarrow \varprojlim_n C_n \longrightarrow 0.$$

▶ *Proof.* (a) Let $\mathbf{A} = \prod_{n \geq 0} A_n$, and define the map

$$d^A : \mathbf{A} \to \mathbf{A}$$
$$(a_0, a_1, \dots) \mapsto (a_n - \theta_{n+1}^A(a_{n+1}))_{n \geq 0}.$$

Define $\mathbf{B}$, $\mathbf{C}$, d^B, and d^C similarly. Then, $\varinjlim_{n \geq 0} A_n = \operatorname{Ker} d^A$, and similarly for B and C. Moreover, we have the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathbf{A} \arrow[r, "f"] \arrow[d, "d^A"] & \mathbf{B} \arrow[r, "g"] \arrow[d, "d^B"] & \mathbf{C} \arrow[r] \arrow[d, "d^C"] & 0 \\
0 \arrow[r] & \mathbf{A} \arrow[r, "f"] & \mathbf{B} \arrow[r, "g"] & \mathbf{C} \arrow[r] & 0.
\end{tikzcd}$$

Thus, Snake Lemma (Lemma 2.3.5) gives the exact sequence

$$0 \longrightarrow \operatorname{Ker} d^A \longrightarrow \operatorname{Ker} d^B \longrightarrow \operatorname{Ker} d^C \longrightarrow \operatorname{Coker} d^A,$$

which gives the desired left exactness.

(b) From above, we have to show that d^A is surjective (so $\operatorname{Coker} d^A = 0$). To do that, suppose $(b_0, b_1, \dots, b_n) \in \mathbf{A}$. We need to find $(a_0, a_1, \dots)$ such that $a_n - \theta_{n+1}^A(a_{n+1}) = b_n$ for all n. Begin by choosing a_0 arbitrarily. Then, since θ_n^A is surjective for all n, we can select a_1 so that $a_0 - \theta_1^A(a_1) = b_0$, select a_2 such that $a_1 - \theta_2^A(a_2) = b_1$, and so on. $\square$

§8.1.2 Completion with respect to Filtration

Let A be a ring, and M be an A-Module.

Definition 8.1.6 (Filtration and completion).

A **filtration** of M by submodules is a sequence $M \supset F_1 \supset F_2 \supset \dots$. Then, the **completion** of M with respect to this filtration is

$$\widehat{M} = \varprojlim_n M/F_n,$$

which is an inverse limit of the inverse system

$$\dots \longrightarrow M/F_3 \longrightarrow M/F_2 \longrightarrow M/F_1 \longrightarrow 0.$$

Each element of $\widehat{M}$ is a sequence $f = (f_1, f_2, \dots)$, where $f_i \in M/F_i$, and the image of f_{i+1} onto M/F_i is equal to f_i (i.e., they are consistent).

Different filtrations can result in the same completion.

Definition 8.1.7 (Bounded difference filtration).

Two filtrations $(F_n)_{n \geq 0}$ and $(G_n)_{n \geq 0}$ have **bounded difference** if and only if there exists c such that $F_{n+c} \subset G_n$ and $G_{n+c} \subset F_n$ for all $n \geq 0$.

Proposition 8.1.8 (Bounded difference filtrations gives the same completion)**.**

If $(F_n)_{n\geq 0}$ and $(G_n)_{n\geq 0}$ are two filtrations with bounded difference, then they result in the same completion

$$\varprojlim_n M/F_n \simeq \varprojlim_n M/G_n.$$

▶ *Proof.* Given $(f_1, f_2, \dots) \in \varprojlim_n M/F_n$, we map it to element $(g_1, g_2, \dots) \in \varprojlim_n M/G_n$ by letting g_n be the image of f_{n+c} through the quotient projection $M/F_{n+c} \to M/G_n$. The inverse map can be constructed similarly, and it is easy to see that they are inverses. ☐

A key example of completion is consider an ideal $I \subset A$ and the I-adic filtration $A \supset I \supset I^2 \supset I^3 \supset \dots$. An analogue of this for a module is the following.

Definition 8.1.9.

- The ***I*-adic filtration** is the filtration

$$M \supset IM \supset I^2M \supset \dots.$$

In particular, the ***I*-adic completion** of M, often denoted $\widehat{M}$ is

$$\widehat{M} = \varprojlim_{n\geq 0} M/I^nM.$$

- An ***I*-filtration** on M is a filtration $(F_n)_{n\geq 0}$ such that $IF_n \subset F_{n+1}$ for all n.
- A **stable *I*-filtration** is a filtration $(F_n)_{n\geq 0}$ such that $IF_n = F_{n+1}$ for all n.

In fact, stable I-filtrations are not much different from the I-adic filtration. We have the following lemma.

Lemma 8.1.10.

Any stable I-filtration $(F_n)_{n\geq 0}$ on M has bounded difference from I-adic filtration $I \supset I^2 \supset \dots$, thus inducing the same completion as the I-adic completion.

▶ *Proof.* For one direction, note that $IF_{n-1} \subset F_n$, so we have $I^n \subset I^{n-1}F_1 \subset I^{n-2}F_2 \subset \cdots \subset IF_{n-1} \subset F_n$, so $I^n \subset F_n$, proving one direction.

For the other direction, pick c such that $I^kF_c = F_{c+n}$ for all n. This gives $F_{n+c} \subset I^n$, done. ☐

§8.2 Hensel's Lemma

Completion allows us to solve many algebraic expression / equation that we cannot do in normal ring. For example, identities like

$$\frac{1}{1-x} = 1 + x + x^2 + \dots$$
$$\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{3}{16}x^3 - \dots = \sum_{n=0}^{\infty} \binom{1/2}{n} x^n$$

were not valid in a normal polynomial ring, but they are valid once you extend to infinite series (i.e., take completion). There is a very general process of solving polynomial equation in the completed ring, called **Hensel's lemma**.

Theorem 8.2.1 (Hensel's Lemma)**.**

Let A be a ring, and let $I \subset A$ be an ideal. Let $f(x) \in A[x]$. Suppose we have $\overline{a} \in A/I$ such that

- $f(\overline{a}) = 0$ in A/I and
- $f'(\overline{a})$ is invertible A/I.

Then, there exists unique $\alpha \in \widehat{A}$ such that $f(\alpha) = 0$ and $\alpha \equiv \overline{a} \pmod{I}$.

▶ *Proof.* Let $a = a_1$. It suffices to find a unique $a_n \in A/I^n$ such that

- $a_n \equiv a_{n-1} \pmod{I^{n-1}}$.
- $f(a_n) = 0 \in A/I^n$.

The sequence $a_1, a_2, \ldots$ defines $\alpha \in \widehat{A} = \varprojlim A/I^n$. We have $f(\alpha) = 0$ since $f(a_n) = 0$ for all n.

We prove this by induction on n. Pick $b \in A/I^{n+1}$ such that $b \equiv a_n \pmod{I^n}$. Then, for $\varepsilon \in I^n/I^{n+1}$, we have

$$f(b+\varepsilon) = f(b) + \varepsilon f'(b) \in A/I^{n+1}$$

because all the ε^2 terms got canceled out. Then, since $f'(\overline{a})$ is invertible in A/I, we have $f'(b)$ is invertible in A/I, so there exists $t \in A$ such that $f'(b)t \equiv 1 \pmod{I}$.

Thus, we have $f(b+\varepsilon) = 0$ if and only if $\varepsilon = -f(b)t$, so this gives unique $a_{n+1} = b + \varepsilon$. The uniqueness of $a_1, a_2, \ldots$ gives the uniqueness of a. ☐

Example 8.2.2.

Let $A = \mathbb{C}[x]$, $I = (x)$, and $f(t) = t^2 - (1+x) \in A[t]$. Then,

- $f(1) = -x \in I$.
- $f'(t) = 2t - (1+x)$, so $f'(1) = 2 - (1+x) = 1 - x$, which reduces to $1 \in A/I$, which is invertible.

Thus, Hensel's lemma gives that there exists a such that $a \equiv 1 \pmod{x}$ and $a^2 = 1 + x$. Define $\sqrt{1+x} := a$. More concretely, the first few terms of $\sqrt{1+x}$ is

$$\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{3}{16}x^3 - \ldots.$$

We now revisit the nodal curves in the introduction of this chapter. Consider

$$R = \left(\frac{\mathbb{C}[x,y]}{(y^2 - x^3 - x^2)}\right)_{(x,y)} \quad \text{and} \quad S = \left(\frac{\mathbb{C}[u,v]}{(u^2 - v^2)}\right)_{(u,v)},$$

which are the rings of the curves $y^2 = x^3 + x^2$ and $u^2 = v^2$, localized at $(0,0)$. One can check that $R \not\simeq S$. However, we claim that the (x,y)-adic completion $\widehat{R}$ of R is isomorphic to the (u,v)-adic completion $\widehat{S}$ of S, and the isomorphism is given by

$$u = x\sqrt{1+x}, \quad v = y. \tag{8.1}$$

To define the inverse map, one needs to solve $x^3 + x^2 = u^2$. Let $x = ut$, so we have to solve the equivalent equation $ut^3 + t^2 = 1$. We again uses Hensel's lemma: set $f(t) = ut^3 + t^2 - 1$, and we check that

- $f(1) = u \in (u)$.

- $f'(1) = 3u + 2$, which is invertible in $S/(u)$.

Hence, Hensel's lemma gives that there exists $t \equiv 1 \pmod{u}$ such that $ut^3 + t^2 = 1$. More concretely, the first few terms of t is

$$t = 1 - \frac{1}{2}u + \frac{5}{8}u^2 - u^3 - \dots$$

There is no closed form of the coefficients, but Hensel's lemma guarantees that you can compute as many terms as you want. Finally, the inverse map is desired by

$$x = u - \frac{1}{2}u^2 + \frac{5}{8}u^3 - u^4 - \dots, \quad y = v, \tag{8.2}$$

and we leave the reader to check that (8.1) and (8.2) define an isomorphism between $\widehat{R}$ and $\widehat{S}$.

§8.3 Artin-Rees Lemma

We now begin proving nice properties of completion. To do that, Artin-Rees lemma is a powerful tool.

§8.3.1 Statement

Next, given a module M with I-adic filtration. For any submodule $M' \subset M$, there are two natural choices of filtrations.

- the I-adic filtration of M' and
- the induced **subspace filtration** $F'_n = M \cap F_n$.

These two filtrations are very different. If $A = \mathbb{Z}$, $I = (p)$, then the I-adic filtration of $\mathbb{Q}$ is a stupid $\mathbb{Q} \supset \mathbb{Q} \supset \dots$, so passing this to $\mathbb{Z}$ gives $\mathbb{Z} \supset \mathbb{Z} \supset \dots$. On the other hand, the I-adic filtration on $\mathbb{Z}$ is $\mathbb{Z} \supset (p) \supset (p^2) \supset \dots$, so these are very different.

The natural question is when are these filtrations the same. It turns out that if A is Noetherian and M is finitely generated, then they are the same!

Theorem 8.3.1 (Artin-Rees Lemma).

Let A be a Noetherian ring, $I \subset A$ be an ideal, and M be a finitely-generated A-module. Let $M \supset F_1 \supset F_2 \supset \dots$ be a stable I-adic filtration. Then, for any submodule $M' \subset M$, the filtration $F'_n = M' \cap F_n$ is stable I-adic filtration too!

§8.3.2 Proof

Proving this theorem requires a quick digression to **graded rings**.

Definition 8.3.2 (Graded ring and graded modules).

A ring is a **graded ring** if and only if it can be written as

$$A_\bullet = \bigoplus_{n=0}^{\infty} A_n$$

such that $A_r \cdot A_s \subset A_{r+s}$ for all r, s. We also let $A_+ = \bigoplus_{n \geq 1} A_n$ be an ideal.

A **graded $A_\bullet$-module** is a direct sum

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

such that $A_j M_i \subset M_{i+j}$ for all $i, j \geq 0$.

An example of graded ring is $\mathbb{C}[x] = \mathbb{C} \oplus \mathbb{C}x \oplus \mathbb{C}x^2 \oplus \dots$.

Lemma 8.3.3 (Condition for graded rings to be Noetherian).

The following are equivalent.

(a) $A_\bullet$ is Noetherian

(b) A_0 is Noetherian and $A_\bullet$ is a finitely-generated algebra.

▶ *Proof.* ($\Leftarrow$) Note that $A_0[x_1, \dots, x_n]$ is Noetherian by Hilbert Basis theorem (Theorem 5.2.3). Thus, $A_\bullet$, which is a quotient of $A_0[x_1, \dots, x_n]$ is Noetherian.

($\Rightarrow$) We have $A_0 = A_\bullet / A_+$ so it is Noetherian. As an ideal, we have $A_+ = (z_1, \dots, z_m)$. Then, $z_1, \dots, z_m$ generates $A_\bullet$ as A_0-algebra (i.e, $A_0[z_1, \dots, z_m] = A_\bullet$). ☐

Next, we will do the following clever construction. For any ring A, we construct the **blowup algebra** (also known as **Rees algebra**)

$$\mathrm{Bl}_I A = \bigoplus_{n \geq 0} I^n \subset \bigoplus_{n \geq 0} A = A[t].$$

This is a graded ring because $I^n I^m \subset I^{n+m}$.

Observe that if A is Noetherian, then by Lemma 8.3.3, we get $\mathrm{Bl}_I A$ is Noetherian.

Now, given a finitely-generated module M and an I-filtration $(F_n)_{n \geq 0}$, define the **blowup module**

$$\mathrm{Bl}_F M = \bigoplus_{n \geq 0} F_n.$$

Therefore, $\mathrm{Bl}_F M$ is a graded $\mathrm{Bl}_I A$-module.

Lemma 8.3.4.

(F_n) is a stable I-filtration if and only if $\mathrm{Bl}_F M$ is a finitely-generated $\mathrm{Bl}_I A$-module.

▶ *Proof.* Observe the following.

(i) $M \oplus F_1 \oplus \cdots \oplus F_n$ is a finitely-generated A-submodule of $\mathrm{Bl}_F M$.

(ii) Therefore, if

$$M_n^\star := M \oplus F_1 \oplus \cdots \oplus F_n \oplus IF_n \oplus I^2 F_n \oplus \dots \subset \mathrm{Bl}_F M,$$

the submodule generated by $M \oplus F_1 \oplus \cdots \oplus F_n$, then $M_n^\star$ is finitely-generated $\mathrm{Bl}_I A$-module.

(iii) We have an infinite ascending chain

$$M_0^\star \subset M_1^\star \subset \cdots \subset \mathrm{Bl}_F M.$$

We are now ready to finish the proof. Each of the following is equivalent to the next.

- $\mathrm{Bl}_F M$ is finitely-generated $\mathrm{Bl}_I A$-module.
- $\mathrm{Bl}_F M = M_n^\star$ for some n (follows from (ii) and (iii)).
- $\bigoplus_{k \geq 0} F_k = M \oplus F_1 \oplus \cdots \oplus F_n \oplus IF_n \oplus I^2 F_n \oplus \dots$ for some n.
- There exists k such that $F_{n+k} = I^k F_n$ for all k.

- The filter (F_n) is stable. ☐

Finally, we prove Artin-Rees Lemma.

▶ *Proof of Artin-Rees Lemma (Theorem 8.3.1).* Consider the blowup module of M'

$$\operatorname{Bl}_F M' = \bigoplus_{n\geq 0}(F_n \cap M') \subset \operatorname{Bl}_F M.$$

Since F is stable, we have by the previous Lemma 8.3.4 $\operatorname{Bl}_F M$ is finitely-generated. Since $\operatorname{Bl}_I A$ is Noetherian, $\operatorname{Bl}_F M'$ is finitely-generated. Thus, $F_n \cap M'$ is stable! ☐

§8.4 Properties of Completion

We now prove various properties of completion.

§8.4.1 Exactness

Theorem 8.4.1 (Exactness of I-adic completion)**.**

Let A be a Noetherian ring, I be an ideal, and we have a short exact sequence of A-module

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0.$$

If N is finitely-generated, then the I-adic completions form an exact sequence

$$0 \longrightarrow \widehat{M} \longrightarrow \widehat{N} \longrightarrow \widehat{P} \longrightarrow 0.$$

▶ *Proof.* View M as a submodule of N. Then, we have a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & M \cap I^k N \arrow[r, hook] \arrow[d, hook] & I^k N \arrow[r] \arrow[d, hook] & I^k P \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & M \arrow[r, hook] & N \arrow[r] & P \arrow[r] & 0
\end{tikzcd}.$$

We apply Snake lemma (Lemma 2.3.5). Reading from $\operatorname{Ker}(I^k P \to P)$ onwards, we get the exact sequence

$$0 \longrightarrow M/(M \cap I^k N) \longrightarrow N/I^k N \longrightarrow P/I^k P \longrightarrow 0.$$

The inverse limit of $N/I^k N$ and $P/I^k P$ are $\widehat{N}$ and $\widehat{P}$. By Artin-Rees lemma (Theorem 8.3.1), the inverse limit of $M/(M \cap I^k N)$ is $\widehat{M}$. Hence, by taking inverse limit of the above sequence and using Lemma 8.1.5, we get the desired exact sequence

$$0 \longrightarrow \widehat{M} \longrightarrow \widehat{N} \longrightarrow \widehat{P} \longrightarrow 0.$$ ☐

§8.4.2 Flatness

Theorem 8.4.2 (Flatness of I-adic completion)**.**

Let A be a Noetherian ring and I be an ideal.

(a) If M is finitely-generated, then $\widehat{A} \otimes_A M \simeq \widehat{M}$.

(b) $\widehat{A}$ is a flat A-module.

⚠ Warning 8.4.3.

For any modules M, N, P, the sequence

$$0 \longrightarrow \widehat{A} \otimes_A M \longrightarrow \widehat{A} \otimes_A N \longrightarrow \widehat{A} \otimes_A P \longrightarrow 0$$

is always exact.

In contrast, the sequence

$$0 \longrightarrow \widehat{M} \longrightarrow \widehat{N} \longrightarrow \widehat{P} \longrightarrow 0$$

is **not always exact**, specifically when N is not finitely-generated. For example, if $A = \mathbb{Z}$, $I = (p)$, $M = \mathbb{Z}$, viewed as a submodule of $N = \mathbb{Q}$, then $\widehat{N} = 0$, so the sequence is definitely not exact.

▶ *Proof.* (a) We note that there is a natural map

$$\eta_M : \widehat{A} \otimes_A M \to \widehat{M}$$

arising from the obvious bilinear map $\widehat{A} \times M \to \widehat{M}$ by sending $(a_0, a_1, \dots)$ and m to $(a_0 m, a_1 m, \dots)$ where $a_n \in A/I^n$ and so $a_n m \in M/I^n M$.

We claim that η_M is an isomorphism for all finitely-generated M. This is obvious when $M = A^{\oplus r}$. We are going to reduce to this case.

To do that, we claim that there exists a right exact sequence

$$G \xrightarrow{\beta} F \xrightarrow{\alpha} M \longrightarrow 0$$

such that F and G are free and finitely-generated. To find this, take any surjective map $F \to M$ (exists since M is finitely-generated). Then, by Proposition 5.1.3, the kernel of this map is finitely-generated, and so one can find a surjective map from a free module G to this kernel, giving the desired map.

Thus, we have the following commutative diagram. The rows are exact by Theorem 2.5.6 and Theorem 8.4.1.

$$\begin{tikzcd}
\widehat{A} \otimes_A G \arrow[r, "\beta_*"] \arrow[d, "\eta_G"', "\sim"] & \widehat{A} \otimes_A F \arrow[r, "\alpha_*"] \arrow[d, "\eta_F"', "\sim"] & \widehat{A} \otimes_A M \arrow[r] \arrow[d, "\eta_M"] & 0 \\
\widehat{G} \arrow[r, "\widehat{\beta}"] & \widehat{F} \arrow[r, "\widehat{\alpha}"] & \widehat{M} \arrow[r] & 0
\end{tikzcd}$$

If you know **Five lemma** (see e.g., [AK13, (5.23)]), then the conclusion is immediate. If not, then it is still a straightforward diagram chase.

- **Surjectivity.** Note that $\eta_M \circ \alpha_* = \widehat{\alpha} \circ \eta_F$. The right hand side is surjective since $\widehat{\alpha}$ and η_F are surjective, so is the left hand side. Hence, η_M is surjective.
- **Injectivity.** Suppose that $m \in \widehat{A} \otimes_A M$ satisfies $\eta_M(m) = 0$.

$$\begin{tikzcd}
g \arrow[r, mapsto, "\beta_*"] \arrow[d, mapsto, "\eta_G"] & f \arrow[r, mapsto, "\alpha_*"] \arrow[d, mapsto, "\eta_F"] & m \arrow[r, mapsto] \arrow[d, mapsto, "\eta_M"] & 0 \\
\hat{g} \arrow[r, mapsto, "\widehat{\beta}"] & \hat{f} \arrow[r, mapsto, "\widehat{\alpha}"] & 0 \arrow[r, mapsto] & 0
\end{tikzcd}$$

  - Since α_* is surjective, find $f \in \widehat{A} \otimes_A F$ such that $\alpha_*(f) = m$.
  - Since $\hat{f} = \eta_F(f) \in \operatorname{Ker} \widehat{\alpha}$, so by exactness, there exists $\hat{g} \in \widehat{G}$ such that $\widehat{\beta}(\hat{g}) = \hat{f}$.
  - Since η_G is surjective, there exists $g \in \widehat{A} \otimes_A G$ such that $\eta_G(g) = \hat{g}$.
  - Thus, $\beta_*(g) = f$, so $f \in \operatorname{Im} \beta_*$, so $f \in \operatorname{Ker} \alpha_*$, implying that $m = \alpha_*(f) = 0$.

This complete the proof.

(b) Suppose that we have a map $\phi : M \to N$ is injective. We have to show that the induced map $\phi_* : \widehat{A} \otimes M \to \widehat{A} \otimes N$ is injective. If we had that M and N are finitely-generated, we would be done by combining (a) and exactness of completion (Theorem 8.4.1). However, we do not, so we need to do a little more work.

Suppose that $0 \neq \sum_{i=1}^{n} a_i \otimes m_i \in \operatorname{Ker} \phi_*$, where $a_i \in \widehat{A}$ and $m_i \in M$. Let M' be the submodule of M generated by $m_1, \ldots, m_n$, and let $N' = \phi(M')$, which is clearly finitely-generated. Then, the restriction $\phi : M' \to N'$ is injective, but the induced map on tensor $\phi_* : \widehat{A} \otimes_A M' \to \widehat{A} \otimes_A N'$ has element $\sum_{i=1}^{n} a_i \otimes m_i$ in the kernel, hence not injective. This contradicts the previous paragraph. $\square$

We note the following useful corollary.

Corollary 8.4.4.

Let A be Noetherian and I, J be ideals. Let $\widehat{A}$ be the I-adic completion.

(a) $\widehat{J} = J\widehat{A}$.

(b) $\widehat{J^n} = (\widehat{J})^n$.

(c) $A/I^n \simeq \widehat{A}/\widehat{I^n}$. (In particular, taking inverse limit shows that $\widehat{\widehat{A}} = \widehat{A}$.)

(d) $I^n/I^{n+1} = \widehat{I^n}/\widehat{I^{n+1}}$.

(Notation: $J\widehat{A}$ denotes ideal extension, while $\widehat{J}$ denote I-adic completion of J as A-module.)

▶ *Proof.* (a) The exact sequence of A-module

$$0 \longrightarrow J \longrightarrow A \longrightarrow A/J \longrightarrow 0$$

gives an exact sequence of $\widehat{A}$-module

$$0 \longrightarrow \widehat{J} \longrightarrow \widehat{A} \longrightarrow \widehat{A/J} \longrightarrow 0.$$

Thus, the third factor is $\widehat{A}/\widehat{J}$. However, $\widehat{A/J} \simeq \widehat{A} \otimes_A A/J = \widehat{A}/J\widehat{A}$, giving the result.

(b) From (a), we have $\widehat{J^n} = J^n\widehat{A} = (J\widehat{A})^n$.

(c) Note that $\widehat{A/I^n} = A/I^n$ because the inverse limit diagram stabilizes at A/I^n. However, by exactness, $\widehat{A/I^n} = \widehat{A}/(\widehat{I})^n = \widehat{A}/\widehat{I^n}$, implying that $A/I^n = \widehat{A}/\widehat{I^n}$,

(d) From (c), we get that $A/I^n = \widehat{A}/\widehat{I^n}$ and $A/I^{n+1} = \widehat{A}/\widehat{I^{n+1}}$ Taking quotient yields the result. $\square$

Finally, we note that completion of local ring is a local ring.

Proposition 8.4.5.

Let A be Noetherian local ring with maximal ideal $\mathfrak{m}$. Then, the $\mathfrak{m}$-adic completion $\widehat{A}$ is a local ring with maximal ideal $\widehat{\mathfrak{m}}$.

▶ *Proof.* Note that $A/\mathfrak{m} = \widehat{A}/\widehat{\mathfrak{m}}$, so $\widehat{\mathfrak{m}}$ is a maximal ideal. Now, for any $x \in \widehat{\mathfrak{m}}$, we have $(1+x)^{-1} = 1 - x + x^2 - \ldots$, converging in $\widehat{A}$, so $1 + x$ is a unit. This implies that $\widehat{\mathfrak{m}}$ is the only maximal ideal. $\square$

§8.4.3 Associated Graded Ring and Noetherianess

We will prove the following.

Theorem 8.4.6.

If A is Noetherian, then the I-adic completion $\widehat{A}$ is Noetherian.

This theorem would be easy if all ideals of $\widehat{A}$ comes from extension of A. However, this is not true because there are way more ideals generated by power series. Thus, we need to do some trick. The plan of the proof is the following.

(i) Prove that if A is Noetherian, then the formal series ring in k variables $A[[x_1, \dots, x_k]]$ is Noetherian.

(ii) Prove that $\widehat{A}$ is a quotient of $A[[x_1, \dots, x_k]]$ for some k.

Clearly, the theorem would follows from (i) and (ii). Part (i) was left as Problem 5.D, and the proof is basically imitating the proof of Hilbert Basis Theorem (Theorem 5.2.3). We thus focus on showing (ii). More precisely, we will prove the following lemma.

Proposition 8.4.7.

If I is finitely-generated, then $\widehat{A}$ is a quotient of $A[[x_1, \dots, x_k]]$ for some $k \geq 0$.

To prove this, we introduce a useful construction that will help us in the next chapter as well.

Definition 8.4.8 (Associated Graded Ring)**.**

If I is an ideal of A, then the **associated graded ring** is the graded ring

$$\operatorname{gr}_I A := \bigoplus_{n \geq 0} I^n / I^{n+1}.$$

For any module M and I-filtration F_n, we define the **associated graded module**

$$\operatorname{gr}_F M := \bigoplus_{n \geq 0} F_n / F_{n+1}.$$

Observe that $\operatorname{gr}_F M$ is a quotient of $\operatorname{Bl}_F M$. Thus, if F is a stable I-filtration, then by Lemma 8.3.4, $\operatorname{Bl}_F M$ is finitely-generated, so $\operatorname{gr}_F M$ is finitely-generated.

Now, we have the following key lemma, which will help us check when maps on completions are injective or surjective.

Lemma 8.4.9.

Suppose that $(F_n)_{n \geq 0}$ and $(G_n)_{n \geq 0}$ are two arbitrary filtrations of abelian groups M and N. If $f : M \to N$ be a map such that $f(F_n) \subset G_n$. We thus have two induced maps

$$\widehat{f} : \widehat{M} \to \widehat{N}, \quad \operatorname{gr} f : \operatorname{gr}_F M \to \operatorname{gr}_G N$$

Then, if $\operatorname{gr} f$ is injective (resp. surjective), then $\widehat{f}$ injective (resp. surjective).

▶ *Proof.* Let $\alpha_n : M/F_n \to N/G_n$. We will prove by induction that α_n is injective/surjective for all n. We have the commuting diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & F_n/F_{n+1} \arrow[r] \arrow[d, "\operatorname{gr}_n f"] & M/F_{n+1} \arrow[r] \arrow[d, "\alpha_{n+1}"] & M/F_n \arrow[r] \arrow[d, "\alpha_n"] & 0 \\
0 \arrow[r] & G_n/G_{n+1} \arrow[r] & N/G_{n+1} \arrow[r] & N/G_n \arrow[r] & 0
\end{tikzcd}$$

Applying Snake Lemma Lemma 2.3.5 gives the long exact sequence

$$0 \to \operatorname{Ker}(\operatorname{gr}_n f) \to \operatorname{Ker}\alpha_{n+1} \to \operatorname{Ker}\alpha_n \to \operatorname{Coker}(\operatorname{gr}_n f) \to \operatorname{Coker}\alpha_{n+1} \to \operatorname{Coker}\alpha_n \to 0.$$

If $\operatorname{gr}_n f$ is injective for all n, we assume the inductive hypothesis $\operatorname{Ker}(\alpha_n) = 0$. Looking at the first few terms gives $0 \to \operatorname{Ker}\alpha_{n+1} \to 0$, so $\operatorname{Ker}\alpha_{n+1} = 0$. This gives α_n injective for all n, so $M/F_n \to N/G_n$ is injective for all n. Since inverse limit is exact (Lemma 8.1.5), we get that $\widehat{M} \to \widehat{N}$ is injective.

If $\operatorname{gr} f$ surjective, we instead assume $\operatorname{Coker}\alpha_n = 0$. Thus, $\operatorname{Coker}\alpha_{n+1}$ is sandwiched between two zeroes, so it is zero. Thus, $M/F_n \to N/G_n$ is surjective for all n. Again, using the fact that inverse limit is exact (Lemma 8.1.5) gives the result. ☐

Finally, we prove Proposition 8.4.7.

► *Proof of Proposition 8.4.7.* Let $I = (f_1, \dots, f_n)$. Define the map

$$\begin{aligned} \phi : A[x_1, \dots, x_n] &\to A \\ x_i &\mapsto f_i. \end{aligned}$$

Let $J = (x_1, \dots, x_k)$. Then, $\phi(J) = I$, it induces the map on J-adic completion on left side and I-adic completion on the right side

$$\widehat{\phi} : A[[x_1, \dots, x_k]] \to \widehat{A}.$$

We claim that $\widehat{\phi}$ is surjective, which finishes the proof. To check this, by Lemma 8.4.9, it suffices to show that the induced map

$$\operatorname{gr} f : \bigoplus_{n\geq 0} I^n/I^{n+1} \to \bigoplus_{n\geq 0} J^n/J^{n+1}$$

is surjective.

However, note that each element in J^n/J^{n+1} is of the form $f_1^{a_1} \dots f_k^{a_k}$ where $a_1 + \dots + a_k = n$. This is preimage of $x_1^{a_1} \dots x_k^{a_k}$, so we are done. ☐

§8.5 Problems

Problem 8.A. Let $f \in \mathbb{C}[x, y]$ be an irreducible polynomial, and let $R = (\mathbb{C}[x, y]/(f))_{(x,y)}$. Suppose that at least one of $(\partial f/\partial x)_{(0,0)}$ and $(\partial f/\partial y)_{(0,0)}$ is nonzero. Prove that the (x, y)-adic completion $\widehat{R}$ is isomorphic to $\mathbb{C}[[x, y]]$.

Problem 8.B. Let A be a local ring with maximal ideal $\mathfrak{m}$ and residue field $k = A/\mathfrak{m}$ such that A is $\mathfrak{m}$-adically complete. Let $f \in A[x]$ be a monic polynomial, and let $\overline{f} \in k[x]$ be its reduction modulo $\mathfrak{m}$. If $\overline{f} = \overline{g}\overline{h}$, where $\overline{g}$ and $\overline{h}$ are monic polynomials in relatively prime in $k[x]$, prove that there exist polynomials $g, h \in A[x]$ such that $g \equiv \overline{g} \pmod{\mathfrak{m}}$, $h \equiv \overline{h} \pmod{\mathfrak{m}}$, and $f = gh$.

Problem 8.C. Let $\mathbb{Z}_p$ be the ring of p-adic integers, defined as the (p)-adic completion of $\mathbb{Z}$. Let $\mathbb{Q}_p$ be the fraction field of $\mathbb{Z}_p$.

(a) Prove that every element of $\mathbb{Q}_p$ is of the form $p^{-u}v$ where $u \in \mathbb{Z}$ and $v \in \mathbb{Z}_p$.

(b) Determine all quadratic extensions of $\mathbb{Q}_p$ (there are finitely many of them![1]). The answer is different for $p = 2$.

Problem 8.D (Krull's intersection theorem)**.** Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Krull's intersection theorem states that $\bigcap_{n\geq 0} \mathfrak{m}^n = 0$.

1. What's wrong with the following proof: let $I = \bigcap_{n\geq 0} \mathfrak{m}^n$, which is finitely-generated. Then,

$$\mathfrak{m}I = \mathfrak{m}\bigcap_{n\geq 0} \mathfrak{m}^n = \bigcap_{n\geq 0} \mathfrak{m}^{n+1} = \bigcap_{n\geq 1} \mathfrak{m}^n = I,$$

so by Nakayama's lemma, $I = 0$?

---

[1] It is a standard fact in algebraic number theory that there are finitely many degree n extension of $\mathbb{Q}_p$.

2. Using Artin-Rees lemma (Theorem 8.3.1), prove Krull's intersection theorem.

Problem 8.E. Let A be a Noetherian ring and I be an ideal in A. Let $\widehat{A}$ be the I-adic completion of A. Suppose that $x \in A$ is not a zero divisor. Prove that the image $\widehat{x}$ of x in $\widehat{A}$ is also not a zero divisor in $\widehat{A}$.

Problem 8.F. For each of the following rings R and maximal ideal $\mathfrak{m}$, compute $\operatorname{gr}_{\mathfrak{m}} R$.

(a) $R = \mathbb{C}[x, y]/(y^2 - x^3 - x)$ and $\mathfrak{m} = (x, y)$.

(b) $R = \mathbb{C}[x, y, z]/(xy, xz)$ and $\mathfrak{m} = (x, y, z)$.

(c) $R = \mathbb{C}[x, y, z, t]/(x^2 + y^3 + z^4 + t^5)$ and $\mathfrak{m} = (x, y, z, t)$.

9 Dimension Theory

We have met the notion of dimension of a ring in Section 4.5. To reproduce the definition, recall that for any ring R, the **Krull dimension** $\dim_{\text{Krull}} R$ is the maximum nonnegative integer n such that there exists a chain of prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \cdots \subsetneq \mathfrak{p}_n \ \subset \ R.$$

This notion of dimension is notoriously difficult to deduce its properties. For example, proving that $\dim \mathbb{C}[x_1, \ldots, x_n] = n$, which we did in Section 4.5, was a nontrivial task.

To give a more robust theory of dimension, we first note that we can reduce to the study of local ring. Since any chain of prime ideals should terminate at a maximal ideal, we deduce that

$$\dim_{\text{Krull}} R = \max_{\mathfrak{m} \text{ maximal}} \dim_{\text{Krull}} R_{\mathfrak{m}} = \max_{\mathfrak{p} \text{ prime}} \dim_{\text{Krull}} R_{\mathfrak{p}}.$$

Thus, the study of $\dim_{\text{Krull}} R$ is reduced to the study of $\dim_{\text{Krull}} R$ of a local ring.

Given a Noetherian local ring R with maximal ideal $\mathfrak{m}$, we will define two other types of dimensions:

- the **primary ideal dimension** $\dim_{\text{primary}} R$, which is the minimum number of generators across all $\mathfrak{m}$-primary ideals;
- the **Hilbert dimension** $\dim_{\text{Hilbert}} R$, which is more complicated and will be discussed in Section 9.2.

Then, the main theorem is $\dim_{\text{Krull}} R = \dim_{\text{Hilbert}} R = \dim_{\text{primary}} R$ for any local ring R.

§9.1 Preliminary: Length of a Module

Definition 9.1.1 (Composition Series)**.**

Given a ring R and R-module M, a **composition series** of a module M is a chain

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_n = 0$$

such that M_k/M_{k+1} is a **simple module** (i.e., have no submodule other than 0 and M_k/M_{k+1}).

Exercise 9.1.2. Prove that M is simple if and only if $M = R/\mathfrak{m}$ for a maximal ideal $\mathfrak{m}$.

This definition is an analogue of vector space. In particular, if $R = k$ is a field and $M \simeq k^n$, then we have the composition series

$$k^d \supset k^{d-1} \supset \cdots \supset k^1 \supset k^0 = \{0\}.$$

However, in contrast to vector spaces, composition series of a module does not always exist. For example, if $M = R = \mathbb{Z}$, then anything in the chain must be isomorphic to $\mathbb{Z}$, so we cannot get it down to zero.

Definition 9.1.3 (Length)**.**

For any module M, define the **length** $l(M)$ as the minimum length of a composition of a composition series of M. (let $l(M) = \infty$ if no finite composition series exists).

For example, we have $l(\mathbb{C}^d) = d$ (as a $\mathbb{C}$-module) and $l(\mathbb{Z}) = \infty$ (as a $\mathbb{Z}$-module).

It is not obvious that length is well-defined. Thus, we prove it.

Proposition 9.1.4 (Length is well-defined)**.**

If $l(M) = n$, then every composition series has length n, and any chain of submodules can be extend to a composition series.

To prove this, we need the following lemma.

Lemma 9.1.5.

If $N \subsetneq M$ and $l(M) < \infty$, then $l(N) < l(M) = n$.

▶ *Proof.* Take a composition series

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

Let $N_i = M_i \cap N$. Then, we have

$$N_0 \supset N_1 \supset \cdots \supset N_n.$$

Then, we can see that $N_k/N_{k+1} \subset M_k/M_{k+1}$, so either $N_k/N_{k+1} = 0$ or N_k/N_{k+1} is simple. Thus, $\{N_k\}$ is a composition series after erasing equal module. Therefore, we already have that $l(N) \leq l(M)$.

If $l(N) = l(M)$, then the only possibility is that we did not do the erasing in the paragraph. In particular, we have that for each k, $N_k/N_{k+1} = M_k/M_{k+1}$. Thus, we have

$$\begin{aligned} N_{n-1}/0 = M_{n-1}/0 &\implies N_{n-1} = M_{n-1}. \\ N_{n-2}/N_{n-1} = M_{n-2}/M_{n-1} &\implies N_{n-2} = M_{n-2} \\ &\vdots \\ &\implies N = M, \end{aligned}$$

which is a contradiction to $N \subsetneq M$. ☐

▶ *Proof of Proposition 9.1.4.* Given any chain of length k, we have

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_k = 0,$$

then by the lemma, we have

$$l(M_0) > l(M_1) > \cdots > l(M_k) \geq 0,$$

so $l(M) \geq k$. In particular, any composition series has length $\geq l(M)$. Moreover, any chain can be extended to a composition series. ☐

We now prove some more properties of a length.

Proposition 9.1.6 (Length behaves well under short exact sequence)**.**

Suppose we have a short exact sequence $0 \to N \to M \to P \to 0$, then $l(M) = l(N) + l(P)$.

▶ *Proof.* By Proposition 9.1.4, given a composition series of N and P, it suffices to find a composition of M. To that end, suppose we have composition series

$$N = N_0 \supsetneq N_1 \supsetneq \cdots \supsetneq N_k = 0$$
$$P = P_0 \supset P_1 \supset \cdots \supset P_\ell = 0.$$

Name the map $\pi : N \to P$. Then, we have a composition series of length $k + \ell$:

$$0 \subset N_k \subset N_{k-1} \subset \cdots \subset N_0 = N = \pi^{-1}(0) \subset \pi^{-1}P_{\ell-1} \subset \pi^{-1}P_{\ell-2} \subset \cdots \subset \pi^{-1}P_0 = P.$$ ☐

Corollary 9.1.7.

If there is a long exact sequence

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow \ldots \longrightarrow M_n \longrightarrow 0,$$

then

$$\sum_{i=1}^{n} (-1)^i l(M_i) = 0.$$

▶ *Proof.* Break the long exact sequence into short exact sequences: Let ϕ_i be the map from $M_i \to M_{i+1}$. Then, we have the short exact sequence

$$0 \longrightarrow \operatorname{Ker} \phi_i \longrightarrow M_i \longrightarrow \operatorname{Im} \phi_i \longrightarrow 0.$$

Thus, by Proposition 9.1.6, we have

$$l(M_i) = l(\operatorname{Im} \phi_i) + l(\operatorname{Ker} \phi_i) = l(\operatorname{Im} \phi_i) + l(\operatorname{Im} \phi_{i-1}).$$

Substituting this into the sum gives the desired result. ☐

Proposition 9.1.8.

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

▶ *Proof.* ($\Rightarrow$) Suppose $M_1 \subset M_2 \subset \ldots$, then $l(M_k)$ is increasing but bounded by $l(M)$. Same goes for descending chain.

($\Leftarrow$) Define

$$\begin{aligned} M_0 &= M \\ M_1 &= \text{maximal proper submodule of } M \\ M_2 &= \text{maximal proper submodule of } M_1 \\ &\vdots \end{aligned}$$

These exist since M is Noetherian. We get a descending chain $M_0 \supset M_1 \supset M_2 \supset \ldots$, so since M is Artinian, this chain eventually terminates. ☐

Corollary 9.1.9.

Let A be an Artinian ring, then any finitely-generated A-module has finite length.

§9.2 Hilbert's Dimension

§9.2.1 Definition

Before going into the definition, let us see some examples first.

Example 9.2.1 (Dimension of $k[x_1, \dots, x_n]$).

Let $R = k[x_1, \dots, x_n]_{(x_1,\dots,x_n)}$ (localized at maximal ideal $(x_1, \dots, x_n)$). Then, R is a local ring with maximal ideal $\mathfrak{m} = (x_1, \dots, x_n)$ and $R/\mathfrak{m} = k$. As a k-vector space, $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is a linear combinations of terms $x_1^{a_1} \cdots x_n^{a_n}$ where $a_1 + \cdots + a_n = i$. Thus,

$$\begin{aligned}\dim_k \mathfrak{m}^i/\mathfrak{m}^{i+1} &= \#\{(a_1, \dots, a_n) : a_1, \dots, a_n \geq 0, a_1 + \cdots + a_n = i\} \\ &= \binom{i+n-1}{n-1},\end{aligned}$$

by "star and bar trick". This is a polynomial of degree $n - 1$, one less than the dimension.

Example 9.2.2 (Artinian local ring).

On the other hand, if R is the Artinian local ring, which has dimension 0, then $\dim_k \mathfrak{m}^i/\mathfrak{m}^{i+1}$ is not a polynomial. Instead, we only know (by Theorem 5.3.2) that $\mathfrak{m}^N = 0$ for some N, so $\dim_k \mathfrak{m}^i/\mathfrak{m}^{i+1} = 0$ for all sufficiently large i.

If we regard zero polynomial as having "degree -1", then again, $\dim_k \mathfrak{m}^i/\mathfrak{m}^{i+1}$ is a polynomial of degree one less than the dimension.

Given a Noetherian local ring R with maximal ideal $\mathfrak{m}$, the above two examples lead us to consider the sequence

$$\ell_i = \dim_k \mathfrak{m}^i/\mathfrak{m}^{i+1}.$$

A sequence $(\ell_i)_{i \geq 0}$ is said to be **eventually polynomial** if there is a polynomial $p \in \mathbb{R}[x]$ such that $\ell_i = p(i)$ for all sufficiently large i. If such p exists (which must then be unique), we say that the sequence $(\ell_i)_{i \geq 0}$ is eventually polynomial with degree $\deg p$. **For the purpose of these notes, the degree of zero polynomial is -1.**

Theorem 9.2.3 (Hilbert dimension).

If R is a Noetherian local ring with maximal ideal $\mathfrak{m}$, then the **Hilbert-Samuel function**

$$\ell_i = \dim_{R/\mathfrak{m}} \mathfrak{m}^i/\mathfrak{m}^{i+1}$$

is eventually polynomial.

If it is eventually polynomial with degree d, then we define the **Hilbert dimension**

$$\dim_{\text{Hilbert}} R := d + 1.$$

We will prove this theorem in a greater generality (that we will need later) in the next section.

§9.2.2 Proof of Polynomiality

▶ **Setup** Let $S_\bullet = S_0 \oplus S_1 \oplus \dots$ be a graded ring such that

- S_0 is Artinian.
- $S_\bullet$ is generated (as an S_0-algebra) by finitely many elements in S_1.

Let $M_\bullet = M_0 \oplus M_1 \oplus \dots$ be a finitely-generated $S_\bullet$-module. This implies that, for each i, M_i is finitely-generated S_0-module, hence has finite length (by Corollary 9.1.9).

▶ **Main Theorem** Now, we state the main theorem.

Theorem 9.2.4 (Hilbert-Serre).

Assuming the above setup, the sequence

$$\ell_i := l_{S_0}(M_i)$$

is eventually polynomial. (The subscript in l_{S_0} means the length as S_0-module.)

Furthermore, if $S_\bullet$ is generated by m elements in S_1, then it is eventually polynomial of degree at most $m-1$.

To deduce Theorem 9.2.3 from Theorem 9.2.4, we plug in the **associated graded ring** (Definition 8.4.8)

$$S_\bullet = M_\bullet = \operatorname{gr}_{\mathfrak{m}} R = \bigoplus_{i \geq 0} \mathfrak{m}^i/\mathfrak{m}^{i+1},$$

and clearly the generators of $\mathfrak{m}$, which sits in $\mathfrak{m}/\mathfrak{m}^2$, are sufficient to generate $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ for all i, so $S_\bullet$ is finitely-generated at degree 1.

(As a consequence, we get that the Hilbert dimension is at most the minimum number of generators of $\mathfrak{m}$. Soon, we will prove a stronger result replacing $\mathfrak{m}$ with any $\mathfrak{m}$-primary ideal, which will play a key role in proving dimension theorem.)

▶ *Proof.* We first note the following elementary fact: if $c \geq 0$ is an integer such that the sequence $\ell_i' = \ell_{i+1} - \ell_i$ is eventually polynomial with degree d, then the sequence ℓ_i is eventually polynomial with degree $d+1$. (This follows from "finite difference".)

We use induction on m, the number of generators. The base case $m = 0$ is clear because then, $M_\bullet$ is finitely-generated S_0-module, so $M_n = 0$ for all large n. Thus, ℓ_i is eventually a zero polynomial, which has degree -1.

Now, assume that the result is known for $m-1$. Let x be one of the generators, and define

$$K_i = \operatorname{Ker}(M_i \xrightarrow{\cdot x} M_{i+1}) \quad \text{and} \quad L_{i+1} = M_{i+1}/xM_i,$$

so that we have the exact sequence

$$0 \longrightarrow K_i \longrightarrow M_i \xrightarrow{\cdot x} M_{i+1} \longrightarrow L_{i+1} \longrightarrow 0,$$

which gives (by Corollary 9.1.7)

$$l_{S_0}(K_i) - l_{S_0}(M_i) + l_{S_0}(M_{i+1}) - l_{S_0}(L_i) = 0.$$

Note that $K_\bullet$ and $L_\bullet$ are graded $S_\bullet/(x)$-module. Note that $S_1/(x)$ is generated by other $m-1$ generators, so by induction hypothesis, $l_{S_0}(K_\bullet)$ and $l_{S_0}(L_\bullet)$ is eventually polynomial of degree at most $m-2$. Thus, $l_{S_0}(M_{i+1}) - l_{S_0}(M_i) = l_{S_0}(L_i) - l_{S_0}(K_i)$ is eventually polynomial of degree at most $m-2$. The elementary fact at the beginning concludes. ☐

We note the following useful fact.

Proposition 9.2.5 (Alternative definition of $\dim_{\text{Hilbert}}$).

If Q is an ideal of R, then the following are equivalent:

(a) $\ell_i = l_{R/Q}(Q^i/Q^{i+1})$ is eventually polynomial of degree d.

(b) $p_i = l_{R/Q}(R/Q^i)$ is eventually polynomial of degree $d+1$.

▶ *Proof.* The exact sequence

$$0 \longrightarrow Q^i/Q^{i+1} \longrightarrow R/Q^{i+1} \longrightarrow R/Q^i \longrightarrow 0$$

gives

$$l_{R/Q}(R/Q^{i+1}) - l_{R/Q}(R/Q^i) = l(Q^{i+1}/Q^i),$$

so $p_i - p_{i+1} = \ell_i$, which implies the result by finite difference. ☐

By plugging in $Q = \mathfrak{m}$, the Hilbert dimension can also be defined as the degree of $l(R/\mathfrak{m}^i)$.

§9.3 Primary Ideal Dimension and Dimension Theorem

§9.3.1 Primary Ideal Dimension

We make the third definition of dimension:

Definition 9.3.1 (Primary ideal dimension).

For any local ring R with maximal ideal $\mathfrak{m}$, we define the **primary ideal dimension**, denoted $\dim_{\text{primary}} R$, to be the minimum nonnegative integer s for which there exists an $\mathfrak{m}$-primary ideal Q generated by $\leq s$ elements.

Example 9.3.2 (Examples of primary ideal dimension).

- Consider $R = \mathbb{C}[x_1, \dots, x_n]_{(x_1,\dots,x_n)}$, which is a local ring with maximal ideal $\mathfrak{m} = (x_1, \dots, x_n)$. The ideal $\mathfrak{m}$ is $\mathfrak{m}$-primary and has n generators, so we get that $\dim_{\text{primary}} R \leq n$.
- Let R be an Artinian local ring with maximal ideal $\mathfrak{m}$. By Theorem 5.3.2, $\mathfrak{m}^N = (0)$ for some N, so (0) is $\mathfrak{m}$-primary, which needs 0 generators, so $\dim_{\text{primary}} R = 0$.
- Consider
  $$R = \frac{\mathbb{C}[x,y]_{(x,y)}}{(xy)}$$
  which is a local ring with maximal ideal $\mathfrak{m} = (x, y)$. This ideal is generated by two elements. However, $Q = (x + y)$ is $\mathfrak{m}$-primary because $x^2 = x(x + y) \in Q$ and $y^2 = y(x + y) \in Q$, so $\sqrt{Q} = \mathfrak{m}$, so by Proposition 6.2.4, Q is $\mathfrak{m}$-primary.

  In particular, this implies that $\dim_{\text{primary}} R \leq 1$, and it is not enough to count the number of generators of $\mathfrak{m}$.

Notice that $\dim_{\text{primary}}$ is easier to provide an **upper bound**. In contrast, $\dim_{\text{Krull}}$ is easier to provide a **lower bound**.

There is no surprise that the main theorem that we will prove is the following.

Theorem 9.3.3 (Dimension Theorem).

For any Noetherian local ring R, we have

$$\dim_{\text{Krull}} R = \dim_{\text{Hilbert}} R = \dim_{\text{primary}} R.$$

Hence, we can safely call them all $\dim R$.

Proving this will occupy the rest of this subsection. We will show a chain of inequalities

$$\dim_{\text{primary}} R \overset{(1)}{\geq} \dim_{\text{Hilbert}} R \overset{(2)}{\geq} \dim_{\text{Krull}} R \overset{(3)}{\geq} \dim_{\text{primary}} R.$$

Section 9.3.2 will prove (1), Section 9.3.3 will prove (2), and Section 9.3.4 will prove (3). Each inequality takes some amount of work.

For the rest of this section, R is a Noetherian local ring, $\mathfrak{m}$ is the maximal ideal, and $k = R/\mathfrak{m}$ is the residue field.

§9.3.2 The Primary Ideal Dimension is at least the Hilbert Dimension

We prove $\dim_{\text{primary}} R \geq \dim_{\text{Hilbert}} R$. In plain terms, given a primary ideal Q with m generators, we have to show that $\dim_k \mathfrak{m}^{i+1}/\mathfrak{m}^i$ is eventually polynomial of degree at most $m-1$.

The strategy for this is to apply Theorem 9.2.4 to graded modules related to Q, and show that the length sequence must be within constant factor of $\dim_k \mathfrak{m}^{i+1}/\mathfrak{m}^i$. This will show that the degrees are equal, and will provide a degree upper bound of $\dim_k \mathfrak{m}^{i+1}/\mathfrak{m}^i$.

To do that, we let M and R be the associated graded ring corresponding to the Q-adic filtration

$$M = S = \operatorname{gr}_Q(R) = \bigoplus_{i\geq 0} Q^i/Q^{i+1}.$$

We check the hypothesis of Theorem 9.2.4.

- $S_0 = R/Q$ is Artinian because Theorem 5.3.2 (condition (c)) applies.
- S is clearly generated in degree 1 by the m generators of Q.

Thus, by Theorem 9.2.4, the sequence $l_{R/Q}(Q^i/Q^{i+1})$ is eventually polynomial with degree $d \leq m-1$.

Now, let d' be the degree of $\dim_k \mathfrak{m}^{i+1}/\mathfrak{m}^i$. We claim that $d = d'$, which will finish the proof. To do this, observe the following.

- By Proposition 9.2.5, $l_{R/Q}(R/Q^i)$ is eventually polynomial with degree $d+1$.
- By Proposition 9.2.5 again, $l_{R/\mathfrak{m}}(R/\mathfrak{m}^i)$ is eventually polynomial with degree $d'+1$.
- Since R is Noetherian and $\sqrt{Q} = \mathfrak{m}$, we get that $Q \supseteq \mathfrak{m}^c$ for some c. This implies that there is a chain of two surjections
  $$R/\mathfrak{m}^{ci} \twoheadrightarrow R/Q^i \twoheadrightarrow R/\mathfrak{m}^i,$$
  which gives
  $$l_{R/\mathfrak{m}}(R/\mathfrak{m}^{ci}) \geq l_{R/\mathfrak{m}}(R/Q^i) \geq l_{R/\mathfrak{m}}(R/\mathfrak{m}^i).$$
  Thus, as $i \to \infty$, $l_{R/\mathfrak{m}}(R/Q^i)$, a polynomial of degree $d+1$, is squeezed between two polynomials of degree $d'+1$. Hence, $d+1 = d'+1$, so $d = d'$.

Hence, the degree of $\dim_k \mathfrak{m}^{i+1}/\mathfrak{m}^i$ is $d \leq m-1$, so $\dim_{\text{Hilbert}} R \leq m$.

§9.3.3 The Hilbert Dimension is at least the Krull Dimension

In this section, we show that $\dim_{\text{Hilbert}} R \geq \dim_{\text{Krull}} R$. The idea is to slice by a non-zero divisor $f \in \mathfrak{m}$ (i.e., replace R with $R/(f)$). We show that the slicing **must** decrease the Hilbert dimension by at least 1, but it decreases the Krull dimension by at most 1. This will allow us to use induction.

Lemma 9.3.4.

Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Let $f \in \mathfrak{m}$ that is not a zero divisor. Then,

$$\dim_{\text{Hilbert}} R/(f) \leq \dim_{\text{Hilbert}} R - 1.$$

▶ *Proof.* Let $k = R/\mathfrak{m}$ and $R' = R/(f)$. Consider the short exact sequence

$$0 \longrightarrow \frac{(f)}{\mathfrak{m}^i \cap (f)} \longrightarrow \frac{R}{\mathfrak{m}^i} \longrightarrow \frac{R'}{\mathfrak{m}^i R'} \longrightarrow 0,$$

where the first map is embedding (f) into R and the second map comes from quotient projection $R \to R'$. Taking dimensions gives

$$\dim_k\left(R'/\mathfrak{m}^i R'\right) = \dim_k(R/\mathfrak{m}^i) - \dim_k\left(\frac{(f)}{(f)\cap\mathfrak{m}^i}\right).$$

By Artin-Rees Lemma (Theorem 8.3.1), the filtration $(f)\cap\mathfrak{m}^i$ is $\mathfrak{m}$-stable. This implies that there exists a constant c for which $(f)\cap\mathfrak{m}^i = f\mathfrak{m}^{i+c}$ for all sufficiently large i. This implies $(f)/((f)\cap\mathfrak{m}^i) \simeq R/\mathfrak{m}^{i+c}$ as R-module for all sufficiently large i. Therefore,

$$\dim_k(R'/\mathfrak{m}^i R') = \dim_k(R/\mathfrak{m}^i) - \dim_k(R/\mathfrak{m}^{i+c}),$$

which is indeed a polynomial of degree at most $\dim_{\text{Hilbert}} R - 1$. ☐

We now proceed to prove the second part of the theorem.

▶ *Proof of* $\dim_{\textit{Hilbert}} R \geq \dim_{\textit{Krull}} R$. We will do induction on $\dim_{\text{Hilbert}} R$.

If $\dim_{\text{Hilbert}} R = 0$, then $l(R/\mathfrak{m}^n)$ is constant for sufficiently large n. In particular, we have $\mathfrak{m}^n = \mathfrak{m}^{n+1} = \mathfrak{m}^{n+2} = \ldots$, so by Nakayama (Corollary 2.2.5), we get that $\mathfrak{m}^n = 0$, so condition (d) of Theorem 5.3.2 applies. Hence, R is Artinian, so $\dim_{\text{Krull}} R = 0$.

Otherwise, assume $\dim_{\text{Hilbert}} R > 0$, then consider the chain of prime ideals

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_s,$$

and we want to show that $\dim_{\text{Hilbert}} R \geq s$.

The first thing we will do is to mod out by $\mathfrak{p}_0$. In particular, note that

$$l(R/\mathfrak{m}^i) = l\left(\frac{R/\mathfrak{p}_0}{\mathfrak{m}^i}\right) \implies \dim_{\text{Hilbert}} R \geq \dim_{\text{Hilbert}} R/\mathfrak{p}_0.$$

Therefore, by replacing R with $R/\mathfrak{p}_0$, we can assume $\mathfrak{p}_0 = (0)$ and R is a domain.

The point of above is to make it easier to find a non-zero divisor for the lemma. In particular, for any $f \in \mathfrak{p}_1 \setminus \{0\}$, f is not a zero divisor. Now, we all we need is to cut the chain down to $R/(f)$. We set $\overline{\mathfrak{p}}_i = \mathfrak{p}_i/(f)$, so that

$$\overline{\mathfrak{p}}_1 \subset \overline{\mathfrak{p}}_2 \subset \cdots \subset \overline{\mathfrak{p}}_s \subset R/(f),$$

so we get a chain of length $s-1$ in R/f. In particular, the induction hypothesis implies $\dim_{\text{Hilbert}} R/(f) \geq s-1$. Hence,

$$\dim_{\text{Hilbert}} R \geq \dim_{\text{Hilbert}} R/(f) + 1 = s,$$

so we are done. ☐

§9.3.4 The Krull Dimension is at least the Primary Ideal Dimension

Finally, we prove the last inequality that $\dim_{\text{Krull}} R \geq \dim_{\text{primary}} R$. In plain language, we have to find an $\mathfrak{m}$-primary ideal generated by at most $\dim_{\text{Krull}} R$ elements. To do that, we use induction on the new measure of complexity of ideals, called **height**.

Definition 9.3.5 (Height).

For any ring R, the **height** (also known as the **codimension**) of a prime ideal $\mathfrak{p}$, denoted $\operatorname{ht}\mathfrak{p}$ is the maximum length of a chain of primes $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$ ending at $\mathfrak{p}$. In other words, $\operatorname{ht}\mathfrak{p} = \dim R_{\mathfrak{p}}$.

The height of an ideal I is defined as

$$\operatorname{ht} I = \min_{\text{prime } \mathfrak{p}\supset I} \operatorname{ht}\mathfrak{p}.$$

We have the following easy properties of heights.

Proposition 9.3.6 (Basic properties of height)**.**

If R is a local ring with maximal ideal $\mathfrak{m}$, then we have the following.

(a) $\operatorname{ht}\mathfrak{p} + \dim R/\mathfrak{p} \leq \dim R$.

(b) $\operatorname{ht} I = 0$ if and only if I is contained in a minimal prime of R.

(c) $\operatorname{ht} I = \dim R$ if and only if $\sqrt{I} = \mathfrak{m}$.

▶ *Proof.* (a) By correspondence theorem, a chain in $R/\mathfrak{p}$ corresponds to a chain in R containing $\mathfrak{p}$, so we can stick the chain of $R/\mathfrak{p}$ with the chain in $\operatorname{ht}\mathfrak{p}$ to get a chain of R, which must have length at most $\dim R$.

(b) $\operatorname{ht} I = 0$ if and only if there is a prime $\mathfrak{p}$ such that $\operatorname{ht}\mathfrak{p} = 0$. This prime $\mathfrak{p}$ must be a minimal prime, so I is contained in a minimal prime of R.

(c) We note that if $\operatorname{ht} I = \dim R$, then for any $\mathfrak{p} \supset I$, we have the chain $\mathfrak{p} = \mathfrak{p}_{\dim R} \supset \mathfrak{p}_{\dim R - 1} \supset \cdots \supset \mathfrak{p}_0$, so $\mathfrak{p}$ is actually a maximal ideal. There is only one maximal ideal in I, so it implies that $\mathfrak{p} = \mathfrak{m}$, so $\sqrt{I} = \mathfrak{m}$. ☐

▶ *Proof of $\dim_{Krull} R \geq \dim_{primary} R$.* Let $d = \dim_{\text{Krull}} R$. We need to find an $\mathfrak{m}$-primary ideal generated by $\leq d$ elements. The key claim is the following: "for each $i \leq d$, there exists $x_1, x_2, \ldots, x_i \in \mathfrak{m}$ such that $\operatorname{ht}((x_1, \ldots, x_i)) \geq i$."

This key claim implies the theorem because we can find $x_1, \ldots, x_{\dim R}$ satisfying the condition. Then, $Q = (x_1, \ldots, x_{\dim R})$ is $\mathfrak{m}$-primary by Proposition 9.3.6 (c), implying that $\dim_{\text{primary}} R \leq d$.

To prove the key claim, we find $x_1, \ldots, x_i$ inductively. Assume that we have $x_1, \ldots, x_{i-1}$ such that $\operatorname{ht}(x_1, \ldots, x_{i-1}) \geq i - 1$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be minimal primes over $(x_1, \ldots, x_{i-1})$ (i.e., minimal among ones containing $(x_1, \ldots, x_{i-1})$); there are finitely many because Corollary 5.2.12 applied on $R/(x_1, \ldots, x_{i-1})$. These primes have height at most $i - 1 \leq d - 1$, so they are not equal to $\mathfrak{m}$. In particular, $\mathfrak{m} \neq \mathfrak{p}_j$ for all j, so by prime avoidance, Problem 1.E, we have $\mathfrak{m} \neq \bigcup_{j=1}^{r} \mathfrak{p}_j$.

Therefore, pick $x_i \in \mathfrak{m}$ such that $x_i \notin \bigcup \mathfrak{p}_j$ for all j. Then, for any prime $\mathfrak{q} \supset (x_1, \ldots, x_{i-1}, x_i)$, we have $\operatorname{ht}(\mathfrak{q}) \geq i - 1$, but $\mathfrak{q} \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_r$, so $\operatorname{ht}(\mathfrak{q}) \geq i$. ☐

§9.4 Consequences of Dimension Theorem

We now harvest some consequences of the dimension theorem.

§9.4.1 Dimension of Local Rings

First, we note the following clear corollary.

Corollary 9.4.1.

If R is Noetherian local ring, then $\dim R$ is finite.

▶ *Proof.* Clear from either Hilbert dimension or primary ideal dimension. ☐

Warning 9.4.2.

In contrast, dimension of Notherian ring is not necessarily finite!

Proposition 9.4.3 (Slicing by f).

If R is a Noetherian local ring with maximal ideal $\mathfrak{m}$ and $f \in \mathfrak{m}$ is not a zero divisor, then

$$\dim R/(f) = \dim R - 1$$

▶ *Proof.* We showed the upper bound $\dim R/(f) \leq \dim R - 1$ over the course of proving dimension theorem (Lemma 9.3.4). To prove the lower bound, we use primary ideal dimension: suppose that $(x_1, \dots, x_d)$ generates an $\mathfrak{m}/(f)$-primary ideal. Then, its contraction to R, which is ideal $(f, x_1, \dots, x_d)$ would generate an $\mathfrak{m}$-primary ideal as well. Hence, $\dim R \leq \dim R/(f) + 1$, as desired. ☐

Example 9.4.4.

Suppose that you want to compute $\dim R$, where

$$R = \frac{\mathbb{C}[x, y, z]}{(xy + yz + zx)}$$

using the above property. We claim that for any maximal ideal $\mathfrak{m}$ of R, we have $\dim R_{\mathfrak{m}} = 2$. To see why, note that a maximal ideal $\mathfrak{m}$ of R is a contraction of a maximal ideal $\mathfrak{n} \subseteq \mathbb{C}[x, y, z]$ such that $xy + yz + zx \in \mathfrak{n}$. Note that $\mathbb{C}[x, y, z]$ is a domain, so $xy + yz + zx$ is not a zero divisor. Thus, by the above Proposition 9.4.3,

$$\dim R_{\mathfrak{m}} = \dim \frac{\mathbb{C}[x, y, z]_{\mathfrak{n}}}{(xy + yz + zx)} = \dim \mathbb{C}[x, y, z]_{\mathfrak{n}} - 1 = 3 - 1 = 2.$$

Thus, taking supremum across all ideals $\mathfrak{m}$ gives $\dim R = 2$.

(This argument would have worked if $xy+yz+zx$ is replaced with any $f \neq 0 \in \mathbb{C}[x, y, z]$.)

Proposition 9.4.5.

If R is a Noetherian local ring with maximal ideal $\mathfrak{m}$ and $\widehat{R}$ is the $\mathfrak{m}$-adic completion, then $\dim \widehat{R} = \dim R$.

▶ *Proof.* By Proposition 8.4.5, $\widehat{R}$ is local with maximal ideal $\widehat{\mathfrak{m}}$, which is a completion of $\mathfrak{m}$ as a module. From Corollary 8.4.4, we get that $\widehat{\mathfrak{m}}^i/\widehat{\mathfrak{m}}^{i+1} \simeq \mathfrak{m}^i/\mathfrak{m}^{i+1}$, so the Hilbert dimensions are the same. ☐

§9.4.2 Krull's Principal Ideal Theorem

Theorem 9.4.6 (Krull's Height Theorem).

Let R be a Noetherian ring, and I be an ideal with n generators. Then, $\operatorname{ht} I \leq n$. (Translation: every prime ideal minimal over I has height at most n.)

▶ *Proof.* Let $\mathfrak{p}$ be a minimal prime among those containing I. Then, $\operatorname{ht}(IR_{\mathfrak{p}}) = \dim R_{\mathfrak{p}}$, so by Proposition 9.3.6, $IR_{\mathfrak{p}}$ is $\mathfrak{p}R_{\mathfrak{p}}$-primary. Hence, using primary ideal dimension, we have

$$\operatorname{ht} \mathfrak{p} = \dim R_{\mathfrak{p}} = \dim_{\text{primary}} R_{\mathfrak{p}} \leq n,$$

so $\operatorname{ht} I \leq n$. ☐

A special case of this is the following.

Corollary 9.4.7 (Krull's Principal Ideal Theorem, or Krull's Hauptidealsatz)**.**

Let R be a Noetherian ring and $f \in R$. Let $\mathfrak{p}$ be a prime ideal minimal among those containing f.

(a) $\operatorname{ht} \mathfrak{p} \leq 1$.

(b) If f is not a zero divisor, then $\operatorname{ht} \mathfrak{p} = 1$.

► *Proof.* (a) follows immediately from Theorem 9.4.6. To prove (b), note that if $\operatorname{ht} \mathfrak{p} = 0$, then, $R_{\mathfrak{p}}$ has dimension 0, hence Artinian (by Theorem 5.3.2 (b)). This means that $f \in \mathfrak{p}R_{\mathfrak{p}}$ is nilpotent (by Theorem 5.3.2 (d)), hence a zero divisor in R, a contradiction. ☐

Remark 9.4.8.

There are other proofs of Krull's principal ideal theorem and Krull's height theorem that does not need knowledge in this chapter. See for example, [Vak24, §12.3]

We also note the following useful property, although the proof is deferred to Corollary 10.4.3.

Proposition 9.4.9.

If R is a Noetherian ring, then $\dim R[x] = \dim R + 1$.

§9.5 Regular Local Ring

§9.5.1 Definition and Basic Properties

For any Noetherian local ring R with maximal ideal $\mathfrak{m}$ and $k = R/\mathfrak{m}$, we note that

$$\begin{aligned} \dim R &\geq \#(\text{generators of } \mathfrak{m}) && \text{(primary ideal dimension)} \\ &\geq \dim_k(\mathfrak{m}/\mathfrak{m}^2). && \text{(Nakayama; Corollary 2.2.6)} \end{aligned}$$

Definition 9.5.1 (Regular local rings)**.**

A Noetherian local ring $(R, \mathfrak{m})$ is a **regular local ring** if the three above quantities are all equal:

$$\dim R = \dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = \#(\text{generators of } \mathfrak{m}).$$

(Equivalently, the first two are equal. Also, we always assume that regular local rings are Noetherian.)

Example 9.5.2 (Regular local rings of dimension 0 and 1.)**.**

- R is regular local with dimension 0, if and only if $\mathfrak{m} = \mathfrak{m}^2$, which (by Nakayama; Corollary 2.2.5) is equivalent to either $\mathfrak{m} = 0$ or R is a field.
- R is a regular local ring with dimension 1 if and only if R is a DVR (by Theorem 7.1.4 (d)).

  Thus, regular local ring generalizes the concept of DVR to higher-dimension.

Example 9.5.3 (Regular local rings correspond to smooth objects).

Regular local rings correspond to rings of smooth varieties localized at a point. We will not explain this connection precisely. Let us first confine ourself to a simpler example of hypersurface

$$R = \left(\frac{k[x_1, \ldots, x_n]}{(f)}\right)_{(x_1,\ldots,x_n)}$$

where k is an algebraically closed field and $f \in k[x_1, \ldots, x_n]$ such that $f(0, \ldots, 0) = 0$. Thus, $\dim R = n - 1$. We write

$$f(x_1, \ldots, x_n) = a_1x_1 + \cdots + a_nx_n + (\text{higher degree terms}).$$

Let $\overline{\mathfrak{m}}$ be the maximal ideal of R, which correspond to the maximal ideal $\mathfrak{m}$ of the localization $k[x_1, \ldots, x_n]_{(x_1,\ldots,x_n)}$. Then, we have

$$\frac{\overline{\mathfrak{m}}}{\overline{\mathfrak{m}}^2} = \frac{\mathfrak{m}}{(\mathfrak{m}^2, f)} = \frac{\mathfrak{m}/\mathfrak{m}^2}{\operatorname{Span}(f \bmod \mathfrak{m}^2)} \simeq \frac{\operatorname{Span}(e_1, \ldots, e_n)}{\langle a_1e_1 + \cdots + a_ne_n = 0\rangle},$$

which has dimension $n - 1$ if and only if at least one of a_i is nonzero.

Equivalently, R is a regular local ring if and only if at least one partial derivative $\partial f/\partial x_i$ does not vanish at $(0, \ldots, 0)$.

In general, if R is a localization at $(x_1, \ldots, x_n)$ of ring in form

$$k[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$$

that has dimension $n - r$, then R is a regular local ring if and only if the Jacobian matrix

$$\left(\left.\frac{\partial f_i}{\partial x_j}\right|_{(0,\ldots,0)}\right)_{1\le i\le r, 1\le j\le n}$$

has rank $n - r$. This is exactly the condition for $k[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$ to be a smooth variety at $(0, \ldots, 0)$.

If k is not algebraically closed, then maximal ideals may not be of the form $(x_1-a_1, \ldots, x_n-a_n)$, in which case checking regularity is harder and beyond the scope of these notes. Separability issues can arise of k is not perfect.

Regular local rings are the nicest kinds of rings that generalize to arbitrary dimension. Unfortunately, studying regular local rings is quite difficult. In the section, we will present something that we can prove with all tools developed thus far. The main highlight is that with mild conditions (that holds in the case of any variety), the $\mathfrak{m}$-adic completion of regular local ring R must be isomorphic to $k[[x_1, \ldots, x_d]]$. Then, in Section 9.5.2, we state some nice facts that we *cannot* prove.

First, we study the associated graded ring $\operatorname{gr}_{\mathfrak{m}} R$ (Definition 8.4.8), defined by

$$\operatorname{gr}_{\mathfrak{m}} R = \bigoplus_{i\ge 0} \mathfrak{m}^i/\mathfrak{m}^{i+1}$$

and show that they are the nicest as possible.

Proposition 9.5.4 (gr of regular local ring).

If R is regular local with maximal ideal $\mathfrak{m}$ and dimension d, then $\operatorname{gr}_{\mathfrak{m}} R \simeq k[x_1, \ldots, x_d]$. Consequently, $\dim_{R/\mathfrak{m}} \mathfrak{m}^i/\mathfrak{m}^{i+1} = \binom{i+d-1}{d-1}$.

▶ *Proof.* Let $\mathfrak{m} = (t_1, \dots, t_d)$ be the minimal generating set. Then, we have a surjective map

$$\begin{aligned} k[x_1, \dots, x_d] &\to \operatorname{gr}_{\mathfrak{m}} R \\ x_i &\mapsto t_i \end{aligned}$$

We have to show that this is injective. Suppose that a nonzero homogeneous f of degree s maps to 0. Then, the map collapse to a surjective map $k[x_1, \dots, x_d]/(f) \to \operatorname{gr}_{\mathfrak{m}} R$. Therefore,

$$\dim \operatorname{gr}_{\mathfrak{m}} R \le \dim \frac{k[x_1, \dots, x_d]}{(f)} = d - 1.$$

However, if $P = \bigoplus_{i \ge 1} \mathfrak{m}^i/\mathfrak{m}^{i+1}$ be the ideal of positive degree, then $(\operatorname{gr}_{\mathfrak{m}} R)_P$ (localize at P) have the same associated graded ring as R, hence having the same Hilbert dimension as R. Thus, $\dim \operatorname{gr}_{\mathfrak{m}} R \ge \dim(\operatorname{gr}_{\mathfrak{m}} R)_P = d$. This is a contradiction. ☐

Corollary 9.5.5.

Any regular local ring is a domain.

▶ *Proof.* Suppose $a, b \ne 0$. There exists i, j such that $a \in \mathfrak{m}^i \setminus \mathfrak{m}^{i+1}$ and $b \in \mathfrak{m}^j \setminus \mathfrak{m}^{j+1}$. Thus, $\overline{a} \in (\operatorname{gr}_{\mathfrak{m}} R)_i$ and $\overline{b} \in (\operatorname{gr}_{\mathfrak{m}} R)_j$ are both nonzero, so we have $\overline{a}\overline{b} \ne 0$. Thus, $ab \in \mathfrak{m}^{i+j} \setminus \mathfrak{m}^{i+j+1}$, so $ab \ne 0$. ☐

Theorem 9.5.6 (Completion of regular local rings is $k[[x_1, \dots, x_d]]$)**.**

Let R be a regular local ring of dimension d, $\mathfrak{m}$ be the maximal ideal, and $k = R/\mathfrak{m}$. If every element $a \in k$ can be lifted to $\widetilde{a} \in R$ such that $a \equiv \widetilde{a} \pmod{\mathfrak{m}}$, then

$$\widehat{R} \simeq k[[x_1, \dots, x_d]]$$

(where $\widehat{R}$ denotes the $\mathfrak{m}$-adic completion).

Note that the lifting map condition holds whenever $R = k[x_1, \dots, x_n]/I$ for some ideal I. Thus, this theorem shows that completion of any smooth variety is isomorphic to $k[[x_1, \dots, x_d]]$!

▶ *Proof.* The idea is that from Proposition 9.5.4, we already have the isomorphism $k[x_1, \dots, x_d] \to \operatorname{gr}_{\mathfrak{m}} R$. One needs to realize this as $\operatorname{gr} \psi$, where $\psi : k[x_1, \dots, x_d] \to R$ is a map. Then, we will be able to use Lemma 8.4.9 to conclude that $\widehat{\psi} : k[[x_1, \dots, x_d]] \to \widehat{R}$ is an isomorphism.

To do this, let $\mathfrak{m} = (t_1, \dots, t_d)$ as above. Define

$$\begin{aligned} \psi : k[x_1, \dots, x_d] &\to R \\ a &\mapsto \widetilde{a} \quad \text{for all } a \in k \\ x_i &\mapsto t_i \end{aligned}$$

Then, it is clear that $\operatorname{gr} \psi$ is the map defined in Proposition 9.5.4, which is an isomorphism. Thus, by Lemma 8.4.9, ψ is an isomorphism. ☐

It's then natrual to ask whether all **complete** regular local rings are of the form $k[[x_1, \dots, x_n]]$. (A ring is complete if it arises from a completion.) It turns out that the answer is no; there is a whole other family of regular local rings.

Example 9.5.7.

Let A be a complete DVR (e.g., $A = \mathbb{Z}_p$). Let $\mathfrak{n} = (\pi)$ be its maximal ideal and $A/\mathfrak{n} = k$. We claim that

$$R = A[[x_1, \dots, x_d]]$$

is regular local of dimension $d+1$ with maximal ideal $\mathfrak{m} = (\pi, x_1, \dots, x_d)$. This is because one can verify that $\operatorname{gr}_{\mathfrak{m}} R = k[\overline{\pi}, \overline{x}_1, \dots, \overline{x}_d]$. For example, $\mathbb{Z}_p[[x, y]]$ is regular local which is not of the above form.

§9.5.2 Harder Facts about Regular Local Rings

Regular local rings enjoy further nice properties. To conclude this section, we state some harder facts about regular local rings that we will not be able to prove.

Theorem 9.5.8 (Auslander–Buchsbaum)**.**

If R is a regular local ring, then R is a UFD (hence integrally closed).

See [Eis95, Thm. 19.19] for the proof. Note that the weaker fact that R is integrally closed is doable by elementary methods.

We also have a surprisingly difficult theorem by Serre.

Theorem 9.5.9 (Serre)**.**

If R is a regular local ring, then for any prime ideal $\mathfrak{p}$, the localization $R_{\mathfrak{p}}$ is still regular.

See [Eis95, Cor. 19.14] for the proof.

These two theorems signify the next step of the subject, which is to introduce **homological methods**. Roughly speaking, homological methods introduces construction originally developed for algebraic topology (e.g., chain complexes, homology, etc.). These constructions allow us to cleanly manipulate a sheer number of spaces and maps, which then allow us to prove more difficult theorems. You will see a glimpse of those homological techniques in Chapter 10.

§9.6 Problems

Problem 9.A. Let A and B be domains with $\dim A = \dim B$. Prove that any surjective map $\phi : A \to B$ is an isomorphism.

Problem 9.B. For each of the rings R and maximal ideal $\mathfrak{m}$ in Problem 8.F, compute the Hilbert dimension of $R_{\mathfrak{m}}$.

Problem 9.C. Let $R = \mathbb{C}[x, y]/(y^2 - x^3 - x)$ and $\mathfrak{m} = (x, y)$. Find an $\mathfrak{m}$-primary ideal of $R_{\mathfrak{m}}$ that is principal (hence showing that $\dim R_{\mathfrak{m}} \leq 1$).

Problem 9.D. Prove that a domain A is a UFD if and only if every prime ideal with height 1 is principal.

Problem 9.E. Prove that the ring

$$\frac{\mathbb{C}[w, x, y, z]}{(wz - xy, wy - x^2, xz - y^2)}$$

has dimension 2 (despite it is cut out by 3 equations).

Problem 9.F. Prove that

$$\left(\frac{\mathbb{C}[x, y, z]}{(x^2 - yz)}\right)_{(x,y,z)}$$

is not a regular local ring, even though Problem 4.C shows that it is integrally closed.

The next two problems concern integrally closed domains.

Problem 9.G (Serre's R1 + S2 Criterion)**.** Let A be a domain. Prove that A is integrally closed if and only if both of the following holds.

(i) $A_\mathfrak{p}$ is a DVR for all prime ideal $\mathfrak{p}$ with height 1.

(ii) For any $f \in A$, all associated primes of A-module $A/(f)$ are minimal over (f) (and thus have codimension 1).

(Hint: to prove that integrally closed implies (ii), reduce to the local case and mimic the proof of Theorem 7.1.4 (b) ⇒ (c). To prove that (i) and (ii) implies integrally closed, use Problem 6.E.)

Problem 9.H (Algebraic Hartogs Lemma)**.** Let A be an integrally closed domain. Prove that

$$A = \bigcap_{\mathfrak{p} \text{ height } 1} A_\mathfrak{p}.$$

[TODO: Cohen-Macaulay]

10 Flatness

Recall from Definition 2.5.10 that we defined an R-module M to be flat if tensoring by M preserves exactness. As tensor is already right-exact, this is equivalent to preserving injection, i.e., if $A \to B$ is injective, then so is the induced map $A \otimes_R M \to B \otimes_R M$. In this chapter, we will explore the properties and uses of flat modules.

The first thing that you probably have noticed is that in order to prove that M is flat, one needs to check that it preserves injectivity for all injective morphisms $A \to B$ (including infintely-generated ones). This is a horrible condition to check. This, in Section 10.1 and Section 10.2, we develop conditions to check if a module is flat (or not flat).

The cleanest way to do this require formidable machinery in homological algebra, which borrows tools from algebraic topology to study algebra. One can motivate this as follows: whenever you see a right exact functor, like $0 \to A \to B \to C \to 0$, which implies the right exact sequence

$$A \otimes_R M \longrightarrow B \otimes_R M \longrightarrow C \otimes_R M \longrightarrow 0,$$

you should dream of extending the sequence indefinitely leftward, giving the **left-derived functor**. In this case, the exact sequence we will construct is

$$\begin{tikzcd}
 & \dots \arrow[r] & \operatorname{Tor}_2^R(C,M) \arrow[dll] & \\
\operatorname{Tor}_1^R(A,M) \arrow[r] & \operatorname{Tor}_1^R(B,M) \arrow[r] & \operatorname{Tor}_1^R(C,M) \arrow[dll] & \\
A \otimes_R M \arrow[r] & B \otimes_R M \arrow[r] & C \otimes_R M \arrow[r] & 0
\end{tikzcd}$$

In some sense, Tor measures the failure of exactness of tensor product, and thus useful for understanding flatness. We will define $\operatorname{Tor}_i^R(A,M)$ at the beginning of Section 10.2. Then, we provide various flatness criteria that we get from understanding the Tor functor.

In algebraic geometry, flat modules are tied closely with flat morphisms.

Definition 10.0.1.

A ring morphisms $\phi : A \to B$ is **flat** if and only if it promotes B to a flat A-algebra.

Geometrically, flat morphism means "nicely varying". An example of morphisms that are not nicely varying is

$$\begin{aligned} \phi : \mathbb{C}[x] &\to \frac{\mathbb{C}[x,y]}{(xy)} \\ x &\mapsto x \end{aligned}$$

Geometrically, this corresponds to the map from variety $\{xy = 0\}$ to an affine line $\{x \in \mathbb{C}\}$ by projecting to the x coordinate. One can check that $\mathbb{C}[x,y]/(xy)$ is not a flat $\mathbb{C}[x]$-algebra (exercise). This is not "nicely-varying" because the map is injective at all points, except above $x = 0$, where an entire line is squished into a single point. The key result of this sort is flatness implies constant dimension of fiber, which we prove in Section 10.4.

§10.1 Homological Algebra Crash Course

Before we can do that, some 18.905 background is in order.

§10.1.1 Homology

▶ Chain Complexes

Definition 10.1.1.

A **chain complex** is a sequence

$$\cdots \xrightarrow{\partial_3} A_2 \xrightarrow{\partial_2} A_1 \xrightarrow{\partial_1} A_0 \xrightarrow{\partial_0} A_{-1} \xrightarrow{\partial_{-1}} A_{-2} \xrightarrow{\partial_{-2}} \cdots$$

such that $\partial_{i-1} \circ \partial_i = 0$ for all i (i.e., $\operatorname{Im} \partial_i \subseteq \operatorname{Ker} \partial_{i-1}$).

(Most chain complexes we consider will be finite. Strictly speaking, they can be extended infinitely in both directions with 0's.)

▶ Homology

Definition 10.1.2.

Given a chain complex A_* as above, the **n-th homology group** is defined as

$$H_n(A_*) := \operatorname{Ker} \partial_n / \operatorname{Im} \partial_{n+1}.$$

Example 10.1.3.

Any exact sequence has all of its homology groups equal to 0. Thus, the homology groups can be thought of as how "far from exact" a chain complex is.

Theorem 10.1.4 (A variant of Snake lemma)**.**

Given a short exact sequence $0 \longrightarrow A_* \longrightarrow B_* \longrightarrow C_* \longrightarrow 0$ of chain complex, i.e., the commuting diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
\cdots \arrow[r] & A_{n+1} \arrow[r, "\partial"] \arrow[d] & A_n \arrow[r, "\partial"] \arrow[d] & A_{n-1} \arrow[r] \arrow[d] & \cdots \\
\cdots \arrow[r] & B_{n+1} \arrow[r, "\partial"] \arrow[d] & B_n \arrow[r, "\partial"] \arrow[d] & B_{n-1} \arrow[r] \arrow[d] & \cdots . \\
\cdots \arrow[r] & C_{n+1} \arrow[r, "\partial"] \arrow[d] & C_n \arrow[r, "\partial"] \arrow[d] & C_{n-1} \arrow[r] \arrow[d] & \cdots \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Then, there exists an exact sequence of homology groups

$$\begin{tikzcd}
\cdots \arrow[r] & H_{n+1}(B_*) \arrow[r] & H_{n+1}(C_*) \arrow[dll, "\delta"'] \\
H_n(A_*) \arrow[r] & H_n(B_*) \arrow[r] & H_n(C_*) \arrow[dll, "\delta"'] \\
H_{n-1}(A_*) \arrow[r] & H_{n-1}(B_*) \arrow[r] & \cdots
\end{tikzcd},$$

This is a more general version of Snake Lemma (Lemma 2.3.5) because if A_*, B_*, and C_* each have two nonzero modules, then we recover Lemma 2.3.5. It can be proven by a similary tedious argument, so we omit the proof.

§10.1.2 Free Resolutions

Definition 10.1.5.

Given an R-module M, a **free resolution** of M is a chain complex of free R-modules which has 0-th homology group M and n-th homology group 0 for $n \neq 0$.

Example 10.1.6.

As a $\mathbb{Z}$-module, $\mathbb{Z}/n\mathbb{Z}$ has a free resolution given by

$$\cdots \longrightarrow 0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \longrightarrow 0 \longrightarrow \cdots .$$

Every module M has a free resolution. Indeed, we can first take a free module M_0 with a surjection $\varphi : M_0 \to M$. Then, take a free module M_1 with a surjection $\partial_1 : M_1 \to \operatorname{Ker} \varphi$. Take a free module M_2 with a surjection $\partial_2 : M_2 \to \operatorname{Ker} \partial_1$, and so on. The resulting complex

$$\cdots \xrightarrow{\partial_3} M_2 \xrightarrow{\partial_2} M_1 \xrightarrow{\partial_1} M_0 \longrightarrow 0 \longrightarrow \cdots$$

is a free resolution of M by construction. (The process may not terminate, but that's fine because free resolutions need not be finite.)

§10.2 Flatness and Tor

§10.2.1 The Tor Functor

Every right-exact functor induces a left derived functor. In the case of the tensor product, the derived functor is Tor.

Definition 10.2.1.

Given R-modules M and N, let N_* be a free resolution of N, and let $M \otimes N_*$ denote the chain complex induced by tensoring each component of N_* with M. Then, the ***n*-th Tor functor** is defined as

$$\operatorname{Tor}_n^R(M, N) := H_n(M \otimes N_*).$$

In particular, Tor_0^R is simply $\otimes_R$.

Example 10.2.2.

We will compute $\operatorname{Tor}_i^{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$. Using the free resolution of $\mathbb{Z}/n\mathbb{Z}$ in the previous section, we simply want the homology groups of

$$\cdots \to 0 \longrightarrow \mathbb{Z}/m\mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z}/m\mathbb{Z} \longrightarrow 0 \longrightarrow \cdots .$$

The image of multiplication by n in $\mathbb{Z}/m\mathbb{Z}$ is all the multiples of $\gcd(m, n)$, and the kernel is isomorphic to $\mathbb{Z}/\gcd(m, n)\mathbb{Z}$, so

$$\operatorname{Tor}_0^{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \simeq \operatorname{Tor}_1^{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/\gcd(m, n)\mathbb{Z},$$

and $\operatorname{Tor}_i^{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = 0$ for $i \geq 2$.

Tor satisfies some nice properties, but proving many them is beyond the scope of this chapter.

Theorem 10.2.3 (Properties of Tor)**.**

(a) $\operatorname{Tor}_n^R(M, N)$ does not depend on the choice of free resolution N_*.

(b) If $0 \to A \to B \to C \to 0$ is a short exact sequence of R-modules, then there is a long exact sequence

$$\begin{tikzcd}
 & \cdots \arrow[r] & \operatorname{Tor}_2^R(C, M) \arrow[dll] & \\
\operatorname{Tor}_1^R(A, M) \arrow[r] & \operatorname{Tor}_1^R(B, M) \arrow[r] & \operatorname{Tor}_1^R(C, M) \arrow[dll] & \\
A \otimes_R M \arrow[r] & B \otimes_R M \arrow[r] & C \otimes_R M \arrow[r] & 0
\end{tikzcd}$$

(c) $\operatorname{Tor}_n^R(M, N) \simeq \operatorname{Tor}_n^R(N, M)$.

(d) If I is a directed set and $(N_i)_{i \in I}$ is a diagram, then

$$\operatorname{Tor}_n^R\left(M, \varinjlim_{i \in I} N_i\right) = \varinjlim_{i \in I} \operatorname{Tor}_n^R(M, N_i)$$

(cf. colimit in Section 2.4).

▶ *Proof.* (a) The proof of this is elementary, but it requires slightly more homological algebra than what we have given. Thus, this is deferred to Theorem B.3.1.

(b) Take a free resolution $\cdots \to M_2 \to M_1 \to M_0$ of M. Since M_i is free (hence flat), we get a commutative diagram with exact rows

$$\begin{tikzcd}
 & \cdots \arrow[d] & \cdots \arrow[d] & \cdots \arrow[d] & \\
0 \arrow[r] & A \otimes_R M_i \arrow[r] \arrow[d] & B \otimes_R M_i \arrow[r] \arrow[d] & C \otimes_R M_i \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A \otimes_R M_{i-1} \arrow[r] \arrow[d] & B \otimes_R M_{i-1} \arrow[r] \arrow[d] & C \otimes_R M_{i-1} \arrow[r] \arrow[d] & 0 \\
 & \cdots & \cdots & \cdots &
\end{tikzcd}$$

In particular, we have the exact sequence of chain complexes $0 \to A \otimes_R M_* \to B \otimes_R M_* \to C \otimes_R M_* \to 0$. Then, the homology long exact sequence Theorem 10.1.4 gives the desired long exact sequence.

(c) Intuitively, this should be true because tensor product is symmetric ($M \otimes_R N = N \otimes_R M$), but this turns out to be a very difficult one to prove. Roughly speaking, we take a free resolution of both M and N. Then, take their product $M_i \otimes_R N_j$ to get a double complex (that looks like an infinite grid). Then, one manipulates homology groups of the double complex and proves the result (typically, this is done via spectral sequence). We refer the reader to [Wei94, Thm. 2.7.2].

(d) This follows from the following two facts:

- Colimit preserves exactness (Theorem 2.4.13), hence preserving kernels, images, and homology groups in a chain complex.
- Colimit commutes with tensor product: $M \otimes_R \varinjlim_{i \in I} N_i = \varinjlim_{i \in I}(M \otimes_R N_i)$. This can be proven quite cleanly by considering universal properties of the respective sides.

Thus, every step in the definition of Tor commutes with the colimit, so Tor commutes with colimit. ☐

§10.2.2 Ideal-theoretic Criterion of Flatness

Theorem 10.2.4 (Ideal-theoretic Criterion of Flatness).

Let M be an R-module. The following are equivalent:

(a) M is flat.

(b) $\operatorname{Tor}_i^R(M, N) = 0$ for all R-modules N and $i \geq 1$.

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

(d) $\operatorname{Tor}_1^R(M, R/I) = 0$ for all ideals $I \subseteq R$.

▶ *Proof.* Note that (b) $\Rightarrow$ (c) $\Rightarrow$ (d) is trivial.

(a) $\Rightarrow$ (b). Consider a free resolution N_* of N given by

$$\cdots \longrightarrow N_2 \longrightarrow N_1 \longrightarrow N_0 \longrightarrow \cdots,$$

and consider the long exact sequence

$$\cdots \longrightarrow N_2 \longrightarrow N_1 \longrightarrow N_0.$$

As M is flat, tensoring by M preserves exactness, so

$$\cdots \longrightarrow M \otimes N_2 \longrightarrow M \otimes N_1 \longrightarrow M \otimes N_0$$

is also exact. Thus, the i-th homology group of $M \otimes N_*$ is 0 for all $i \geq 1$.

(d) $\Rightarrow$ (a). We prove this in three steps.

1. **$\operatorname{Tor}_1^R(M, N) = 0$ for all finitely-generated modules N.** We use induction on the number of generators n of N. First, if $n = 1$, then $N \simeq R/I$ for some ideal I, so the result is clear. Now, assume that the result is true for $n - 1$ generators. Let N be a module with n generators $e_1, \ldots, e_n$. Then, we have the exact sequence

$$0 \longrightarrow R[e_n] \longrightarrow N \longrightarrow N/R[e_n] \longrightarrow 0,$$

which gives long exact sequence (by Theorem 10.2.3 (b))

$$\ldots \longrightarrow \operatorname{Tor}_1^R(M, R[e_n]) \longrightarrow \operatorname{Tor}_1^R(M, N) \longrightarrow \operatorname{Tor}_1^R(M, N/R[e_n]) \longrightarrow \ldots.$$

Since $N/R[x]$ is generated by $e_1, \ldots, e_{n-1}$, we have by induction hypothesis that $\operatorname{Tor}_1^R(M, R[e_n]) = \operatorname{Tor}_1^R(M, N/R[e_n]) = 0$, so $\operatorname{Tor}_1^R(M, N) = 0$.

2. **$\mathrm{Tor}_1^R(M,N)=0$ for all modules N.** Note that N is a colimit of finitely-generated modules $\lim_{i\in I} N_i$ (by Proposition 2.4.8). We know that from Step 1. that $\mathrm{Tor}_1^R(M,N_i)=0$, so by Theorem 10.2.3 (d), we get that

$$\mathrm{Tor}_1^R(M,N)=\mathrm{Tor}_1^R\left(M,\varinjlim_{i\in I} N_i\right)=\varinjlim_{i\in I}\mathrm{Tor}_1^R(M,N_i)=\varinjlim_{i\in I}0=0.$$

3. **M is flat.** Let $\phi: A\to B$ be injective. Then, the exact sequence $0\to A\to B\to B/A\to 0$ gives the long exact sequence

$$0=\mathrm{Tor}_1^R(B/A,M)\longrightarrow A\otimes M\longrightarrow B\otimes M\longrightarrow (B/A)\otimes M\longrightarrow 0,$$

giving that $A\otimes M\to B\otimes M$ is injective. ☐

How useful are these conditions? It turns out the last two have a natural interpretation.

Theorem 10.2.5.

$\mathrm{Tor}_1^R(M,R/I)=0$ if and only if $\varphi: I\otimes_R M\to M$ given by $i\otimes m\mapsto im$ is injective.

▶ *Proof.* Consider the short exact sequence $0\to I\to R\to R/I\to 0$. Since $R\otimes M=M$ and $\mathrm{Tor}_1^R(R,M)=0$ (free modules are flat), we get a long exact sequence

$$0\longrightarrow \mathrm{Tor}_1^R(R/I,M)\xrightarrow{\alpha} I\otimes M\xrightarrow{\beta} M\longrightarrow (R/I)\otimes M\longrightarrow 0.$$

Since α is injective, its image is 0 if and only if $\mathrm{Tor}_1^R(R/I,M)=0$. On the other hand, $\mathrm{Im}\,\alpha=\mathrm{Ker}\,\beta$, and $\mathrm{Ker}\,\beta=0$ if and only if $\beta: I\otimes M\to M$ is injective. Thus, the two are equivalent. ☐

We can now do a nontrivial example of checking that a morphism is flat.

Example 10.2.6.

Consider a ring morphism

$$\phi:\mathbb{C}[z]\to\frac{\mathbb{C}[x,y]}{(xy)}$$
$$z\mapsto x+y$$

(Geometrically, this corresponds to mapping point (x,y) from variety $xy=0$ to point $z=x+y$.)

We claim that this makes $\mathbb{C}[x,y]/(xy)$ a flat $\mathbb{C}[z]$-algebra. To prove this, note that since flatness is a local property, it suffices to show that

$$M=(\mathbb{C}[x,y]/(xy))_{(z-a)}\text{ is a flat }\mathbb{C}[z]_{(x-a)}\text{-algebra is flat for all }a\in\mathbb{C}.$$

(Be careful, M only allows denominator of the form $x+y-b$ for all $b\neq a$.)

To check this, we use ideal-theoretic criterion. The good news is $R=\mathbb{C}[z]_{(z-a)}$ has not many ideals: $(z-a)^n$! Then, it suffices to show that $\mathrm{Tor}_1^R(M,R/(z-a)^n)=0$. To do this, we consider the free resolution

$$R\xrightarrow{\cdot(z-a)^n}R$$

Tensor with M:

$$M\xrightarrow{\cdot(x+y-a)^n}M$$

Since $x+y-b$ is not a zero divisor in $\mathbb{C}[x,y]/(xy)$ for all $b\in\mathbb{C}$, it follows that this map is injective, so we are done.

§10.2.3 Flatness over Local Rings

In the case of local rings, we can say a lot more about flatness.

Theorem 10.2.7 (Flat Modules over Local Rings are Free).

Let R be a local ring with maximal ideal $\mathfrak{m}$, and let M be a finitely-presented R-module. The following are equivalent:

(a) M is free.

(b) M is flat.

(c) $\operatorname{Tor}_1^R(R/\mathfrak{m}, M) = 0$.

▶ *Proof.* Note (a) ⇒ (b) is trivial, and (b) ⇒ (c) was proved in Theorem 10.2.4. Thus, we prove that (c) implies (a).

Suppose $\operatorname{Tor}_1^R(R/\mathfrak{m}, M) = 0$. Observe that $M/\mathfrak{m}M$ is a module over the field $R/\mathfrak{m}$, so it is free. As it is also finitely generated, we can find $m_1, m_2, \ldots, m_n \in M$ such that their images $\overline{m_1}, \ldots, \overline{m_n}$ in $M/\mathfrak{m}M$ form a basis. By Nakayama (Corollary 2.2.6), $m_1, \ldots, m_n$ generate M.

Now define a free R-module F with basis $\{f_1, \ldots, f_n\}$, and consider the surjective map $\beta : F \to M$ which maps $f_i \mapsto m_i$ for all i. Let $K = \operatorname{Ker}\beta$, with the embedding $\alpha : K \to F$. We have a short exact sequence

$$0 \longrightarrow K \xrightarrow{\alpha} F \xrightarrow{\beta} M \longrightarrow 0.$$

Note that for any module N, $N \otimes R/\mathfrak{m} = N/\mathfrak{m}N$. Thus, by tensoring the sequence with $R/\mathfrak{m}$, we have an exact sequence

$$0 = \operatorname{Tor}_1^R(M, R/\mathfrak{m}) \longrightarrow K/\mathfrak{m}K \xrightarrow{\alpha_*} F/\mathfrak{m}F \xrightarrow{\beta_*} M/\mathfrak{m}M \longrightarrow 0.$$

Let $\overline{f_i}$ denote the image of f_i in $F/\mathfrak{m}F$. Then, β_* maps $\overline{f_i} \mapsto \overline{m_i}$, so it maps the basis $\{\overline{f_1}, \ldots, \overline{f_n}\}$ of $F/\mathfrak{m}F$ to the basis $\{\overline{m_1}, \ldots, \overline{m_n}\}$ of $M/\mathfrak{m}M$. Hence, β_* is an isomorphism. By the exactness of the sequence above, α_* is injective and has image 0, so $K/\mathfrak{m}K = 0$. Since M is finitely presented, K is finitely generated (we won't prove this fact, sorry), so by Nakayama, $K = 0$. It follows that $M \simeq F$ is free. ☐

Corollary 10.2.8 (Equivalence of Flat and Locally Free).

Let R be a ring and M be a finitely-presented R-module. Then, M is flat if and only if M is locally free (i.e., for every prime ideal $\mathfrak{p}$, $M_\mathfrak{p}$ is free).

▶ *Proof.* If M is flat, then for all prime $\mathfrak{p}$, $M_\mathfrak{p}$ is a flat $R_\mathfrak{p}$-module and hence free.

If $M_\mathfrak{p}$ is free for all prime $\mathfrak{p}$, then $M_\mathfrak{m}$ is free and hence flat for all maximal $\mathfrak{m}$. By Proposition 3.3.4, M is flat. ☐

§10.2.4 (Bonus) Local Criteria of Flatness

The above result is nice, but it assumes that M is finitely-presented. Most morphisms of variety is not finite. Therefore, we give a more powerful condition that allows us to work on non-finitely-generated ring as well.

Theorem 10.2.9 (Local criteria of flatness).

Let R and S be Noetherian local rings. Let $\mathfrak{m}$ and $\mathfrak{n}$ be maximal ideals of R and S, respectively. Let $\phi : R \to S$ be a **local morphism**, i.e., $\phi^{-1}\mathfrak{n} = \mathfrak{m}$.

Let M be a finitely-generated S-module. If $\operatorname{Tor}_1^R(M, R/\mathfrak{m}) = 0$, then M is flat over R.

▶ *Proof.* It suffices to show that $\operatorname{Tor}_1^R(M, R/I) = 0$ for all ideals $I \subset R$. If this is not true, take I to be the maximal among all counterexamples (we can do this since R is Noetherian). Pick $f \in \mathfrak{m} \setminus I$. We have two cases.

- **If f is not a zero divisor in R/I**, then we get a short exact sequence

  $$0 \longrightarrow R/I \xrightarrow{f} R/I \longrightarrow R/((f)+I) \longrightarrow 0.$$

  The ideal $(f)+I$ strictly contains I, so by maximality, we have $\operatorname{Tor}_1^R(M, R/((f)+I)) = 0$. Therefore, we get a surjective map

  $$\operatorname{Tor}_1^R(M, R/I) \xrightarrow{\cdot f} \operatorname{Tor}_1^R(M, R/I).$$

  To avoid clutter, let $N = \operatorname{Tor}_1^R(M, R/I)$, which has the structure of S-module because $M \otimes \bullet$ has the structure of S-module, and from above, we get a surjective map $N \to N$ by multiplication by $\phi(f)$. Then, $N = (\phi(f))N$, so by Nakayama's lemma, there exists $x \in (\phi(f))$ such that $n = x\phi(f)n$ for all $n \in N$. However, from $\phi^{-1}\mathfrak{n} = \mathfrak{m}$, we get that $\phi(f) \in \mathfrak{n}$. Thus, $(1 - x\phi(f))$ is a unit, so $n = 0$ for all $n \in N$, so $N = 0$. Thus, $\operatorname{Tor}_1^R(M, R/I) = 0$.

- **If f is a zero divisor in R/I,** then let $J = \operatorname{Ann}_{R/I}(f)$, so J strictly contains I. Then, we have an exact sequence

  $$0 \longrightarrow R/J \longrightarrow R/I \longrightarrow R/((f)+I) \longrightarrow 0.$$

  Again, by maximality assumption, $\operatorname{Tor}_1^R(M, R/J) = 0$ and $\operatorname{Tor}_1^R(M, R/((f)+I)) = 0$. which implies by long exact sequence that $\operatorname{Tor}_1^R(M, R/I) = 0$. This is a contradiction. ☐

§10.3 Going-Down Theorem, Flat Version

In Theorem 4.3.11, we proved a version of going down for integral extensions of integrally-closed domains. In this section, we will prove another version of the statement which instead assumes flatness.

Theorem 10.3.1 (Going-Down Theorem, Flat Version)**.**

Given a morphism $\phi : A \to B$, we say that prime ideal $\mathfrak{q} \subset B$ **lies over** $\mathfrak{p} \subset A$ if $\phi^{-1}\mathfrak{q} = \mathfrak{p}$.

Suppose that $\phi : A \to B$ is a flat morphism. Given that $\mathfrak{p} \subset \mathfrak{p}' \subset A$ be prime ideals and $\mathfrak{q}'$ lies over $\mathfrak{p}'$, then there exists a prime ideal $\mathfrak{q} \subset \mathfrak{q}'$ lying over $\mathfrak{p}$.

$$\begin{tikzcd}
\mathfrak{q} \arrow[d, dash, dashed] & \subset & \mathfrak{q}' \arrow[d, dash] & \subset & B \arrow[d, dash] \\
\mathfrak{p} & \subset & \mathfrak{p}' & \subset & A
\end{tikzcd}$$

Before we prove this, we will need a new definition.

§10.3.1 Faithful Flatness

One way of stating the definition of flatness is as follows: a module M is flat if $A \to B \to C$ being exact implies $A \otimes M \to B \otimes M \to C \otimes M$ is exact.

Definition 10.3.2.

A module M is **faithfully flat** if the following is true: $A \to B \to C$ is exact **if and only if** $A \otimes M \to B \otimes M \to C \otimes M$ is exact.

Similarly, a morphism of rings $\varphi : A \to B$ is **faithfully flat** if it makes B a faithfully flat A-algebra.

Example 10.3.3.

Finitely-generated free modules are faithfully flat, as $A \otimes_R R^{\oplus n} \cong A^{\oplus n}$. (In fact, all free modules are faithfully flat.)

An example of a flat module which is not faithfully flat is $\mathbb{Q}$ as a $\mathbb{Z}$-module. Indeed, by Corollary 3.2.4, $\mathbb{Q} = (\mathbb{Z} \setminus \{0\})^{-1}\mathbb{Z}$ is flat. Further note $(\mathbb{Z}/n\mathbb{Z}) \otimes \mathbb{Q} = 0$, as $m \otimes q = (nm) \otimes (q/n) = 0$ for all m and q. Thus, while

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\cdot 1} \mathbb{Z}/n\mathbb{Z} \xrightarrow{\cdot 1} \mathbb{Z}/n\mathbb{Z}$$

is not exact, its tensor with $\mathbb{Q}$ is $0 \to 0 \to 0$, which is exact.

Definition 10.3.4.

Let R be a ring and $\mathfrak{p} \subseteq R$ be a prime ideal. The **residue field** is defined as

$$\kappa(\mathfrak{p}) := \operatorname{Frac}(R/\mathfrak{p}).$$

Theorem 10.3.5.

Let M be a flat R-module. The following are equivalent;

(a) M is faithfully flat.

(b) If $N \otimes_R M = 0$, then $N = 0$.

(c) For all prime ideals $\mathfrak{p} \subseteq R$, $\kappa(\mathfrak{p}) \otimes_R M \neq 0$.

(d) For all maximal ideals $\mathfrak{m} \subseteq R$, $\kappa(\mathfrak{m}) \otimes_R M \neq 0$.

▶ *Proof.* It is clear that (b) $\Rightarrow$ (c) $\Rightarrow$ (d).

(a) $\Rightarrow$ (b). Suppose M is faithfully flat. If $M \otimes N = 0$, then $0 \to M \otimes_R 0 \to M \otimes_R N \to M \otimes_R 0 \to 0$ is exact, so $0 \to 0 \to N \to 0 \to 0$ is exact. Thus, $N = 0$.

(b) $\Rightarrow$ (a). Suppose $N \otimes_R M = 0$ only when $N = 0$, and suppose for modules A, B, and C, the tensored sequence

$$A \otimes_R M \xrightarrow{\alpha_*} B \otimes_R M \xrightarrow{\beta_*} C \otimes_R M$$

is exact. Then, $\operatorname{Im}(\beta\alpha) \otimes_R M = \operatorname{Im}(\beta_*\alpha_*) = 0$, so $\operatorname{Im}(\beta\alpha) = 0$, i.e., $\operatorname{Im}\alpha \subseteq \operatorname{Ker}\beta$. By flatness,

$$\frac{\operatorname{Ker}\beta}{\operatorname{Im}\alpha} \otimes_R M = \frac{\operatorname{Ker}\beta \otimes_R M}{\operatorname{Ker}\alpha \otimes_R M} = \frac{\operatorname{Ker}\beta_*}{\operatorname{Im}\alpha_*} = 0,$$

so $\operatorname{Ker}\beta / \operatorname{Im}\alpha = 0$, i.e., $A \to B \to C$ is exact. Thus, M is faithfully flat.

(d) $\Rightarrow$ (b). Suppose $M \otimes_R \kappa(\mathfrak{m}) \neq 0$ for all maximal $\mathfrak{m}$. Consider any nonzero module N. Let $x \in N$ be a nonzero element. Observe $R/\operatorname{Ann}(x)$ embeds into N under the map, so $(R/\operatorname{Ann}(x)) \otimes_R M$ embeds into $N \otimes_R M$.

Let $\mathfrak{m}$ be any maximal ideal containing $\operatorname{Ann}(x)$. Then, $(R/\operatorname{Ann}(x)) \otimes_R M$ surjects onto $(R/\mathfrak{m}) \otimes_R M$. The latter is nonzero by assumption, so the former is also nonzero. It embeds into $N \otimes_R M$, so $N \otimes_R M \neq 0$, as desired. ☐

The module $M \otimes_R \kappa(\mathfrak{p})$ has a geometric significance: it is a **fiber**. To see this, we first note that since localization commutes with quotient, we get $\kappa(\mathfrak{p}) \simeq R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$, so we have the exact sequence

$$\mathfrak{p}R_\mathfrak{p} \longrightarrow R_\mathfrak{p} \longrightarrow \kappa(\mathfrak{p}) \longrightarrow 0,$$

so tensoring gives

$$\mathfrak{p}M_\mathfrak{p} \longrightarrow M_\mathfrak{p} \longrightarrow \kappa(\mathfrak{p}) \otimes_R M \longrightarrow 0,$$

which implies that

$$\kappa(\mathfrak{p}) \otimes_R M \simeq M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p}. \tag{10.1}$$

Now, suppose that $M = S$ is an R-algebra. Then, $\kappa(\mathfrak{p}) \otimes_R S \simeq S_\mathfrak{p}/\mathfrak{p}S_\mathfrak{p}$ as R-algebra as well. We claim the following:

Proposition 10.3.6.

If $\phi : R \to S$ be a morphism (so S is an R-algebra), then there is a bijective correspondence between

$$\{\text{prime ideals of } \kappa(\mathfrak{p}) \otimes_R S\} \longleftrightarrow \{\text{prime ideals } \mathfrak{q} \subset S \text{ such that } \phi^{-1}\mathfrak{q} = \mathfrak{p}\}.$$

▶ *Proof.* Recall (10.1) that $\kappa(\mathfrak{p}) \otimes_R S = S_\mathfrak{p}/\mathfrak{p}S_\mathfrak{p}$. First, note that $S_\mathfrak{p}$ is a localization of S with multiplicative set $\phi(R/\mathfrak{p})$. Thus, every prime ideal of $S_\mathfrak{p}$ (and hence $S_\mathfrak{p}/\mathfrak{p}S_\mathfrak{p}$) is extended from a prime ideal $\mathfrak{q} \in S$. Observe the following:

- In order to get a prime ideal in $S_\mathfrak{p}$, we must have $\mathfrak{q} \cap \phi(R \setminus \mathfrak{p}) = \emptyset$, This is equivalent to $\phi^{-1}\mathfrak{q} \subseteq \mathfrak{p}$ (which we left as an easy exercise to check).
- In order to get a prime ideal in $S_\mathfrak{p}/\mathfrak{p}S_\mathfrak{p}$, we must have $\mathfrak{q}R_\mathfrak{p} \supseteq \phi(\mathfrak{p})R_\mathfrak{p}$, which means $\mathfrak{q} \supseteq \phi(\mathfrak{p})$ or equivalently $\phi^{-1}\mathfrak{q} \supseteq \mathfrak{p}$.

Combining both items gives $\mathfrak{q}$ extends to a prime ideal in $S_\mathfrak{p}/\mathfrak{p}S_\mathfrak{p}$ if and only if $\phi^{-1}\mathfrak{q} = \mathfrak{p}$. ☐

In particular, $\operatorname{Spec}(\kappa(\mathfrak{p}) \otimes_R S) \simeq \phi^{-1}(\{\mathfrak{p}\})$. This is why $\kappa(\mathfrak{p}) \otimes_R S$ is an algebraic realization of the fiber of $\phi^\# : \operatorname{Spec} S \to \operatorname{Spec} R$ at $\mathfrak{p}$.

§10.3.2 Proof of Going Down

Corollary 10.3.7.

If $\varphi : A \to B$ is faithfully flat (i.e., makes B a faithfully flat A-module), then $\varphi^\# : \operatorname{Spec} B \to \operatorname{Spec} A$ is surjective.

▶ *Proof.* Let $\mathfrak{p}$ be any prime ideal of A. From Theorem 10.3.5, $\kappa(\mathfrak{p}) \otimes_A B \neq 0$, so there exists at least one prime ideal, which by Proposition 10.3.6 must then correspond to prime ideal in $\operatorname{Spec} B$ that contracts to $\mathfrak{p}$. ☐

Corollary 10.3.8.

If $\varphi : A \to B$ is flat and $\mathfrak{q} \in \operatorname{Spec} B$ lies over $\mathfrak{p} \in \operatorname{Spec} A$, then $B_\mathfrak{q}$ is faithfully flat over $A_\mathfrak{p}$.

▶ *Proof.* First, we show flatness. Let $B_\mathfrak{p} = (A \setminus \mathfrak{p})^{-1}B$ be an $A_\mathfrak{p}$-module (warning: it is not an algebra). Then, by Corollary 3.2.4, we get that $B_\mathfrak{p}$ is a flat $A_\mathfrak{p}$-module. Localizing $B_\mathfrak{p}$ further gives that $B_\mathfrak{q}$ is a flat $B_\mathfrak{p}$-module, hence a flat $A_\mathfrak{p}$-module by forgetting scalar.

Now, we show faithful flatness. Since $A_\mathfrak{p}$ is local with maximal ideal $\mathfrak{p}A_\mathfrak{p}$, which $\mathfrak{q}B_\mathfrak{q} \subseteq B_\mathfrak{q}$ lies over, $\mathfrak{p}A_\mathfrak{p}$ is in the image of $\varphi^\# : \operatorname{Spec} B_\mathfrak{q} \to \operatorname{Spec} A_\mathfrak{p}$. Thus, $B_\mathfrak{q}$ is faithfully flat over $A_\mathfrak{p}$. ☐

▶ *Proof of Going Down Theorem 10.3.1.* Suppose B is a flat A-module, and define $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{q}'$ as in the statement. By Corollary 10.3.8, $B_{\mathfrak{q}'}$ is faithfully flat over $A_{\mathfrak{p}'}$. By Corollary 10.3.7, some prime in $B_{\mathfrak{q}'}$ lies over $\mathfrak{p}A_{\mathfrak{p}'}$. Lifting this prime back to B, we get a prime that lies over $\mathfrak{p}$. ☐

§10.4 Flatness Implies Constant-Dimension Fibers

Theorem 10.4.1.

If R and S are Noetherian local rings with maximal ideals $\mathfrak{m}$ and $\mathfrak{n}$ and $\varphi : R \to S$ is a ring morphism such that $\varphi^{-1}\mathfrak{n} = \mathfrak{m}$. Then,

$$\dim S \leq \dim R + \dim S/\mathfrak{m}S.$$

Moreover, if φ is flat, then the equality holds.

Before proving this theorem, let us consider geometric interpretation. Let $\varphi : A \to B$ be a flat morphism, $\mathfrak{q}$ be a prime ideal of B, and $\mathfrak{p} = \varphi^{-1}A$. Then, φ induces a local morphism $\varphi_* : A_{\mathfrak{p}} \to B_{\mathfrak{q}}$. Then, we have

$$\dim B_{\mathfrak{q}} \leq \dim A_{\mathfrak{p}} + \dim B_{\mathfrak{q}}/\mathfrak{p}B_{\mathfrak{q}}. \tag{10.2}$$

Note that by localization in stages,

$$B_{\mathfrak{q}}/\mathfrak{p}B_{\mathfrak{q}} = (B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}})_{\mathfrak{q}} \overset{(10.1)}{=} (B \otimes_A \kappa(\mathfrak{p}))_{\mathfrak{q}}$$

(where $B_{\mathfrak{p}} = (\phi(A \setminus \mathfrak{p}))^{-1}B$). The A-algebra $B \otimes_A \kappa(\mathfrak{p})$ is the **fiber** of the morphism $\varphi^{\#} : \operatorname{Spec} B \to \operatorname{Spec} A$ at $\mathfrak{p}$ (i.e., $\operatorname{Spec}(B \otimes_A \kappa(\mathfrak{p})) = (\varphi^{\#})^{-1}(\{\mathfrak{p}\})$). This theorem says that for flat morphisms, the local dimension of fiber at $\mathfrak{q}$ is the difference of the local dimension of B at $\mathfrak{q}$ and of A at $\mathfrak{p}$.

Example 10.4.2.

Consider the morphism

$$\phi : k[x] \to \frac{k[x,y]}{(xy)}$$

mentioned in the introduction. Let $A = k[x]$, $B = k[x,y]/(xy)$, $\mathfrak{q} = (x,y) \subseteq B$, so $\mathfrak{p} = \phi^{-1}\mathfrak{q} = (x) \subseteq A$. Then, using the fact that localization commutes with quotient, we compute

$$\frac{B_{\mathfrak{q}}}{\mathfrak{p}B_{\mathfrak{q}}} = \frac{B_{(x,y)}}{(x)B_{(x,y)}} = \left(\frac{B}{(x)}\right)_{(x,y)} = k[y]_{(y)},$$

which has dimension 1. This correspond to the geometric intuition that inverse image of $\{0\}$ is the y-axis.

On the other hand, $\dim A_{\mathfrak{p}} = \dim B_{\mathfrak{q}} = 1$ by Proposition 9.4.3. This violates (10.2).

▶ *Proof of Theorem 10.4.1.* Let $d = \dim R$ and $e = \dim S/\mathfrak{m}S$. From primary ideal dimension, there exists an $\mathfrak{m}$-primary ideal $(x_1, \ldots, x_n) \subseteq R$, i.e., there exists n_1 for which $\mathfrak{m}^{n_1} \subseteq (x_1, \ldots, x_n) \subseteq \mathfrak{m}$ (this utilizes R is Noetherian). Similarly, there exists n_2 and an $\mathfrak{n}/\mathfrak{m}S$-primary ideal $(y_1, \ldots, y_e) \subseteq \mathfrak{n}$ containing $\mathfrak{m}S$ such that

$$\left(\frac{\mathfrak{n}}{\mathfrak{m}S}\right)^{n_2} \subseteq \frac{(y_1, \ldots, y_e)}{\mathfrak{m}S} \subseteq \frac{\mathfrak{n}}{\mathfrak{m}S}.$$

Since $S/\mathfrak{m}S$ is local with maximal ideal $\mathfrak{n}/\mathfrak{m}S$, we know $\mathfrak{n}^{n_2} \subseteq (y_1, \ldots, y_e) + \mathfrak{m}S$. Thus,

$$\begin{aligned} \mathfrak{n}^{n_1 n_2} &\subseteq ((y_1, \ldots, y_e) + \mathfrak{m}S)^{n_1} \\ &\subseteq (y_1, \ldots, y_e) + (x_1, \ldots, x_d)S \\ &= (y_1, \ldots, y_e, \varphi(x_1), \ldots, \varphi(x_d)) \\ &\subseteq \mathfrak{n}, \end{aligned}$$

so there exists an $\mathfrak{n}$-primary ideal with $d + e$ generators. We conclude $\dim S \leq d + e$, the desired inequality.

Now suppose φ is flat. Given a chain of prime ideals

$$\begin{gathered}\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d = \mathfrak{m} \ \subseteq \ R \\ \frac{\mathfrak{q}_0}{\mathfrak{m}S} \subsetneq \frac{\mathfrak{q}_1}{\mathfrak{m}S} \subsetneq \cdots \subsetneq \frac{\mathfrak{q}_e}{\mathfrak{m}S} \ \subseteq \ \frac{S}{\mathfrak{m}S}\end{gathered}$$

(where $\mathfrak{q}_0 \supseteq \mathfrak{m}S$), one construct a chain of prime ideals in S as follows. Note that $\mathfrak{m} \supseteq \varphi^{-1}\mathfrak{q}_0 \supseteq \varphi^{-1}\mathfrak{m}S \supseteq \mathfrak{m}$, so $\varphi^{-1}\mathfrak{q}_0 = \mathfrak{m}$, so $\mathfrak{q}_0$ lies above $\mathfrak{p}_d = \mathfrak{m}$, so by going down theorem Theorem 10.3.1, there exists prime ideals $\overline{\mathfrak{p}}_i$ such that $\varphi^{-1}\overline{\mathfrak{p}}_i = \mathfrak{p}_i$. The whole construction can be summarized in the diagram below.

$$\begin{tikzcd}
S/\mathfrak{m}S: & & & & & & & & & \frac{\mathfrak{q}_0}{\mathfrak{m}S} \arrow[d, dash] & \subsetneq & \frac{\mathfrak{q}_1}{\mathfrak{m}S} \arrow[d, dash] & \subsetneq & \cdots & \subsetneq & \frac{\mathfrak{q}_e}{\mathfrak{m}S} \arrow[d, dash] \\
S: & \overline{\mathfrak{p}}_0 \arrow[d, dash, dashed] & \subsetneq & \overline{\mathfrak{p}}_1 \arrow[d, dash, dashed] & \subsetneq & \cdots & \subsetneq & \overline{\mathfrak{p}}_{d-1} \arrow[d, dash, dashed] & \subsetneq & \mathfrak{q}_0 \arrow[d, dash] & \subsetneq & \mathfrak{q}_1 & \subsetneq & \cdots & \subsetneq & \mathfrak{q}_e \\
R: & \mathfrak{p}_0 & \subsetneq & \mathfrak{p}_1 & \subsetneq & \cdots & \subsetneq & \mathfrak{p}_{d-1} & \subsetneq & \mathfrak{p}_d = \mathfrak{m} & & & & & &
\end{tikzcd}$$

Now, our chain of prime ideal is $\overline{\mathfrak{p}}_0 \subsetneq \overline{\mathfrak{p}}_1 \subsetneq \cdots \subsetneq \overline{\mathfrak{p}}_{d-1} \subsetneq \mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_e$. ☐

As an application, we now give the deferred proof of Proposition 9.4.9.

Corollary 10.4.3.

Let R be a Noetherian ring. Then, $\dim R[x] = \dim R + 1$.

▶ *Proof.* First, we note that the morphism $R \to R[x]$ is flat because $R[x]$ is a free R-module. Let $\mathfrak{q}$ be a prime ideal of $R[x]$, and let $\mathfrak{p}$ be its contraction to R. By the previous corollary, we get that

$$\dim R[x]_{\mathfrak{q}} = \dim R_{\mathfrak{p}} + \dim(R[x]_{\mathfrak{q}}/\mathfrak{p}R[x]_{\mathfrak{q}}).$$

However, we note that since localization commutes with everything,

$$R[x]_{\mathfrak{q}}/\mathfrak{p}R[x]_{\mathfrak{q}} = (R[x]/\mathfrak{p}R[x])_{\mathfrak{q}} = ((R/\mathfrak{p})[x])_{\mathfrak{q}} = \kappa(\mathfrak{p})[x]_{\mathfrak{q}},$$

which has dimension 1. Therefore,

$$\dim R[x]_{\mathfrak{q}} = \dim R_{\mathfrak{p}} + 1$$

for all prime ideal $\mathfrak{q}$. Taking maximum across all prime ideal $\mathfrak{q}$ (noting that $\operatorname{Spec} R[x] \to \operatorname{Spec} R$ is surjective because $\mathfrak{p}[x]$ maps to $\mathfrak{p}$), we get that $\dim R[x] = \dim R + 1$. ☐

§10.5 Problems

Problem 10.A. Let M be a module over ring $k[t]/(t^2)$. Prove that M is flat if and only if the multiplication by t map $M/tM \to tM$ is an isomorphism.

Problem 10.B. Let $R = \mathbb{C}[x,y]/(xy)$. Compute $\operatorname{Tor}_n^R(R/(x), R/(x))$. Your answer should depend on whether $n = 0$, n is odd, or n is even and positive.

Problem 10.C. Let R be a regular local ring of dimension n with maximal ideal $\mathfrak{m}$ and residue field k. Recall [TODO: cross-reference the Cohen-Macaulay problem] that there exists a sequence $x_1, x_2, \ldots, x_n \in \mathfrak{m}$ such that $\mathfrak{m} = (x_1, \ldots, x_n)$ and x_i is not a zero-divisor of $R/(x_1, \ldots, x_{i-1})$.

(a) Prove that for any R-module M, we have $\operatorname{Tor}_i^R(M,k)=0$ for all $i>n$.

(Hint: There are at least two ways to do this. One is to use $0 \to R/(x_1,\dots,x_i) \to R/(x_1,\dots,x_i) \to R/(x_1,\dots,x_{i+1}) \to 0$. The other is to explicitly find a free resolution of k)

(b) Prove that any R-module M has a free resolution $F_n \to \cdots \to F_1 \to F_0$ of length at most n.[1]

(Hint: start with any free resolution $\cdots \to F_1 \to F_0$. Truncate it to a resolution $K \to F_{n-1} \to \cdots \to F_1 \to F_0$ where $K = \operatorname{Im}(F_n \to F_{n-1})$ and use Theorem 10.2.7 to show that K is free.)

(c) For each n, given an example showing that the bound n in (b) cannot be improved.

---

[1] The following converse holds: if R is Noetherian local ring such that the residue field k has a finite free resolution, then R is regular. See [Eis95, Theorem 19.12] for the proof.

A Background

This appendix provides some background material. Appendix A.1 and Appendix A.2 introduces basic category theory (readers interested in learning further are encouraged to consulte [Lei14]). Appendix A.3 gives a quick review of topological spaces and topological notions.

§A.1 Category and Functors

Any mathematical structure you will care about forms a category.

Definition A.1.1.

A **category** $\mathcal{C}$ consists of:

- a set of **objects** $\operatorname{obj}\mathcal{C}$;
- for any $A, B \in \operatorname{obj}\mathcal{C}$, the set of **morphisms** $\operatorname{Mor}(A, B)$; and
- for any $A, B, C \in \operatorname{obj}\mathcal{C}$, the composition operation $\circ$ which takes morphisms, one in $\operatorname{Mor}(A, B)$ and one in $\operatorname{Mor}(B, C)$ to get a morphism $\operatorname{Mor}(A, C)$

satisfying the following conditions (which are mild)

- **associativity.** $f \circ (g \circ h) = (f \circ g) \circ h$ for any compatible morphisms f, g, h.
- **identity.** for any $A \in \operatorname{obj}(\mathcal{C})$, there exists identity morphism $1_A \in \operatorname{Mor}(A, A)$ such that $1_A \circ f = f \circ 1_B = f$ for all $f \in \operatorname{Mor}(A, B)$.

Example A.1.2.

Commutative rings form a category **Rings** with objects being rings and morphisms being ring homomorphisms.

Similarly, the category R-**Mod** of R-modules has objects being R-modules and morphisms being R-module homomorphisms. A special case of this is vector spaces (when $R = k$ is a field) and abelian groups (when $R = \mathbb{Z}$).

We can also study maps between two categories, called the **functor**.

Definition A.1.3.

A **covariant functor** from $\mathcal{C} \to \mathcal{D}$ consists of two maps: $F^{\text{obj}} : \operatorname{obj}\mathcal{C} \to \operatorname{obj}\mathcal{D}$ and $F^{\text{Mor}} : \operatorname{Mor}(A, B) \to \operatorname{Mor}(F(A), F(B))$ satisfying the following conditions:

- **preserves composition.** $F(f \circ g) = F(f) \circ F(g)$.
- **perserves identity.** $F(1_A) = 1_{F(A)}$ for all $A \in \operatorname{obj}\mathcal{C}$

(In contrast, a **contravariant functor** from $\mathcal{C} \to \mathcal{D}$ two maps: $F^{\text{obj}} : \operatorname{obj}\mathcal{C} \to \operatorname{obj}\mathcal{D}$ and $F^{\text{Mor}} : \operatorname{Mor}(A, B) \to \mathbf{Mor}(\boldsymbol{F}(\boldsymbol{B}), \boldsymbol{F}(\boldsymbol{A}))$ satisfying similar axioms. The difference is that it reverses the direction of morphisms.)

Example A.1.4.

We have the following examples of functors.

- There is a functor from commutative rings to abelian groups that maps a ring A to a unit group $A^\times$. The morphism mapping is given by $(A \overset{\phi}{\to} B) \mapsto (A^\times \overset{\phi}{\to} B^\times)$ by just restriction.
- There is a functor from commutative rings to commutative rings by $A \mapsto A[x]$.

§A.2 Universal Properties

Universal properties (also known as **universal mapping properties** or **mapping properties**) determine an object up to isomorphism. They are of a very specific format, which is best seen through examples.

▶ **Product** Let $\mathcal{C}$ be a category with objects M and N. Then, the product $M \times N$ is an object P, equipped with morphisms $\mu : P \to M$ and $\nu : P \to N$, such that the following universal property holds: "for any object P' and maps $\mu' : P' \to M$ and $\nu' : P' \to N$

$$\begin{tikzcd}
P' \arrow[rrd, "\mu'"] \arrow[rd, dashed] \arrow[rdd, "\nu'"'] & & \\
& P \arrow[r, "\mu"'] \arrow[d, "\nu"] & M \\
& N &
\end{tikzcd},$$

there exists unique morphism $\phi : P' \to P$ (in dashed arrow) that makes the diagram above commute."

(We say that a diagram of objects and morphisms **commutes** if for any objects P and Q in the diagram, every directed path from P to Q compose to the same map $P \to Q$.)

Let's suppose that $\mathcal{C}$ is the category **Sets** (objects are sets, and morphisms are any function between two sets). Given sets M and N, why does the definition above agree with the usual product

$$P = \{(m, n) : m \in M, n \in N\}?$$

First, the morphisms μ and ν are defined by $\mu((m, n)) = m$ and $\nu((m, n)) = n$. Now, let us verify that the above property holds. Suppose that there exists P', μ', and ν' as above. Then, $\phi : P' \to P$ is uniquely determined to be $\phi(p) = (\mu'(p), \nu'(p))$. Thus, P satisfy the above universal property.

Now, we claim that **any two products satisfying the universal property above are isomorphic**. To prove this, suppose that we have two products P_1 and P_2:

$$\begin{tikzcd}
P_1 \arrow[r, "\mu_1"'] \arrow[d, "\nu_1"] & M & & P_2 \arrow[r, "\mu_2"'] \arrow[d, "\nu_2"] & M \\
N & & \text{and} & N &
\end{tikzcd}.$$

Then, by letting P_2 play the role of P and P_1 play the role of P' gives a morphism $\phi_1 : P_1 \to P_2$ making the following diagram commute.

$$\begin{tikzcd}
P_2 \arrow[rd, bend left, "\phi_2"] \arrow[rrd, bend left, "\mu_2"] \arrow[rdd, bend right, "\nu_2"'] & & \\
& P_1 \arrow[lu, bend left, "\phi_1"] \arrow[r, "\mu_1"'] \arrow[d, "\nu_1"] & M \, . \\
& N &
\end{tikzcd}$$

Similarly, there exists a morphism $\phi_2 : P_2 \to P_1$ that makes the diagram above commute.

Now, we plug in $P = P' = P_1$. Then, there exists a unique morphism $P_1 \to P_1$ that commutes with both μ_1 and ν_1. However, we can name two such morphisms: $\phi_2 \circ \phi_1$ and the identity map. Thus, $\phi_2 \circ \phi_1 = \mathrm{id}_{P_1}$. Similarly, $\phi_1 \circ \phi_2 = \mathrm{id}_{P_2}$, so P_1 and P_2 are isomorphic.

Notice how this argument does not use the nature of our category $\mathcal{C}$ at all. Thus, if one changes category $\mathcal{C}$ to other categories (e.g., **Rings** or R-**Mod**), then the exact same argument shows that any two products are isomorphic. What's left, however, is to show that product exists for each category that you want to define a product.

▶ Polynomial Rings Let R be a ring. Then, the polynomial ring $R[x]$ is the ring S with element $x \in S$ and morphism $\iota : R \to S$ satisfying the following universal property: "for ring S', element $y \in S'$, and any morphism $\phi : R \to S'$, there exists a unique morphism $f : S \to S'$ such that $f(x) = y$ and the diagram

$$\begin{tikzcd}
& R \arrow[ld, "\iota"'] \arrow[rd, "\phi"] & \\
S \arrow[rr, "f"] & & S' \\
\rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\
x \arrow[rr, mapsto] & & y
\end{tikzcd}$$

commutes".

✍ **Exercise A.2.1.** Using the same argument as products, verify that the universal property given above characterizes S up to isomorphism.

We now check that a ring S satisfying the above universal property exists. To do this, we give the usual construction: define

$$S = \{a_0 + a_1 x + \cdots + a_n x^n : a_0, a_1, \ldots, a_n \in R\},$$

and the addition / multiplication operations are the standard polynomial addition / multiplication. Then, for any S' and ϕ satisfying the above, one can see that the map $f : S \to S'$ is forced to be

$$f(a_0 + a_1 x + \cdots + a_n x^n) = \phi(a_0) + \phi(a_1) y + \cdots + \phi(a_n) y^n.$$

We leave the reader to check that this defines a valid morphism. To do this, one needs to check that it is compatible under polynomial addition (easy) and multiplication (harder, but still straightforward).

▶ Universal Property in General In general, the recipe for defining an object through universal properties is as follows.

1. Define the universal property.
2. Prove that this property characterizes an object up to an isomorphism (a routine process).
3. Give a construction of an object (possibly difficult).

In these notes, we will soon see examples (e.g., tensor product, Section 2.5) where Step 3. is nontrivial, and therefore, the construction of the object itself makes it very hard to prove properties. When such situation arises, we often forget about Step 3. and use universal properties to deduce properties about that object.

Remark A.2.2 (Towards Yoneda's lemma).

In fact, one can formalize a theorem which says that "any universal property determines an object up to isomorphism". The result is **Yoneda's lemma**, which require a little bit more category theory to state than we want to do here (see [Lei14, §4.2] for more details).

As a starting point towards Yoneda's lemma, let us rephrase the universal properties of product and polynomial rings a little bit.

- (P, μ, ν) is a product if for each P', there exists a bijective corresondence between
$$\{\text{morphisms } \phi : P' \to P\} \longleftrightarrow \{(\text{morphisms } \mu' : P' \to M \text{ and } \nu' : P' \to N)\}.$$
- (S, x) is a polynomial ring if for each S', there exists a bijective correspondence between
$$\{\text{morphisms } S \to S'\} \longleftrightarrow \{\text{morphisms } R \to S',\ \text{image of } x\}.$$

In the first case, the universal property is classifying morphisms from any object to P, while in the second case, the universal property is classifying morphisms from S to any object.

These represent two types of universal properties of X: properties classifying the set of morphisms **from** X and properties classifying the set of morphisms **to** X. Yoneda's lemma states that, provided with some other mild conditions, properties of these two types classify objects up to isomorphism.

§A.3 Topological Spaces

We give a quick review of topological spaces and topological notions used in commutative algebra.

Definition A.3.1.

A **topological space** $(X, \mathcal{T})$ consists of

- a set X of points.
- a set $\mathcal{T} \subseteq 2^X$ of **open sets**

that satisfy the following conditions:

- $\emptyset$ and X are both in $\mathcal{T}$.
- for an arbitrary (possibly infinite, even uncountable) collection $(U_i)_{i \in I}$ where $U_i \in \mathcal{T}$, we have $\bigcup_{i \in I} U_i \in \mathcal{T}$.
- for any $U_1, U_2 \in \mathcal{T}$, we have $U_1 \cap U_2 \in \mathcal{T}$.

A set is **closed** if and only if its complement is open.

Originally, these terms are constructed to model geometric spaces such as $\mathbb{R}^n$ or a torus (see [Mun00] for more details). However, in algebra, we often borrow words from topology to describe structure that may or may not have geometric meaning. The words necessary for commutative algebra are as follows.

Definition A.3.2.

Let $(X, \mathcal{T})$ be a topological space, and let $S \subseteq X$. Then, the **induced topology** on S is defined by the list of open sets

$$\mathcal{T}' = \{V \subseteq S : V = U \cap S \text{ for some open set } U \in \mathcal{T}\}.$$

Definition A.3.3 (Bases)**.**

Let $(X, \mathcal{T})$ be a topological space. A collection of open sets $\mathcal{B} \subseteq \mathcal{T}$ forms a **bases** if and only if any open set in $\mathcal{T}$ can be written as a union of sets in $\mathcal{B}$.

Definition A.3.4 (Connectedness and Quasicompactness)**.**

A topological space $(X, \mathcal{T})$ is said to be

- **connected** if $\emptyset$ and X are the only subsets that are both closed and open (equivalently, X cannot be partition into disjoint union of open sets $U_1 \sqcup U_2$).
- **quasicompact** if any open covering has a finite subcovering. In other words, for any collection $(U_i)_{i \in I}$ such that $\bigcup_{i \in I} U_i = X$, there exists a finite subset $J \subseteq I$ such that $\bigcup_{j \in J} U_j = X$.

Remark A.3.5.

In some other contexts, the definition of quasicompact given above is the definition of compact, but in some places, compact means quasicompact and Hausdorff. Thus, we use the word quasicompact to make clear that we do not need Hausdorff condition.

Exercise A.3.6. Prove that any closed subset (with its induced topology) of a quasicompact space is quasicompact.

B More About Free Resolutions

The goal of this appendix is to prove Theorem 10.2.3 (a), that $\operatorname{Tor}_i^R(M,N)$ does not depend on the choice of free resolution of N. To do this, we need to introduce a little more homological algebra.

§B.1 Chain Homotopy

First, we define morphism between two chain complexes.

Definition B.1.1 (Morphism between chain complexes)**.**

Let C_* and D_* be two chain complexes of R-modules. A **morphism** between two chain complexes $f : C_* \to D_*$ is the sequence of morphisms $\dots, f_0, f_1, \dots$ such that the following diagram commutes

$$\begin{tikzcd}
\dots \arrow[r] & C_1 \arrow[r, "\partial_1"] \arrow[d, "f_{-1}"] & C_0 \arrow[r, "\partial_0"] \arrow[d, "f_0"] & C_{-1} \arrow[r] \arrow[d, "f_1"] & \dots \\
\dots \arrow[r] & D_1 \arrow[r, "\partial_1"] & D_0 \arrow[r, "\partial_0"] & D_{-1} \arrow[r] & \dots
\end{tikzcd}$$

This promotes the set of chain complexes of R-modules to be a category $\operatorname{ch}(R\text{-}\mathbf{Mod})$.

For any morphism $f : C_* \to D_*$, you can check that f_n induces a map $H_n(f) : H_n(C_*) \to H_n(D_*)$. (This makes H_n a functor $H_n : \operatorname{ch}(R\text{-}\mathbf{Mod}) \to R\text{-}\mathbf{Mod}$.) For any two maps f, g, we are interested in the condition at which $H_n(f) = H_n(g)$. One sufficient condition is chain homotopy.

Definition B.1.2 (Chain homotopy)**.**

Let C_* and D_* be two chain complexes of R-modules. A **chain homotopy** between two morphisms $f, g : C_* \to D_*$ is a sequence of morphism $h_n : C_n \to D_{n+1}$ such that

$$\partial_{n+1} h_n - h_{n-1}\partial_n = g_n - f_n.$$

If there exists such h, then we say that f and g are **chain homotopic**.

Proposition B.1.3.

If h is a chain homotopy between $f, g : C_* \to D_*$, then $H_n(f) = H_n(g)$ (as homomorphisms from $H_n(C_*) \to H_n(D_*)$) for all n.

▶ *Proof.* Suppose that $z \in \operatorname{Ker}(\partial_n)$, i.e., $\partial_n(z) = 0$. We need to show that $f(z) - g(z) \in \operatorname{Im}(\partial_{n+1})$. To do this, we note that

$$g_n(z) - f_n(z) = \partial_{n+1}(h_n(z)) - h_{n-1}(\partial_n(z)) = \partial_{n+1}(h_n(z)) \in \operatorname{Im}\partial_{n+1} \qquad \square$$

§B.2 Fundamental Theorem of Homological Algebra

Theorem B.2.1 (Fundamental theorem of homological algebra)**.**

Let N and N' be two R-modules. Let N_* and N'_* be free resolutions of N and N'. Then, any morphism $\phi : N \to N'$ can be lifted to morphism between free resolutions $\widetilde{\phi} : N_* \to N'_*$. Furthermore, any two lifts are chain homotopic.

▶ *Proof.* We use the following properties labeled (♠) of free modules: if F is a free module, then for any surjective map $f : P \to Q$, it is possible to lift any map $\pi : F \to Q$ to $\widetilde{\pi} : F \to P$

$$\begin{tikzcd} & F \arrow[dl, dashed, "\exists\widetilde{\pi}"'] \arrow[d, "\psi"] \\ P \arrow[r, two heads, "f"'] & Q \end{tikzcd} .$$

(Aside: Modules with this property are called **projective modules**, and this is the only condition of N_i that we need to make this theorem works, so instead of free resolutions, you can use a more general projective resolutions.) To verify this property, simply send a generator $e_i \in F$ to any element in $f^{-1}(\{\psi(e_i)\})$.

Now, we prove the theorem.

Existence of a lift. First, we show existence by construction the map $\widetilde{\phi}_i : N_i \to N'_i$ by induction. In the base case, consider the following diagram

$$\begin{tikzcd} N_0 \arrow[r, two heads] \arrow[d, dashed] \arrow[dr] & N \arrow[d, "\phi"] \\ N'_0 \arrow[r, two heads] & N' \end{tikzcd}$$

Thus, we use (♠) to find the map $\widetilde{\phi}_0$ such that the diagram above commute.

Now, for the inductive step, suppose we have $\widetilde{\phi}_{i-1} : N_{i-1} \to N'_{i-1}$. Let $K_{i-1} = \operatorname{Ker}(N_{i-1} \to N_{i-2})$ and $K'_{i-1} = \operatorname{Ker}(N'_{i-1} \to N'_{i-2})$ Then, $\widetilde{\phi}_{i-1}$ induces the map $\widetilde{\phi}_{i-1} : K_{i-1} \to K'_{i-1}$. Then, we have the diagram

$$\begin{tikzcd} N_i \arrow[r, two heads] \arrow[d, dashed] \arrow[dr] & K_{i-1} \arrow[d, "\widetilde{\phi}_{i-1}"] \\ N'_i \arrow[r, two heads] & K'_{i-1} \end{tikzcd} ,$$

and again, we can use (♠) to find $\widetilde{\phi}_i : N_i \to N'_i$ so that the above diagram commutes.

Any two lifts are chain homotopic. We have to construct the chain homotopy. Consider two lifts $\psi, \pi : N_* \to N'_*$. Let $\ell = \psi - \pi$. We need h such that $\partial h - h\partial = \ell$. We, again, do this by induction. Ths base case is to find h_0 so that the following diagram commutes:

$$\begin{tikzcd} & & N_0 \arrow[r, two heads] \arrow[dll, dashed, "h_0"'] \arrow[dl, dashed] \arrow[d, "\ell_0"] & N \arrow[d, "0"] \\ N'_1 \arrow[r, two heads] & K'_1 \arrow[r, hook] & N'_0 \arrow[r, two heads] & N' \end{tikzcd}$$

This is done in two steps. First, note that the composition $N \to N'_0 \to N'$ is zero map, so that composition factors through K'_1. Therefore, we get $N_0 \to K'_1$. Then, use (♠) again to find $N_0 \to N'_1$. Since the term $h\partial$ vanishes, we get that the chain homotopy condition is verified at 0.

Now, the inductive step is similar. We have the diagram

$$\begin{tikzcd}
 & & N_i \arrow[dll, dashed, "h_i"'] \arrow[dl, dashed] \arrow[d, "\ell_i+h_{i-1}\partial_i"] \\
N'_{i+1} \arrow[r, two heads] & K'_{i+1} \arrow[r, hook] & N'_i
\end{tikzcd}$$

We have to construct h_i such that $\partial_{i+1}h_i - h_{i-1}\partial_i = \ell_i$. To do this, we first note that

$$\begin{aligned}
\partial_i\Big(\ell_i + h_{i-1}\partial_i\Big) &= \partial_i\ell_i + \partial_i h_{i-1}\partial_i \\
&= \ell_{i-1}\partial_i + \partial_i h_{i-1}\partial_i && (\ell \text{ commutes with boundary maps}) \\
&= (\ell_{i-1} + \partial_i h_{i-1})\partial_i \\
&= h_{i-2}\partial_{i-1}\partial_i && (\text{chain homotopy definition}) \\
&= 0,
\end{aligned}$$

so $\ell_i + h_{i-1}\partial_i$ factors through K'_{i+1}, getting the map $N_i \to K'_{i+1}$. Finally, use (♠) to lift it to h_i, giving the desired chain homotopy condition. ☐

§B.3 Proof that Tor does not Depend on Free Resolution

We now prove Theorem 10.2.3 (a).

Theorem B.3.1 (Tor does not depend on free resolution)**.**

The functor $\operatorname{Tor}_n^R(M, N)$ (defined in Definition 10.2.1) does not depend on the choice of N_*.

▶ *Proof.* Consider two free resolutions N_* and N'_* for N. Thus, by the fundamental theorem of homological algebra (Theorem B.2.1), the identity map $\mathrm{id} : N \to N$ lifts to $\phi : N_* \to N'_*$ and $\psi : N'_* \to N_*$. Then, $\phi \circ \psi : N_* \to N_*$ is a lift of id as well. However, the identity map is one such liftlift of id, so $\phi \circ \psi$ is chain homotopic to identity.

Tensoring with M, we get two maps $\phi_* : M \otimes N_* \to M \otimes N'_*$ and $\psi_* : M \otimes N'_* \to M \otimes N_*$. Since everything is an additive functor, the chain homotopic condition is preserved through tensoring with M. Thus, $\phi_* \circ \psi_*$ is chain homotopic to identity. Similarly, $\psi_* \circ \phi_*$ is chain homotopic to identity. Thus, by using Proposition B.1.3, $H_n(\phi_*)$ and $H_n(\psi_*)$ provide isomorphism between $H_n(M \otimes N_*) \simeq H_n(M \otimes N'_*)$. This implies that $\operatorname{Tor}_n^R(M, N)$ gives the same result for two resolutions N_* and N'_*. ☐

Index

I-adic completion, 102, 104
I-adic filtration, 104
I-filtration, 104
$\mathfrak{p}$-primary, 85
$m \otimes n$ (pure tensor), 31
n-th Tor functor, 133
n-th homology group, 132

additive functor, 23
algebra, 35
alternating pairing, 48
annihilator, 18
Artin-Rees lemma, 106
Artinian module, 69
Artinian ring, 69
ascending chain condition (ACC), 69
associated graded module, 111
associated graded ring, 111
associated prime, 81

base change, 36
bases, 149
bilinear, 30
blowup algebra, 107
blowup module, 107
bounded difference, 103

category, 145
Cayley-Hamilton Theorem, 19, 20
chain complex, 132
chain homotopic, 151
chain homotopy, 151
characteristic polynomial, 19
Chinese Remainder Theorem, 7
class group, 98
class number, 99
closed map, 59
closed points, 13
closed sets, 12, 148
codimension, 122
coherent sequences, 101
cokernel, 18
colimit, 26
commutative algebra, 1
commutes, 146
completion, 103
composition series, 115
connected, 149
contraction, 3
contravariant functor, 146
coprime, 7
coproduct, 18
correspondence theorem, 4
covariant functor, 145
cyclic module, 19

Dedekind Domain, 94
descending chain condition (DCC), 69
determinant, 49
dimension, 65, 91
direct limit, 26
direct product, 18
direct sum, 18
directed system, 25, 26, 28
discrete valuation, 91
discrete valuation ring (DVR), 91
distinguished open set, 14
domain, 5

elliptic curve group law, 100
elliptic curves, 99
eventually polynomial, 118
exact, 21, 24
exact sequence, 21
extension, 3
exterior power, 48

faithfully flat, 139
fiber, 140, 141
field, 5
filtered, 28
filtration, 103
finite algebra, 54
finite module, 19
finite-type algebra, 54
finitely-generated algebra, 54
finitely-generated module, 19
finitely-presented module, 19
first isomorphism theorem, 4
flat module, 35
flat morphisms, 131
formal series ring, 8
fractional ideal, 97
free module, 18

free resolution, 133
Frobenius morphism, 2
functor, 145

generic point, 13
genus, 99, 100
Going-down Theorem, 60
Going-up Theorem, 58
graded module, 106
graded ring, 106
graded rings, 106

height, 122
Hensel's lemma, 104
Hilbert dimension, 115, 118
Hilbert Nullstellensatz, 64
Hilbert's basis theorem, 72
Hilbert's Nullstellensatz, 63
Hilbert-Samuel function, 118

ideal, 2
image, 18
indecomposable, 87
induced topology, 148
integral closure, 53
integral element, 51
integral extension, 53
integral morphism, 53
integrally closed, 53
inverse limit, 101
inverse system, 101
invertible, 97
irreducible topological space, 74

Jacobian, 100

kernel, 18
Krull dimension, 65, 115
Krull's theorem, 9

left-derived functor, 131
left-exact, 24
length, 116
lies over, 57, 138
local morphism, 137
local ring, 8
localization at prime ideal $\mathfrak{p}$, 41
localization away from f, 41
localization of module, 44
localization of ring, 39
locally free, 47
Lying Over Theorem, 58

mapping property, 146
maximal ideal, 7
maximal irreducible closed set, 74
maximal spectrum, 12
minimal prime ideal, 16
module, 17
module homomorphism, 17
morphism, 151
morphisms, 145
multiplicative set, 39

Nakayama's lemma, 20, 21
nilpotent, 5
nilradical, 5, 10
Noether Normalization Lemma, 61
Noetherian module, 69
Noetherian ring, 69
Noetherian topological space, 73
normal, 53
number fields, 1

objects, 145
open sets, 12, 148

partially ordered set, 9
permanence of identities, 20
PID Structure Theorem, 19
polynomial ring, 2
poset, 9
primary decomposition, 86
primary ideal dimension, 115, 120
primary ideals, 81, 85
prime avoidance, 16
prime ideal, 7
principal, 97
principal ideal domain (PID), 6
principal ideals, 3
product of modules, 18
product ring, 2
projective, 38
projective modules, 152
pure tensors, 31

quasicompact, 149
quotient module, 17
quotient ring, 4

radical, 10
radical ideal, 10
rank, 47, 50
reduced, 5
reducible topological space, 73
Rees algebra, 107
regular local ring, 125
residue field, 139
restriction of scalar, 18
right-exact, 24
ring, 1
ring morphism, 2
ring of integers, 51
ring of regular functions, 11

scheme, 12
separable, 95
short exact sequence, 22
simple module, 115
small category, 27
snake lemma, 22

spectrum, 12
stable I-filtration, 104
stalk, 46
stalk-local property, 46
submodule, 17
subspace filtration, 106

tensor product, 31
topological space, 148
totally ordered set, 9
transcendence degree, 66

unique factorization domain (UFD), 6
unit, 5
universal mapping property, 146
universal property, 146

vanishing locus, 63
variety, 11

Yoneda’s lemma, 148

Zariski topology, 12
zero divisor, 5
Zorn’s lemma, 9

Notations

$(A:I)$ (colon fractional ideal), 97
(T) (ideal generated by set T), 3
$(x_1,\dots,x_n)$ (ideal generated by $x_1,\dots,x_n$), 3
$A[[x_1,\dots,x_k]]$ (formal series ring), 111
$A[b]$ (smallest subring containing B), 51
A_* (a chain complex), 132
A_+ (ideal of positive degree elements), 106
$A_\bullet$ (a graded ring), 106
$D(f)$ (distinguished open sets of Zariski topology), 14
$H_n(A_*)$ (n-th homology group), 132
$H_n(f)$ (induced map of homology groups), 151
$I(Z)$ (ideal of functions vanishing at Z), 63
$I+J$ (ideal addition), 3
IJ (ideal multplication), 3
IM (submodule generated by ideal), 18
IS (extended ideal), 3
M/N (quotient module), 17
$M\otimes_R N$ (tensor product), 31
$M_1\oplus\cdots\oplus M_n$ (direct sum of modules), 18
$M_1\times\cdots\times M_n$ (product of modules), 18
$M_\bullet$ (a graded module), 106
R/I (quotient ring), 4
$R[f^{-1}]$, R_f (localization away from f), 41
$R[x]$ (polynomial ring), 2
R-$\mathbf{Mod}$ (the category of R-modules), 17
$R\times S$ (product ring), 2
$R^\vee$ (dual of locally free module), 48
$R^{\oplus n}$ (free module), 18
$R_\mathfrak{p}$ (localization at $\mathfrak{p}$), 41
$S^{-1}I$ (localization of ideal I), 41
$S^{-1}M$ (localization of a module), 44
$S^{-1}R$ (localization of a ring), 39
$V(I)$ (closed set of Zariski topology), 12
$V_m(J)$ (vanishing locus of ideal J), 63
$\mathrm{Ann}(M)$ (annihilator of the module), 18
$\mathrm{Ann}(m)$ (annihilator of an element), 18
$\mathrm{Ass}(M)$ (associated primes), 81
$\mathrm{Cl}\,A$ (class group), 98
$\mathrm{Coker}\,\phi$ (cokernel), 18
$\mathrm{End}_R(M)$ (endomorphism module), 18
$\mathrm{Frac}\,R$ (fraction field), 40
$\mathrm{Hom}_R(M,N)$ (Hom module), 18
$\mathrm{Hom}_R(P,\bullet)$ (a covariant Hom functor), 23
$\mathrm{Hom}_R(\bullet,P)$ (a contravariant Hom functor), 23
$\mathrm{Ker}\,\phi$ (kernel of module morphism), 18
$\mathrm{Ker}\,f$ (kernel of ring homomorphism), 3
$\mathrm{Nil}\,R$ (nilradical), 5
$\mathrm{Spec}\,R$ (spectrum of R), 12
$\bullet\otimes_R M$ (the tensor functor), 33
$\det P$ (determinant of locally free module), 49
$\dim A$ (dimension of a ring), 65
$\dim_{\text{Hilbert}} R$ (Hilbert dimension), 118
$\dim_{\text{Krull}} R$ (Krull dimension), 115
$\dim_{\text{primary}} R$ (primary ideal dimension), 120
$\mathrm{gr}_F\, M$ (associated graded module), 111
$\mathrm{gr}_I\, A$ (associated graded ring), 111
$\mathrm{ht}\,I$ (height), 122
$\kappa(\mathfrak{p})$ (residue field), 139
$\mathrm{mSpec}\,R$ (maximal spectrum of R), 12
$\mathbf{Rings}$ (category of rings), 145
$\mathcal{I}_A$ (group of invertible fractional ideal), 98
$\mathcal{O}_K$ (ring of integers), 51
$\mathrm{Bl}_F\, M$ (blowup module), 107
$\mathrm{Bl}_I\, A$ (blowup algebra), 107
$\mathrm{Im}\,\phi$ (image), 18
$\mathrm{Mor}(A,B)$ (set of morphisms), 145
$\mathrm{Tor}_n^R(M,N)$ (n-th Tor functor), 133
$\mathrm{ch}(R\text{-}\mathbf{Mod})$ (category of chain complexes of R-modules), 151
$\mathrm{obj}\,\mathcal{C}$ (set of objects), 145
$\phi^\#$ (induced map on Spec), 14
$\sqrt{I}$ (radical ideal), 10
$\mathrm{tr\,deg}\,K/k$ (transcendence degree), 66
$\varinjlim_{i\in I} M_i$ (colimit), 26
$\varprojlim_n A_n$ (inverse limit), 101
${}_RN$ (restriction of scalar), 18
$l(M)$ (length of a module), 116

Bibliography

[AK13] Allen Altman and Steven Kleiman. *A term of Commutative Algebra*. May 2013. URL: https://www.mi.fu-berlin.de/en/math/groups/arithmetic_geometry/teaching/exercises/Altman_-Kleiman---A-term-of-commutative-algebra-_2017_.pdf.

[Art11] M. Artin. *Algebra*. Pearson Education, 2011. ISBN: 9780132413770. URL: https://books.google.com/books?id=QsOfPwAACAAJ.

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969, pp. ix+128. URL: https://webhomes.maths.ed.ac.uk/~v1ranick/papers/AtiyahMacdonald.pdf.

[Che25] Evan Chen. "An Infinitely Large Napkin". June 2025. URL: https://web.evanchen.cc/napkin.html.

[Eis95] David Eisenbud. *Commutative algebra*. Vol. 150. Graduate Texts in Mathematics. With a view toward algebraic geometry. Springer-Verlag, New York, 1995, pp. xvi+785. ISBN: 0-387-94268-8. DOI: 10.1007/978-1-4612-5350-1. URL: https://doi.org/10.1007/978-1-4612-5350-1.

[Lei14] Tom Leinster. *Basic category theory*. Vol. 143. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2014, pp. viii+183. ISBN: 978-1-107-04424-1. DOI: 10.1017/CBO9781107360068. URL: https://doi.org/10.1017/CBO9781107360068.

[Mun00] James R. Munkres. *Topology*. Second. Prentice Hall, Inc., Upper Saddle River, NJ, 2000, pp. xvi+537. ISBN: 0-13-181629-2.

[Stacks] The Stacks Project Authors. *Stacks Project*. https://stacks.math.columbia.edu. 2018.

[Vak24] Ravi Vakil. "The Rising Sea: Foundations of Algebraic Geometry". Sept. 2024. URL: https://math.stanford.edu/~vakil/216blog/.

[Vám78] P. Vámos. "On the minimal prime ideals of a tensor product of two fields". eng. In: *Mathematical proceedings of the Cambridge Philosophical Society* 84.1 (1978), pp. 25–35. ISSN: 0305-0041.

[Wei94] Charles A. Weibel. *An Introduction to Homological Algebra*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1994.