

Notes on Algebraic Geometry and Commutative Algebra

Eric Liu

CONTENTS

CHAPTER 1 THE VERY BASICS PAGE 4

| | | |
|-----|---|----|
| 1.1 | Rings | 4 |
| 1.2 | Modules and Algebra | 10 |
| 1.3 | Tensor product for modules and algebras | 14 |
| 1.4 | Localization | 16 |
| 1.5 | Integral dependence | 20 |
| 1.6 | Homological lemmas | 22 |
| 1.7 | Valuation Rings | 24 |
| 1.8 | Noetherian | 26 |
| 1.9 | Length | 29 |

CHAPTER 2 VALUATION RING AND DVR PAGE 32

| | | |
|-----|---|----|
| 2.1 | Localization of ideals | 32 |
| 2.2 | Uniqueness of Primary Decomposition | 34 |
| 2.3 | Existence of Primary Decomposition in Noetherian ring | 38 |
| 2.4 | Artin Rings | 39 |
| 2.5 | Equivalent Characterizations of DVR | 42 |
| 2.6 | UFT for ideals in 1-Krull-dimensional Noetherian domain | 44 |
| 2.7 | Fractional Ideal | 46 |
| 2.8 | Dedekind domain | 48 |

CHAPTER 3 DIMENSION AND COMPLETION PAGE 50

| | | |
|-----|--------------------------|----|
| 3.1 | Completion | 50 |
| 3.2 | Filtrations | 52 |
| 3.3 | Graded rings and modules | 53 |

| | | |
|-----|------------------|----|
| 3.4 | Dimension | 55 |
| 3.5 | Hilbert function | 56 |

CHAPTER 4 THE CLASSICAL PAGE 57

| | | |
|------|------------------------------------|----|
| 4.1 | Topology of Zariski | 57 |
| 4.2 | Affine variety | 61 |
| 4.3 | Projective variety | 64 |
| 4.4 | Quasi variety morphism | 68 |
| 4.5 | Coordinate ring and function field | 73 |
| 4.6 | Category of quasi varieties | 79 |
| 4.7 | Segre embedding | 80 |
| 4.8 | Rational map | 84 |
| 4.9 | Singularity | 88 |
| 4.10 | Intersection | 92 |

CHAPTER 5 SCHEMES PAGE 99

| | | |
|-----|------------------------|-----|
| 5.1 | Direct limit | 99 |
| 5.2 | Sheaves | 101 |
| 5.3 | Scheme | 105 |
| 5.4 | \mathcal{O} -modules | 109 |

CHAPTER 6 NOT USED YET PAGE 110

| | | |
|-----|------------------------------------|-----|
| 6.1 | Maybe later | 110 |
| 6.2 | Some Fulton | 111 |
| 6.3 | Dimension Theory | 112 |
| 6.4 | Some Fulton 2 | 113 |
| 6.5 | More Equivalent Definitions of DVR | 114 |
| 6.6 | PID, UFD and Gauss Lemma | 115 |
| 6.7 | Archived | 118 |

CHAPTER 7 THE GREAT THEOREMS PAGE 119

| | | |
|-----|---|-----|
| 7.1 | Hilbert's Nullstellensatz and basis theorem | 119 |
|-----|---|-----|

| | | |
|-----|--|-----|
| 7.2 | Noether Normalization Lemma (Half way there) | 121 |
| 7.3 | Hilbert-Serre Theorem | 123 |

Chapter 1

The Very Basics

1.1 Rings

The precise meaning of the term **ring** varies across different books, depending on the context and purpose. In this note, the multiplication of a ring is always associative, commutative, and has an identity. The additive identity is denoted by 0. From the axioms, we can straightforwardly show that $x \cdot 0 = 0$ for all x . Consequently, the multiplicative and additive identities are always distinct unless the ring contained only one element, and in such case, we say the ring is the **zero ring**. By **ring homomorphisms**, we mean mappings between two rings respecting addition¹, multiplication, and multiplicative identity. Clearly, inverse of a bijective ring homomorphism is also a ring homomorphism.

An **ideal** of a ring A is an additive subgroup \mathfrak{a} such that $xy \in \mathfrak{a}$ for all $x \in \mathfrak{a}, y \in A$. **Quotient ring** is a ring A/\mathfrak{a} together with a surjective ring homomorphism $\pi : A \rightarrow A/\mathfrak{a}$ that satisfies the **universal property of quotient ring**: For each ring homomorphism $f : A \rightarrow B$ that vanishes on \mathfrak{a} , there exists a unique $\tilde{f} \in \text{Hom}(A/\mathfrak{a}, B)$ that makes the diagram:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \pi \downarrow & \nearrow \tilde{f} & \\ A/\mathfrak{a} & & \end{array}$$

commutes.

Equivalent Definition 1.1.1. (First isomorphism theorem for rings) Let A be a ring and $\mathfrak{a} \subseteq A$. The followings are equivalent:

¹Respecting addition immediately implies respecting 0 and negation.

- (i) \mathfrak{a} is an ideal in A .
- (ii) \mathfrak{a} is the kernel of some ring homomorphism.

Proof. Unroll the definition. ■

Theorem 1.1.2. (Second isomorphism theorem for rings) Let A be a ring, $B \subseteq A$ a subring, and $\mathfrak{a} \subseteq A$ an ideal. Then:

- (i) $B + \mathfrak{a} \triangleq \{b + a \in A : b \in B, a \in \mathfrak{a}\}$ forms a subring of A .
- (ii) $B \cap \mathfrak{a}$ forms an ideal in B .
- (iii) $(B + \mathfrak{a})/\mathfrak{a} \cong B/(B \cap \mathfrak{a})$ as rings.

Proof. Unroll the definitions. ■

One should always be careful with the word **unit** and the word **zero-divisor**. In nonzero rings, the set of units is always disjoint with the set of zero-divisors. Given rings $A \subseteq B$, it is possible that $a \in A$ forms a non-zero-divisor (or unit) in A but not in B . Under our initial requirement that rings are commutative unital, for a nonzero ring A to be an **integral domain**, we only need all nonzero elements to be non-zero-divisors, and for A to be a **field**, we only need all nonzero elements to be units.

Equivalent Definition 1.1.3. (Field) Let A be a nonzero ring. The followings are equivalent:

- (i) A is a field.
- (ii) A have only two ideals, i.e., $\{0\}$ and A .
- (iii) Every ring homomorphism of A into a nonzero ring B is injective.

Proof. Unroll the definitions. ■

We use the term **proper** to describe strict set inclusion. A **maximal ideal** is a proper ideal contained by no other proper ideals. A **prime ideal** is a proper ideal \mathfrak{p} such that the product of two element lies in \mathfrak{p} implies one of them lies in \mathfrak{p} .

Equivalent Definition 1.1.4. (Prime ideals) Let $\mathfrak{p} \subseteq A$ be an ideal. The followings are equivalent:

- (i) \mathfrak{p} is prime.
- (ii) A/\mathfrak{p} forms an integral domain.

Proof. Unroll the definitions. ■

Equivalent Definition 1.1.5. (Integral domain) Let A be a ring. The followings are equivalent:

- (i) A is an integral domain.
- (ii) The zero ideal of A is prime.

Proof. Unroll the definitions. ■

Theorem 1.1.6. (Third isomorphism theorem and correspondence theorem for rings) Let A be a ring, $\mathfrak{a} \subseteq \mathfrak{b} \subseteq A$ be two ideals, S the collection of ideals in A that contains \mathfrak{a} , and $\pi : A \twoheadrightarrow A/\mathfrak{a}$ the quotient map. We denote $\mathfrak{b}/\mathfrak{a} \triangleq \pi(\mathfrak{b})$. Then:

- (i) $\mathfrak{b}/\mathfrak{a} \subseteq A/\mathfrak{a}$ forms an ideal.
- (ii) $(A/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}) \cong A/\mathfrak{b}$ as rings.
- (iii) The map $\mathfrak{c} \in S \mapsto \mathfrak{c}/\mathfrak{a}$ forms a bijection between S and the collection of ideals in A/\mathfrak{a} , a bijection between $S \cap \text{Spec } A$ and $\text{Spec}(A/\mathfrak{a})$, and a bijection between $S \cap \text{Max } A$ and $\text{Max}(A/\mathfrak{a})$.

Proof. Unroll the definition. ■

Let A be a ring. Chain of prime ideals $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ has **length** n . Given a prime ideal \mathfrak{p} , its **height** $\text{ht}(\mathfrak{p})$ is:

$$\text{ht}(\mathfrak{p}) \triangleq \sup \{n \in \mathbb{Z} : \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n \subseteq \mathfrak{p}\}$$

Given an ordinary ideal \mathfrak{a} , its **height** is:

$$\text{ht}(\mathfrak{a}) \triangleq \inf \{\text{ht}(\mathfrak{p}) \in \mathbb{Z} : \mathfrak{a} \subseteq \mathfrak{p} \in \text{Spec } A\}$$

The **Krull dimension** $\text{Krudim}(A)$ of A is:

$$\text{Krudim}(A) \triangleq \sup \{\text{ht}(\mathfrak{p}) : \mathfrak{p} \in \text{Spec } A\}$$

Equivalent Definition 1.1.7. (Krull dimension) Let A be a ring. The Krull dimension of A equals to the supremum of the length of chain of prime ideals in A .

Proof. ■

Equivalent Definition 1.1.8. (Maximal ideals) Let $\mathfrak{m} \subseteq A$ be an ideal. The followings are equivalent:

- (i) \mathfrak{m} is maximal.
- (ii) A/\mathfrak{m} forms a field.

Proof. This follows from **correspondence theorem for rings** and **equivalent definitions of field**. ■

Corollary 1.1.9. (Maximal ideals are prime) Let A be a ring. If $\mathfrak{m} \subseteq A$ is maximal, then \mathfrak{m} is prime.

Proof. This follows from **equivalent definition of prime ideals** and **equivalent definition of maximal ideals**. ■

Intersection of ideals clearly always form an ideal. We now introduce a key property of prime ideals:

Theorem 1.1.10. (Property of prime ideal)

- (i) $\mathfrak{a} \subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n \implies \mathfrak{a} \subseteq \mathfrak{p}_i$ for some i .
- (ii) $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n \subseteq \mathfrak{p} \implies \mathfrak{a}_i \subseteq \mathfrak{p}$ for some i .
- (iii) $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{p} \implies \mathfrak{a}_i = \mathfrak{p}$ for some i .

Proof. (i) is proved by induction. Assume not and cause a contradiction by considering $\sum(x_1 \cdots \hat{x}_i \cdots x_n)$ where $x_i \in \mathfrak{a} - \mathfrak{p}_i$. For (ii), assume not, and cause a contradiction by considering $\prod a_i$ where $a_i \in \mathfrak{a}_i - \mathfrak{p}$. (iii) follows from (ii). ■

For all subsets S of some ring A , the ideal $\langle S \rangle$ **generated** by S is the smallest ideals that contain S .

Equivalent Definition 1.1.11. (Generated ideals) Let A be a ring and $S \subseteq A$. We have:

$$\langle S \rangle = \left\{ \sum_{\text{finite}} a_i s_i \in A : a_i \in A, s_i \in S \right\}$$

Proof. Unroll the definitions. ■

A **principal ideal** $\langle x \rangle$ is an ideal generated by a single element. There are many ideals operations. Given any family of ideal (\mathfrak{a}_i) in A , their **sum ideal** is:

$$\sum \mathfrak{a}_i \triangleq \left\{ \sum_{\text{finite}} a_i \in A : a_i \in \mathfrak{a}_i \right\}$$

Equivalent Definition 1.1.12. (Sum of ideals) Let A be a ring and $\{\mathfrak{a}_i : i \in I\}$ a family of ideals in A . Then:

$$\sum_{i \in I} \mathfrak{a}_i = \left\langle \bigcup_{i \in I} \mathfrak{a}_i \right\rangle = \bigcup_{\substack{J \subseteq I \\ J \text{ finite}}} \sum_{j \in J} \mathfrak{a}_j$$

7

Proof. Unroll the definitions. ■

Theorem 1.1.13. (Expressing image of ideals in quotient ring using ideals sum) Let A be a ring, $\mathfrak{a}, \mathfrak{b}$ be two ideals in A , and $\pi : A \rightarrow A/\mathfrak{a}$ be the quotient map. We always have:

$$\pi(\mathfrak{b}) = \mathfrak{a} + \mathfrak{b}/\mathfrak{a}$$

Proof. Unroll the definitions. ■

Given any finite family $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ of ideals in A , their **product ideal** is:

$$\prod_{i=1}^n \mathfrak{a}_i \triangleq \left\{ \sum_{j=1}^m a_{j,1} \cdots a_{j,n} \in A : a_{j,i} \in \mathfrak{a}_i \right\}$$

Equivalent Definition 1.1.14. (Product of ideals) Let A be a ring and $\{\mathfrak{a}_1, \dots, \mathfrak{a}_n\}$ a finite family of ideals in A . The product ideal $(\mathfrak{a}_1 \cdots \mathfrak{a}_n)$ is generated by $\{a_1 \cdots a_n \in A : a_i \in \mathfrak{a}_i\}$.

Proof. Unroll the definitions. ■

One should check that both the definitions of sum and product for ideals are consistent in the sense that they indeed are both associative. Moreover, we have the distributive law:

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

Given two ideals $\mathfrak{a}, \mathfrak{b}$ in A , their **quotient ideal** $(\mathfrak{a} : \mathfrak{b})$ is:

$$(\mathfrak{a} : \mathfrak{b}) \triangleq \{x \in A : xb \in \mathfrak{a}, \quad \text{for all } b \in \mathfrak{b}\}$$

To simplify matter, we write $(\mathfrak{a} : x)$ instead of $(\mathfrak{a} : \langle x \rangle)$. This notation is justified since $(\mathfrak{a} : \langle x \rangle) = \{y \in A : xy \in \mathfrak{a}\}$. The **Jacobson radical** $\text{Jacob}(A)$ is the intersection of all maximal ideals of A . An element $x \in A$ is called **nilpotent** if $x^n = 0$ for some $n \in \mathbb{N}$. The set of all nilpotent elements clearly form an ideal $\text{Nil}(A)$ in A , which is the **nilradical** of A .

Theorem 1.1.15. (Equivalent Definition for Nilradical) Let A be a ring. We have:

$$\text{Nil}(A) = \bigcap \text{Spec } A$$

Proof. $\text{Nil}(A) \subseteq \bigcap \text{Spec } A$ is clear. Assume $x \in \bigcap \text{Spec } A - \text{Nil}(A)$ for a contradiction. Let Σ be the set of ideals \mathfrak{a} such that $x^n \notin \mathfrak{a}$ for all $n > 0$. Because unions of chains in Σ belong to Σ and because $0 \in \Sigma$, by Zorn's Lemma, there exists some maximal element $\mathfrak{a} \in \Sigma$. Because $x \notin \mathfrak{a}$, to close out the proof, we only have to show \mathfrak{a} is prime.

Let $yz \in \mathfrak{a}$. Assume for a contradiction that $y \notin \mathfrak{a}$ and $z \notin \mathfrak{a}$. By maximality of \mathfrak{a} , both $\mathfrak{a} + \langle y \rangle, \mathfrak{a} + \langle z \rangle$ don't belong to Σ . This implies $x^n \in \mathfrak{a} + \langle y \rangle$ and $x^m \in \mathfrak{a} + \langle z \rangle$ for some $n, m > 0$, which cause a contradiction to $\mathfrak{a} \in \Sigma$, since $x^{n+m} \in \mathfrak{a} + \langle yz \rangle = \mathfrak{a}$. ■

Let \mathfrak{a} be an ideal of the ring A . Its **radical** $\sqrt{\mathfrak{a}}$ in A is:

$$\sqrt{\mathfrak{a}} \triangleq \{x \in A : x^n \in \mathfrak{a} \text{ for some } n > 0\}$$

Equivalent Definition 1.1.16. (Radical of ideal) Let A be a ring and $\mathfrak{a} \subseteq A$ an ideal. The following are equivalent:

- (i) $\sqrt{\mathfrak{a}}$.
- (ii) The ideal in A that **correspond** to $\text{Nil}(A/\mathfrak{a})$ with respect to quotient map $A \twoheadrightarrow A/\mathfrak{a}$.
- (iii) The intersection of all prime ideals in A that contains \mathfrak{a} .

Proof. (i) = (ii): Unroll the definition. (ii) = (iii): Consider the **correspondence theorem** and $\text{Nil}(A/\mathfrak{a}) = \bigcap \text{Spec } A/\mathfrak{a}$. ■

Let A be a ring and $\mathfrak{a} \subseteq A$ be an ideal. A **minimal prime ideal \mathfrak{p} over \mathfrak{a}** is a prime ideal minimal among all prime ideals that contain \mathfrak{a} . Because of the **third definition of radical**, \mathfrak{a} and $\sqrt{\mathfrak{a}}$ share same set of minimal prime ideal. It should be noted that there is a "less is more" philosophy in our wording and notations for product, quotient and radical of ideals. For any ideal $\mathfrak{a}, \mathfrak{b}$, we have

$$\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \subseteq \sqrt{\mathfrak{a}} \text{ and } \mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$$

Let A be a ring. A **radical ideal** \mathfrak{a} in A satisfies $\sqrt{\mathfrak{a}} = \mathfrak{a}$.

Equivalent Definition 1.1.17. (Radical ideals) Let A be a ring and $\mathfrak{a} \subseteq A$ be an ideal. The followings are equivalent:

- (i) \mathfrak{a} is radical.
- (ii) $\mathfrak{a} = \sqrt{\mathfrak{b}}$ for some ideal $\mathfrak{b} \subseteq A$.

Proof. (i) \implies (ii) is trivial. (ii) \implies (i) is done by unrolling the definitions, which give us $\sqrt{\sqrt{\mathfrak{b}}} = \sqrt{\mathfrak{b}}$. ■

For ease in the section on fraction of rings and modules, we close this section by introducing two concept. Let $f : A \rightarrow B$ be some ring homomorphism. If E is a subset of A , we call the ideal in B generated by $f(E)$ the **extension** of E , which we denote by E^e . If E is a subset of B , we call the ideal in A generated by $f^{-1}(E)$ the **contraction** of E , which we denote by E^c . Clearly, if E is an ideal in B , then $E^c = f^{-1}(E)$.

1.2 Modules and Algebra

Let A be some ring. By an A -**module**, we mean an abelian group M together with a compatible A -scalar multiplication. An A -**module homomorphism** $f : M \rightarrow N$ is a function that respect addition², multiplication, and multiplicative identity. Note that every ring form a module over itself, and there is one-to-one correspondence between ideals and submodules when we do such.

Let N be a submodule of A -module M . **Quotient A -module** is an A -module M/N together with a surjective A -module homomorphism $\pi : M \rightarrow M/N$ that satisfies the **universal property of quotient module**: For each A -module homomorphism $f : M \rightarrow L$ that vanishes on N , there exists a unique A -module homomorphism $\tilde{f} : M/N \rightarrow L$ that makes the diagram:

$$\begin{array}{ccc} M & \xrightarrow{f} & L \\ \pi \downarrow & \nearrow \tilde{f} & \\ M/N & & \end{array}$$

commutes.

Equivalent Definition 1.2.1. (First isomorphism theorem for modules) Let N be a subset of an A -module M . The followings are equivalent:

- (i) N is an A -submodule of M .
- (ii) N is the kernel of some A -module homomorphism.

Proof. Unroll the definition. ■

Theorem 1.2.2. (Second isomorphism theorem for modules) Let N, T be two A -submodules of M . Then:

- (i) $N + T \triangleq \{x + y \in M : x \in N, y \in T\}$ forms an A -submodule.
- (ii) $N \cap T$ forms an A -submodule.
- (iii) $(N + T)/T \cong N/(N \cap T)$ as A -modules.

Proof. Unroll the definitions. ■

Theorem 1.2.3. (Third isomorphism theorem and correspondence theorem for modules) Let M be an A -module, $T \subseteq N \subseteq M$ be two A -submodules, S the collection of submodules of M that contains T , and $\pi : M \twoheadrightarrow M/T$ the quotient map. Then:

²Respecting addition immediately implies respecting 0 and negation.

- (i) $\pi(N)$ forms a submodule isomorphic to N/T , which shall be how we identify N/T as a submodule of M/T .
- (ii) $(M/T)/(N/T) \cong M/N$ as A -modules.
- (iii) The map $G \in S \mapsto G/T$ forms a bijection between S and the collection of submodules of M/T .

Proof. Unroll the definition. ■

Let $\{M_i : i \in I\}$ be a collection of A -modules. If we give the Cartesian product $\prod M_i$ the obvious addition and multiplication, then we say it is the **direct product**. It is clear that

$$\left\{ (x_i)_{i \in I} \in \prod_{i \in I} M_i : x_i \neq 0 \text{ for finitely many } i. \right\}$$

forms a submodule of the direct product. We denote this submodule by $\bigoplus M_i$, and call it the **direct sum**. Obviously, if the index set I is finite, then the direct product and direct sum are identical. Given a subset S of A -module M , its **span** is the smallest A -submodule of M that contains S .

Equivalent Definition 1.2.4. (Spanned modules) Let M be an A -module and $S \subseteq M$. We have:

$$\text{span}(S) = \left\{ \sum_{\text{finite}} a_i s_i \in M : a_i \in A, s_i \in S \right\}$$

Proof. Unroll the definitions. ■

We say an A -module is **finitely generated** if it can be spanned by some of its finite subset. Note that one should be careful with the term "generated", since when one identify a ring as a module over itself, the spanned module and the generated ideal of a fixed set can be distinct.

Theorem 1.2.5. (Property of finitely generated modules) Let M be an A -module spanned by $\{x_1, \dots, x_n\}$. M is isomorphic to some quotient modules of A^n .³

Proof. Clearly, $(a_1, \dots, a_n) \mapsto \sum a_i x_i$ forms a surjective A -module homomorphism from A^n to M . The rest of the proof then follows from **first isomorphism theorem for modules**. ■

Quite often, we are required to consider **extension of scalars**: Given ring homomorphism $f : A \rightarrow B$ and B -module N , we can give N an A -module by setting $an \triangleq f(a)n$.

³Albeit seems quite arbitrary and unimportant for now, this property will later prove useful for it guarantees that finitely generated module over rings of some certain properties carry the same property. For example, this shows that **finitely generated module over Noetherian ring is Noetherian**.

Theorem 1.2.6. (Finite generation and scalar extension) Given ring homomorphism $f : A \rightarrow B$ and some finitely generated B -module N , if B is finitely generated as an A -module under extension of scalar, then N is also finitely generated as an A -module under extension of scalar.⁴

Proof. If b_1, \dots, b_k generate B over A and n_1, \dots, n_r generate N over B , then clearly $\{b_i n_j \in N : i \in \{1, \dots, k\} \text{ and } j \in \{1, \dots, r\}\}$ generates N over A . ■

Given an ideal \mathfrak{a} of A , an A -module M and an A -submodule $N \subseteq M$, the **product $\mathfrak{a}N$ of the submodule N by the ideal \mathfrak{a}** is the A -submodule:

$$\mathfrak{a}N \triangleq \left\{ \sum_{\text{finite}} a_i x_i \in M : a_i \in \mathfrak{a} \text{ and } x_i \in N \right\}$$

We may now state **Nakayama's Lemma**.

Lemma 1.2.7. (Nakayama) Let M be a finitely generated A -module. If there exists some ideal $\mathfrak{a} \subseteq A$ contained by $\text{Jacob}(A)$ that makes $\mathfrak{a}M = M$, then $M = 0$.

Proof. Assume for a contradiction that $M \neq 0$. Let u_1, \dots, u_n be a minimal set of generators of M . Write $u_n = a_1 u_1 + \dots + a_n u_n$ where $a_i \in \mathfrak{a}$. This give us

$$(1 - a_n)u_n = a_1 u_1 + \dots + a_{n-1} u_{n-1} \quad (1.1)$$

We know that $1 - a_n$ must be a unit, otherwise by Zorn's Lemma⁵ there exists a maximal ideal \mathfrak{m} containing $1 - a_n$, which is impossible since $a_n \in \text{Jacob}(A)$ would have implies $1 \in \mathfrak{m}$. Because $1 - a_n$ is a unit, by **Equation 1.1**, u_n can be generated by $\{u_1, \dots, u_{n-1}\}$, a contradiction to the minimality of $\{u_1, \dots, u_n\}$. ■

Given two A -submodules N, P of M , their **quotient** $(N : P)$ is the collection of $a \in A$ that maps P into N , which clearly need to be an ideal in A . In particular, the **annihilator** $\text{Ann}(M)$ of M is $(0 : M)$. Clearly, if $\mathfrak{a} \subseteq \text{Ann}(M)$, we may view M as an A/\mathfrak{a} -module. We say M is a **faithful A -module** if $\text{Ann}(M) = 0$.

Equivalent Definition 1.2.8. (Faithful modules) Let M be an A -module. The followings are equivalent:

- (i) M is faithful.
- (ii) For each $a \neq b \in A$, there exists $x \in M$ such that $ax \neq bx$.
- (iii) Each $a \in A$ defines a unique endomorphism of M .

⁴This will be later used in **section on integral dependence**.

⁵Note that union of proper ideals is always proper because otherwise one of them would have contain 1.

Proof. Unroll the definitions. ■

Let M be an A -module, clearly M is always faithful as an $A/\text{Ann}(M)$ -module, and A is always faithful as an A -module. An **exact** sequence of A -modules is a sequence of A -modules whose every image equals to kernel of the next A -module homomorphism. Let A be a ring, \mathfrak{C} a subcategory of A -modules, and G an abelian group. A function $\lambda : \mathfrak{C} \rightarrow G$ is said to be **additive** if for each short exact sequence $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ in \mathfrak{C} , we have $\lambda(M) = \lambda(M') + \lambda(M'')$.

Theorem 1.2.9. (Examples of additive functions) The followings are examples of additive functions:

- (i) Let A be a field. The map $V \mapsto \dim V$ is an additive function on the category of finite-dimensional vector space with codomain \mathbb{Z} .

Proof. (i): Unroll the definition with rank-nullity theorem. ■

There are multiple equivalent definitions for the term **algebra B over ring A** . The easiest one is to say we have a ring homomorphism $f : A \rightarrow B$, which induces the scalar product: $a(b) \triangleq f(a)b$. Let B, C be two A -algebras with scalar defining map f, g . By an **A -algebra homomorphism**, we mean some ring homomorphism $h : B \rightarrow C$ that is also a A -module homomorphism.

Equivalent Definition 1.2.10. (Algebra homomorphisms) Let B, C be two A -algebras with scalar defining map f, g , and $h : B \rightarrow C$ be a ring homomorphism. The followings are equivalent:

- (i) h is an A -algebra homomorphism.
- (ii) $h \circ f = g$.

Proof. Unroll the definitions. ■

Let B be an A -algebra. B is **finitely generated as an A -algebra** if $B = A[x_1, \dots, x_n]$ for some $\{x_1, \dots, x_n\} \subseteq B$. Because there are three structures on B , one shall again be careful with the wording.

1.3 Tensor product for modules and algebras

Let R be some ring. By **free R -modules**, we mean R -modules of the form $\bigoplus_{i \in I} M_i$ where $M_i \cong R$. We denote the free module $\bigoplus_{i \in I} M_i$ by $R^{(I)}$. Given a finite collection $\{M_1, \dots, M_n\}$ of R -modules, by the term **tensor product space**, we mean a R -module denoted by $\bigotimes M_i$ and a R -multilinear map $\otimes : \prod M_i \rightarrow \bigotimes M_i$ that satisfies the **universal property**: For each multilinear map $f : \prod M_i \rightarrow P$, there exists unique linear map $\tilde{f} : \bigotimes M_i \rightarrow P$ such that the diagram

$$\begin{array}{ccc} \prod M_i & \xrightarrow{\otimes} & \bigotimes M_i \\ & \searrow f & \downarrow \tilde{f} \\ & & P \end{array}$$

commutes. This definition is unique up to isomorphism: If $\bigotimes' M_i$ is also a tensor product, then there exists some module isomorphism from $\bigotimes M_i$ to $\bigotimes' M_i$ that sends $m_1 \otimes \dots \otimes m_n$ to $m_1 \otimes' \dots \otimes' m_n$. One common construction of the tensor product space is to quotient the free module $R^{(\prod M_i)}$ with the submodule spanned by the set:

$$\begin{aligned} & \bigcup_{i=1}^n \left[\left\{ (x_1, \dots, rx_i, \dots, x_n) - r(x_1, \dots, x_n) \right\} \right. \\ & \quad \left. \cup \left\{ (x_1, \dots, x_i + x'_i, \dots, x_n) - (x_1, \dots, x_i, \dots, x_n) - (x_1, \dots, x'_i, \dots, x_n) \right\} \right] \end{aligned}$$

Denoting this spanned submodule by D , our tensor product space $\bigotimes M_i$ is now $R^{(\prod M_i)} / D$, and because of the forms of the generators of D , the tensor product map $\otimes : \prod M_i \rightarrow \bigotimes M_i$ defined by

$$x_1 \otimes \dots \otimes x_n \triangleq [(x_1, \dots, x_n)]$$

is clearly multilinear. Because free module $R^{(\prod M_i)}$ is a direct sum, it is clear that $\bigotimes M_i$ is generated by the **basic elements**⁶, and because of such, for every multilinear map $f : \prod M_i \rightarrow P$, the induced map $\tilde{f} : \bigotimes M_i \rightarrow P$ must be unique. To actually induce \tilde{f} , one first extend f to the whole free module $\bar{f} : R^{(\prod M_i)} \rightarrow P$ by setting $\bar{f}(\sum r(x_1, \dots, x_n)) \triangleq \sum r f(x_1, \dots, x_n)$, and see that because \bar{f} vanishes on the generators of D , we may induce some mapping from $\bigotimes M_i$ to P that clearly has the desired action of \tilde{f} on the basic elements.

⁶Elements of the form $x_1 \otimes \dots \otimes x_n$

Note that the **tensor-horn adjunction** isomorphism

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

maps $f \in \mathrm{Hom}(M \otimes N, P)$ to $\tilde{f} \in \mathrm{Hom}(M, \mathrm{Hom}(N, P))$ with the action

$$\tilde{f}(m)n \triangleq f(m \otimes n)$$

1.4 Localization

Let A be a ring. We say $S \subseteq A$ is a **multiplicatively closed subset** of A if S contains 1 and is closed under multiplication. We say a ring B and a homomorphism $f : A \rightarrow B$ satisfies the **universal property of localization of A by S** if

- (a) $f(S) \subseteq B^\times$.
- (b) $f(a) = 0 \implies as = 0$ for some $s \in S$.
- (c) $B = \{f(a)f(s)^{-1} : a \in A \text{ and } s \in S\}$

Suppose $f : A \rightarrow B$ satisfies the universal property of localization of A by S . Clearly, given any ring homomorphism $g : A \rightarrow C$ that maps S into C^\times , the ring homomorphism $\tilde{g} : B \rightarrow C$ well-defined by $\tilde{g}(f(a)f(s)^{-1}) \triangleq g(a)g(s)^{-1}$ is the unique ring homomorphism such that the diagram

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow g & \downarrow \tilde{g} \\ & & C \end{array}$$

commutes.⁷ By **localization of A by S** , we merely mean some $A \xrightarrow{f} B$ that satisfies the universal property of localization of A by S . Moreover, we always use the notation $S^{-1}A$ to denote B , and refer to f as the **canonical ring homomorphism**. Adopting the convention of denoting $f(a)f(s)^{-1} \in S^{-1}A$ by $\frac{a}{s}$, we see that we have the intuitive:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \text{ and } \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

and by universal property

$$\frac{a}{s} = \frac{a'}{s'} \iff (as' - a's)s'' = 0 \text{ for some } s'' \in S.$$

Just as our fraction notation suggest, if $T \subseteq S$ is another multiplicatively closed subset of A , then clearly the canonical ring homomorphism $A \longrightarrow S^{-1}A$ maps T into $(S^{-1}A)^\times$. This by universal property implies the existence and uniqueness of a ring homomorphism from $T^{-1}A$ to $S^{-1}A$ that forms a commutative triangle with the two canonical ring homomorphism. This ring homomorphism have the obvious action, and will be how we are going to

⁷Just like the universal properties for other mathematical objects, one many check that if $A \xrightarrow{f'} B'$ also satisfies the universal property of localization of A by S , then $B \cong B'$, and the proof is exactly the same as the ones for other mathematical objects.

identify $T^{-1}A$ as a subring of $S^{-1}A$ ⁸. Similarly, given $A \hookrightarrow B$, universal property implies the existence and uniqueness of a ring homomorphism from $S^{-1}A$ to $S^{-1}B$ that forms a commutative triangle with $A \longrightarrow S^{-1}A$ and the composited $A \hookrightarrow B \longrightarrow S^{-1}B$, which have the obvious action and will be how we are going to identify $S^{-1}A$ as a subring of $S^{-1}B$.

There are even more reason to adopt the fractional notation for localizations: observe

- (i) $S^{-1}A = 0$ if $0 \in S$, aligning with our intuition that 0 can never be a denominator.
- (ii) $(\{1\})^{-1}A \cong A$.
- (iii) $as^{-1} \in S^{-1}A$ is a unit in $S^{-1}A$ if and only if $a \in S$.

Let A be a ring, and let $S \subseteq A$ be a multiplicatively closed subset that contains no zero-divisors. Clearly, in $S^{-1}A$,

$$\frac{a}{s} = \frac{b}{t} \text{ if and only if } at = bs.$$

This implies that the canonical ring homomorphism $A \longrightarrow S^{-1}A$ is injective, which is how we are going to identify A as a subring of $S^{-1}A$. Using the universal property, we see that the **field of fraction** $\text{Frac}(D) \triangleq (D^*)^{-1}D$ is the smallest field that contains a subring isomorphic to D .

Let A be some ring, $S \subseteq A$ an multiplicatively closed subset, and M an A -module. By the **localization of M by S** , we mean an A -module $S^{-1}M$ and a canonical A -module homomorphism $M \xrightarrow{j} S^{-1}M$ that satisfies the **universal property for localization of M by S** :

- (a) Every $s \in S$ acts invertibly on $S^{-1}M$.
- (b) For any A -module N on which all $s \in S$ acts invertibly and any A -module homomorphism $M \xrightarrow{g} N$, there exists a unique A -module homomorphism \tilde{g} such that the diagram

$$\begin{array}{ccc} M & \xrightarrow{j} & S^{-1}M \\ & \searrow g & \downarrow \tilde{g} \\ & & N \end{array}$$

commutes.

⁸One may check that this ring homomorphism is indeed injective.

Just like localization of ring, we adopt the fractional notation $y \triangleq \frac{m}{s}$ for $sy = j(m)$, which give us the intuitive:

$$\frac{m}{s} + \frac{n}{t} = \frac{mt + ns}{st} \text{ and } a \cdot \frac{m}{s}$$

and also by universal property:

$$\frac{m}{s} = \frac{m'}{s'} \iff (ms' - m's)s'' = 0 \text{ for some } s'' \in S.$$

Again, if $T \subseteq S$ is another multiplicatively closed subset of A , if there exists injective ring homomorphism $A \hookrightarrow B$, and if there exists A -submodule $N \subseteq M$, then the obvious action is what the universal property will induce, thus being how we identify one as subsets of another.

Contrary to ring localization, there is one more thing to note about localization of module. Given some A -module N on which all $s \in S$ act invertibly, we may give N the **canonical** $S^{-1}A$ -module structure⁹, and this is how we are going to view $S^{-1}M$ as an $S^{-1}A$ -module. Also, given an A -module homomorphism $M \xrightarrow{f} N$, one may check that the unique A -module homomorphism $S^{-1}f$ from $S^{-1}M$ to $S^{-1}N$ that forms a commutative triangle with $M \longrightarrow S^{-1}M$ and $M \xrightarrow{f} N \longrightarrow S^{-1}N$ have the action $\frac{a}{s} \mapsto \frac{f(a)}{s}$, and is thus also an $S^{-1}A$ -module homomorphism. Note that we have the result:

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \implies S^{-1}(g \circ f) = S^{-1}g \circ S^{-1}f$$

where the left hand side diagram happens in the category of A -module. In other words, localization forms a functor.

Theorem 1.4.1. (Localization is an exact functor) If

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

is exact, then

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$$

is also exact.

Proof. Clearly, we only have to prove $\text{Ker}(S^{-1}g) \subseteq \text{Ker}(S^{-1}f)$. Suppose $\frac{m}{s} \in \text{Ker}(S^{-1}g)$. We have $tg(m) = 0$ for some $t \in S$. This implies $tm \in \text{Ker } g = \text{Im } f$. Suppose $f(m') = tm$. This now give us $\frac{m}{s} = S^{-1}f(\frac{m'}{st})$. ■

⁹It is the obvious one.

If $f \in A$, we often write A_f in place of $(\{f^n : n \geq 0\})^{-1}A$, and if \mathfrak{p} is a prime ideal of A , we often just call $A_{\mathfrak{p}} \triangleq (A \setminus \mathfrak{p})^{-1}A$ the **localization of A at \mathfrak{p}** . Clearly, every nontrivial localizations of integral domain A , even not at primes, are still integral domain, so it make sense to talk the fraction field of $S^{-1}A$. Moreover, a routine, long, and tedious proof from universal property, shows that the obvious map from $\text{Frac}(S^{-1}A)$ to $\text{Frac}(A)$ is an isomorphism, so we usually treat $S^{-1}A$ as a subring of $\text{Frac}(A)$ containing A . In fact, one have $A = \bigcap A_{\mathfrak{m}}$ where \mathfrak{m} runs over all maximal ideals of A ¹⁰.

A **local ring** is a ring that has only one maximal ideal.

Equivalent Definition 1.4.2. (Local rings) Let A be a ring. The followings are equivalent:

- (i) A is a local ring.
- (ii) A is the localization of some ring B at some $\mathfrak{p} \in \text{Spec } B$.
- (iii) Its set of non-units form an ideal.

Proof. (i) \implies (ii): Check that $B \triangleq A$ and $\mathfrak{p} \triangleq \mathfrak{m}$ suffice. (ii) \implies (iii): Because \mathfrak{p} is prime, we see that the set of non-units in $B_{\mathfrak{p}}$ is exactly $\{b/s \in B_{\mathfrak{p}} : b \in \mathfrak{p}\}$. This set forms an ideal as one can check. (iii) \implies (i): The proof follows from noting that any ideal that contains some unit contains the whole ring. ■

One of the key property of local ring A is that if we let \mathfrak{m} be its unique maximal ideal, then the quotient A -module $\mathfrak{m}/\mathfrak{m}^2$ forms a A/\mathfrak{m} -vector space, called the **cotangent space of A** , with the obvious assignment of scalar product. If A is local, we often write (A, \mathfrak{m}, k) to mean that \mathfrak{m} is the unique maximal ideal of A and k the residue field $k \triangleq A/\mathfrak{m}$. A **regular local ring** A satisfies $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = \text{Krudim}(A)$.

¹⁰Because if $s \in A$ is not in any maximal ideal of A , then s must be a unit.

1.5 Integral dependence

Let A be a subring of some ring B . We say $x \in B$ is **integral over** A if x is a root of some monic polynomial with coefficients in A .

Theorem 1.5.1. (Cayley-Hamilton Theorem for finitely generated module) Suppose $\mathfrak{a} \subseteq A$ is an ideal, and M is a finitely generated A -module. If $\phi \in \text{End}(M)$ satisfies $\text{Im } \phi \subseteq \mathfrak{a}M$, then there exists some $a_0, \dots, a_{n-1} \in \mathfrak{a}$ such that

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

Proof. Let $\{m_1, \dots, m_n\}$ generate M . Because $\text{Im}(\phi) \subseteq \mathfrak{a}M$, we may write

$$\phi(m_i) = \sum_{j=1}^n a_{ij}m_j, \quad \text{where } a_{ij} \in \mathfrak{a}$$

Clearly, for each i , we have

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

where $\mathbf{1} \in \text{End}(M)$ is the identity operator and δ_{ij} is the Kronecker delta. Defining $R \triangleq A[\phi] \subseteq \text{End}(M)$, we may now view $\delta_{ij}\phi - a_{ij}\mathbf{1}$ as an $n \times n$ matrix, whose entries are elements of ring R . Because R is a commutative unital ring, there exist R -matrix X **adjugate** to $(\delta_{ij}\phi - a_{ij}\mathbf{1})$, i.e., $X(\delta_{ij}\phi - a_{ij}\mathbf{1}) = \det(\delta_{ij}\phi - a_{ij}\mathbf{1})I$, where I is the identity R -matrix. This implies that

$$\det(\delta_{ij}\phi - a_{ij}\mathbf{1})m_k = 0, \quad \text{for all } k \in \{1, \dots, n\}$$

Noting that $\det(\delta_{ij}\phi - a_{ij}\mathbf{1})$ is an \mathfrak{a} -polynomial in ϕ and $M = \langle m_1, \dots, m_n \rangle$, our proof is done. ■

Cayley-Hamilton Theorem for finitely generated module allow us to give the **equivalent definitions of integral dependence**, which are the keys for defining integral closure.

Equivalent Definition 1.5.2. (Equivalent Definitions for integral dependence)

Let A be a subring of B , and let $x \in B$. The following are equivalent:

- (i) $x \in B$ is integral over A .
- (ii) $A[x]$ is a finitely generated A -module.
- (iii) $A[x]$ is contained in a subring C of B such that C as an A -module is finitely generated.
- (iv) There exists a faithful $A[x]$ -module M which is finitely generated as an A -module.

Proof. (i) \implies (ii) \implies (iii) \implies (iv) is clear. We now prove (iv) \implies (i). Define an A -module endomorphism $\phi : M \rightarrow M$ by $y \mapsto xy$. By **Cayley-Hamilton Theorem for finitely generated module**, $\phi^n + a_{n-1}\phi^{n-1} + \cdots + a_0 = 0$. In other words, $(x^n + a_{n-1}x^{n-1} + \cdots + a_0)y = 0$ for all $y \in M$. Consider the case when $c = 1$, and we are done. ■

Corollary 1.5.3. (Polynomial rings of integral elements are finitely generated)

Let $A \subseteq B$ be rings, and $\{x_1, \dots, x_n\} \subseteq B$ all be integral over A . Subring $A[x_1, \dots, x_n] \subseteq B$ is finitely generated as an A -module.

Proof. The proof is done by induction on n . Base case $n = 1$ follows from **equivalent definitions for integral dependence**. We now do the inductive case, where $n > 1$. Clearly, x_n is integral over $A[x_1, \dots, x_{n-1}]$. This by **equivalent definitions for integral dependence** implies $A[x_1, \dots, x_n]$ is finitely generated as a $A[x_1, \dots, x_{n-1}]$ -module. Inductive hypothesis said that $A[x_1, \dots, x_{n-1}]$ is finitely generated as an A -module. The rest of the proof then follows from **theorem 1.2.6**. ■

Corollary 1.5.4. (Integral closure is well-defined) Let $A \subseteq B$ be rings. The set of $x \in B$ integral over A forms a ring.

Proof. Let $x, y \in B$ be integral over A . We are required to prove $x \pm y, xy$ are also integral over A . **Corollary 1.5.3** stated that $A[x, y]$ is finitely generated as an A -module. The rest of the proof then follows from **equivalent definitions for integral dependence** and the observation $A[x + y], A[xy] \subseteq A[x, y]$. ■

Because of **corollary 1.5.4**, we may well define **integral closure of A in B** to be the ring of elements of B integral over A . If A itself is the integral closure of itself in B , we say A is **integrally closed in B** . An integral domain is said to be an **integrally closed domain** if it is integrally closed in its field of fraction.

Note that integral and algebraic dependence are related as expected. Given two integral domains $A \subseteq B$ where B is integral over A , $\text{Frac}(B)$ is algebraic over A .

Corollary 1.5.5. (Transitivity of Integral Closure) Let $A \subseteq B \subseteq C$ be rings. If C is integral over B and B is integral over A , then C is integral over A .

Proof. Let $x \in C$. Because C is integrally over B , we know

$$x^n + b_n x^{n-1} + \cdots + b_1 = 0, \quad \text{for some } b_1, \dots, b_n \in B$$

1.6 Homological lemmas

Let R be some ring. Given a sequence of R -modules and R -modules homomorphism

$$\cdots \longrightarrow M_{k-1} \xrightarrow{f} M_k \xrightarrow{g} M_{k+1} \longrightarrow \cdots$$

we say the sequence is **exact** at M_k if $\text{Im}(f) = \text{Ker}(g)$, and we say a sequence is **exact** if it is exact at each of its module. By a **short** exact sequence, we mean exact sequence of the form

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

Lemma 1.6.1. (Five Lemma) Given a commutative diagram in the category of R -module:

$$\begin{array}{ccccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D & \xrightarrow{j} & E \\ \downarrow l & & \downarrow m & & \downarrow n & & \downarrow p & & \downarrow q \\ A' & \xrightarrow{r} & B' & \xrightarrow{s} & C' & \xrightarrow{t} & D' & \xrightarrow{u} & E' \end{array}$$

If the two rows are exact, m, p are isomorphism, l is surjective and q is injective, then n is also an isomorphism. The proof of Five Lemma follows immediately from the two Four Lemma, and their proof are both just diagram chasing. For demonstration, we present a proof for the **first four lemma**.

Lemma 1.6.2. (First Four Lemma) Given a commutative diagram in the category of R -module:

$$\begin{array}{ccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D \\ \downarrow l & & \downarrow m & & \downarrow n & & \downarrow p \\ A' & \xrightarrow{r} & B' & \xrightarrow{s} & C' & \xrightarrow{t} & D' \end{array}$$

If the two rows are exact, m, p are injective, l is surjective, then n is injective.

Proof. Let $c \in C$ such that $n(c) = 0$. We are required to show $c = 0$. Using the hypothesis, we may deduce

$$n(c) = 0 \implies t \circ n(c) = 0 \implies p \circ h(c) = 0 \implies h(c) = 0 \implies c = g(b)$$

for some $b \in B$. Observing that $s(m(b)) = n \circ g(b) = n(c) = 0$, we see $m(b) = r(a')$ for some $a' \in A'$. Because l is surjective, $a' = l(a)$ for some $a \in A$. Now, because

$$m \circ f(a) = r \circ l(a) = r(a') = m(b)$$

by injectivity of m , we may deduce $b = f(a)$. This together with first row being exact shows that

$$c = g(b) = g \circ f(a) = 0$$

■

Lemma 1.6.3. (Second Four Lemma) Given a commutative diagram in the category of R -modules:

$$\begin{array}{ccccccc} B & \xrightarrow{g} & C & \xrightarrow{h} & D & \xrightarrow{j} & E \\ \downarrow m & & \downarrow n & & \downarrow p & & \downarrow q \\ B' & \xrightarrow{s} & C' & \xrightarrow{t} & D' & \xrightarrow{u} & E' \end{array}$$

If the two rows are exact, m, p are surjective, q is injective, then n is surjective. As a special case of the **Five Lemma**, we now have the **Short Five Lemma**.

Lemma 1.6.4. (Short Five Lemma) Given a commutative diagram in the category of R -modules:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \longrightarrow & C & \longrightarrow & D & \longrightarrow & 0 \\ & & \downarrow m & & \downarrow n & & \downarrow p & & \\ 0 & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & D' & \longrightarrow & 0 \end{array}$$

If the two rows are exact and m, p are isomorphisms, then n is an isomorphism.

1.7 Valuation Rings

Let K be a field and D a subring of K . If for each $x \neq 0 \in K$ either $x \in D$ or $x^{-1} \in D$, then the mapping $K \longrightarrow \text{Frac}(D)$ defined by

$$x \mapsto \begin{cases} \frac{x}{1} & \text{if } x \in D \\ \frac{1}{x^{-1}} & \text{if } x \notin D \end{cases}$$

forms a ring isomorphism¹¹. Because of this identification, for each integral domain D , it make sense to say D is a **valuation ring of field K** if

$$x \in \text{Frac}(D) \implies x \in D \text{ or } x^{-1} \in D \quad (1.2)$$

since if we replace $\text{Frac}(D)$ with K in [equation 1.2](#), we know that K is isomorphic to $\text{Frac}(D)$. Given a field K and a totally ordered abelian group Γ , we say $\nu : K \rightarrow \Gamma \cup \{\infty\}$ is a **valuation** if it satisfies:

- (a) $\nu^{-1}(\infty) = \{0\}$.
- (b) $\nu(xy) = \nu(x) + \nu(y)$.
- (c) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$, with the equality holds true if $\nu(x) \neq \nu(y)$.

Equivalent Definition 1.7.1. (Equivalent Definitions of valuation rings) Let D be an integral domain. The following are equivalent

- (i) D is a valuation ring.
- (ii) The principal ideals of D are totally ordered by inclusion.
- (iii) The ideals of D are totally ordered by inclusion.
- (iv) There is a totally ordered abelian group Γ and a valuation $\nu : \text{Frac}(D) \rightarrow \Gamma \cup \{\infty\}$ such that $D = \{x \in \text{Frac}(D) : \nu(x) \geq 0 \in \Gamma\}$.

Proof. It is easy to prove (vi) \implies (i) \implies (ii) \implies (iii) \implies (i). For (i) \implies (iv), let D^\times be the set of units of D . Clearly, D^\times is a normal subgroup of $(\text{Frac } D)^*$. Because D is a valuation ring, we may well define a total order on $\Gamma \triangleq (\text{Frac } D)^* / D^\times$ by

$$[x] \geq [y] \iff xy^{-1} \in D$$

It is routine to check that $\nu : \text{Frac}(D) \rightarrow \Gamma \cup \{\infty\}$ defined by

$$\nu(x) \triangleq \begin{cases} [x] & \text{if } x \neq 0 \\ \infty & \text{if } x = 0 \end{cases}$$

is a valuation such that $D = \{x \in \text{Frac}(D) : \nu(x) \geq 0 \in \Gamma\}$. ■

¹¹Category of fields is a subcategory of rings. Field homomorphisms are ring homomorphisms.

Obviously, the name "valuation rings" comes from the fact an integral domain D is a valuation ring if and only if its field of fraction admits some valuation whose preimage of nonnegative element is exactly D . Because of such, given field K and valuation $\nu : K \rightarrow \Gamma \cup \{\infty\}$, when we want to refer to the valuation ring $\{x \in K : \nu(x) \geq 0 \in \Gamma\}$, we may refer it as the valuation ring *of* ν .

Theorem 1.7.2. (Valuation rings are integrally closed) If D is a valuation ring, then D is integrally closed.

Proof. Let $x \in \text{Frac}(B)$ be integral over B , say,

$$x^n + b_1x^{n-1} + \cdots + b_n = 0, \quad \text{where } b_i \in B.$$

If $x \in B$ there is nothing to prove. If not, then $x^{-1} \in B$ and thus $x = -(b_1 + b_2x^{-1} + \cdots + b_nx^{1-n}) \in B$. ■

Clearly, if D is a valuation ring of ν , then the set of units of D is exactly the preimage $\nu^{-1}(0)$.¹² This tell us for all $x \in K$, we have

| | $x \in D$ | $x \notin D$ |
|-------------------|--------------|--------------|
| $x^{-1} \in D$ | $\nu(x) = 0$ | $\nu(x) < 0$ |
| $x^{-1} \notin D$ | $\nu(x) > 0$ | impossible |

Moreover, because **ideals of valuation rings are totally ordered by inclusion**, we know valuation ring is local, and thus the set of non-units form an ideal, the unique maximal ideal \mathfrak{m} . In fact, \mathfrak{m} has the form:

$$\mathfrak{m} = \{x \in D : \nu(x) > 0 \in \Gamma\}$$

Theorem 1.7.3. () Let K be a field, Ω an algebraically closed field, Σ the set of all pairs (A, f) , where A is a subring of K and f is a ring homomorphism of A into Ω . If we partially order Σ by

$$(A, f) \leq (A', f') \iff A \subseteq A' \text{ and } f'|_A = f$$

¹²Because $0 = \nu(1) = \nu(x) + \nu(x^{-1})$ and $D = \nu^{-1}(\{x \in K : \nu(x) \geq 0 \in \Gamma\})$, we know $x, x^{-1} \in D \implies \nu(x) = 0$, and we also know $\nu(x) = 0 \implies \nu(x^{-1}) = 0 \implies x^{-1} \in D$.

1.8 Noetherian

Given some collection Σ of sets, we say Σ satisfies the **ascending chain condition, a.c.c.**, if for each chain $x_1 \subseteq x_2 \subseteq \cdots$ there exists n such that $x_n = x_{n+1} = \cdots$, and we say Σ satisfies the **descending chain condition, d.c.c.**, if for each chain $x_1 \supseteq x_2 \supseteq \cdots$ there exists n such that $x_n = x_{n+1} = \cdots$. Let M be some module. We say M is **Noetherian** if the collection of submodules of M satisfies a.c.c., and we say M is **Artinian** if the collection of submodules satisfies d.c.c. Thanks to axiom of choice, we have:

Equivalent Definition 1.8.1. (Noetherian modules) Let M be a module. The following are equivalent:

- (a) M is Noetherian.
- (b) Every nonempty collection of submodules of M has a maximal element.
- (c) Every submodule of M is finitely generated.

Immediately from the equivalent definitions of Noetherian, we have the following useful properties for ideals in Noetherian ring. How useful? See how we established equivalent characterization of DVR with [corollary 1.8.2](#) in [theorem 2.5.1](#).

Corollary 1.8.2. (Ideals in Noetherian always contain some powers of its radical) If $\mathfrak{a} \subseteq A$ for Noetherian A , then $\mathfrak{a} \supseteq (\sqrt{\mathfrak{a}})^n$ for some n .

Proof. Suppose $\sqrt{\mathfrak{a}} = \langle x_1, \dots, x_k \rangle$ and $x_i^{n_i} \in \mathfrak{a}$. Defining

$$m \triangleq \left(\sum_{i=1}^k n_i - 1 \right) + 1$$

We have

$$(\sqrt{\mathfrak{a}})^m = \left\langle \left\{ x_1^{r_1} \cdots x_k^{r_k} \in A : \sum_{i=1}^k r_i = m \text{ and } r_i \geq 0 \right\} \right\rangle$$

Now, by definition of m , we have

$$\sum_{i=1}^k r_i = m \text{ and } r_i \geq 0 \implies r_i \geq n_i \text{ for at least one } i$$

which implies $x_1^{r_1} \cdots x_k^{r_k} \in \mathfrak{a}$ for all $\sum_{i=1}^k r_i = m$ and $r_i \geq 0$. ■

Corollary 1.8.3. (Primary ideals of Noetherian rings) Let A be Noetherian and $\mathfrak{m} \subseteq A$ maximal. For any ideal $\mathfrak{q} \subseteq A$, we have

$$\mathfrak{q} \text{ is } \mathfrak{m}\text{-primary} \iff \mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m} \text{ for some } n > 0$$

Proof. (\implies) : This follows from [corollary 1.8.2](#). (\impliedby) : $\mathfrak{m} = \sqrt{\mathfrak{q}}$ follows from $\mathfrak{m} \subseteq \sqrt{\mathfrak{m}^n} \subseteq \sqrt{\mathfrak{q}} \subseteq \sqrt{\mathfrak{m}} = \mathfrak{m}$. It remains to prove \mathfrak{q} is indeed primary.

Because $\mathfrak{m} = \sqrt{\mathfrak{q}}$, by definition of radical \mathfrak{m} is preimage of $\text{Nil}(A/\mathfrak{q})$. This implies by correspondence theorem for rings¹³ that $\text{Nil}(A/\mathfrak{q})$ is the only prime ideal of A/\mathfrak{q} .¹⁴ We have shown A/\mathfrak{q} is local, so $\text{Nil}(A/\mathfrak{q})$ is exactly the collection of non-units of A/\mathfrak{q} . This implies every zero-divisor in A/\mathfrak{q} is nilpotent, which implies \mathfrak{q} is primary. ■

We close this section by showing Noetherian and Artinian properties are closed under multiple operations.

Proposition 1.8.4. (Formal properties of Noetherian and Artinian modules)

Given a short exact sequence of A -modules:

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$$

M is Noetherian if and only if M' and M'' are both Noetherian. Also, M is Artinian if and only if M' and M'' are both Artinian.

Proof. Consider chain condition definition. For the "if" part, let L_n be an ascending chain of submodules of M , and use [short five lemma](#) on

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \alpha^{-1}(L_n) & \xrightarrow{\alpha} & L_n & \xrightarrow{\beta} & \beta(L_n) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \alpha^{-1}(L_{n+1}) & \xrightarrow{\alpha} & L_{n+1} & \xrightarrow{\beta} & \beta(L_{n+1}) & \longrightarrow & 0 \end{array}$$

to conclude that L_n must stop at some point. ■

Theorem 1.8.5. (closed property of Noetherian) Let A be a Noetherian ring, $S \subseteq A$ a multiplicatively closed subset, $\mathfrak{a} \subseteq A$ an ideal, M an A -module, and $N \subseteq M$ an A -submodule. We have:

- (i) A^n as an A -module is Noetherian.
- (ii) If M is Noetherian, then M/N is also Noetherian.
- (iii) If M is finitely generated, then M is Noetherian.
- (iv) \mathfrak{a} as an A -module is Noetherian.

¹³What we mean by the correspondence theorem for ring is [this](#).

¹⁴This is because $\text{Nil}(A/\mathfrak{q}) = \bigcap \text{Spec}(A/\mathfrak{q})$. See [theorem 1.1.15](#). The proof is nontrivial.

Proof. For (i), just apply [Proposition 1.8.4](#) inductively to

$$0 \longrightarrow A \longrightarrow A^n \longrightarrow A^{n-1} \longrightarrow 0$$

And for (ii), just apply [Proposition 1.8.4](#) to

$$0 \longrightarrow 0 \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

For (iii), one simply note that if $M = \langle x_1, \dots, x_n \rangle$, then $\phi : A^n \rightarrow M; (a_1, \dots, a_n) \mapsto a_1x_1 + \dots + a_nx_n$ forms a surjective A -module homomorphism, thus M isomorphic to $A/\text{Ker } \phi$ is Noetherian by (i) and (ii). (iv) is clear. ■

Theorem 1.8.6. (closed property of Artinian) Let A be a Artinian ring, $S \subseteq A$ a multiplicatively closed subset, $\mathfrak{a} \subseteq A$ an ideal, M an A -module, and $N \subseteq M$ an A -submodule. We have:

- (i) A^n as an A -module is Artinian.
- (ii) If M is Artinian, then M/N is also Artinian.
- (iii) If M is finitely generated, then M is Artinian.
- (iv) \mathfrak{a} as an A -module is Artinian.

Proof. The proofs are identical to that of [Theorem 1.8.5](#). ■

1.9 Length

Given a finite **chain** of submodules

$$M_0 \subset M_1 \subset \cdots \subset M_n$$

we say this chain is of **length** n . Under the obvious assignment of order on the collection of all finite chains of submodules of M , we may define the **composition series** of M to be the maximal finite chains. Clearly, a finite chain

$$0 = M_0 \subset \cdots \subset M_n = M$$

is maximal if and only if M_k/M_{k-1} are simple.

Theorem 1.9.1. (Length of modules is well defined) Every composition series of a module M have the same length.

Proof. Suppose M has a composition series, and let $l(M)$ denote the least length of a composition series of M . We wish to show every chain has length smaller than $l(M)$. Before such, we first prove

$$N \subset M \implies l(N) < l(M) \tag{1.3}$$

Let $M_0 \subset \cdots \subset M_n = M$ be a composition series of least length. Define $N_k \triangleq N \cap M_k$ for all $k \in \{0, \dots, n\}$. Consider the obvious homomorphism $N_k/N_{k-1} \rightarrow M_k/M_{k-1}$. We see that either $N_k/N_{k-1} \cong M_k/M_{k-1}$ or $N_k = N_{k-1}$. This implies that the chain $N_0 \subset \cdots \subset N_n$ will be a composition series of N after the unnecessary terms are removed. It remains to show there are unnecessary terms in $N_0 \subset \cdots \subset N_n$. Assume not for a contradiction. Because $N_1 \subseteq M_1$ and $N_1/\{0\} \cong M_1/\{0\}$, we have $N_1 = M_1$. Repeating the same argument, we have $N = N_n = M_n = M$, a contradiction. We have proved **statement 1.3**.

Now, let $M'_0 \subset \cdots \subset M'_r$ be some composition series of M . The proof then follows from using **statement 1.3** to deduce

$$l(M) = l(M'_r) > \cdots > l(M'_0) = 0 \implies r \leq l(M)$$

■

Because of **Theorem 1.9.1**, we may well define the **length** $l(M)$ of module. For obvious reason, if module M has no composition series, we say M has infinite length and write $l(M) = \infty$. Clearly, if M is of finite length, then M is both Noetherian and Artinian. Conversely, if M is both Noetherian and Artinian, then by the maximal element definition of Noetherian, there exists a decreasing sequence $M = M_0 \supset M_1 \supset M_2 \supset \cdots$, which by d.c.c. must be finite.

Theorem 1.9.2. (Artinian and Noetherian are equivalent for vector space) Let k be some field, and V some k -vector space. The following are equivalent:

- (i) V is finite dimensional.
- (ii) V is of finite length.
- (iii) V is Noetherian.
- (iv) V is Artinian.

Moreover, $l(V) = \dim(V)$ in such case.

Proof. (i) \implies (ii) \implies (iii) and (ii) \implies (iv) are clear. It remains to prove (iii) \implies (i) and (iv) \implies (i). Assume for a contradiction that $\{v_i \in V : i \in \mathbb{N}\}$ is linearly independent. The contradiction to Noetherian of V then occurs at $(\text{span}\{v_i \in V : i \leq n\})_n$ doesn't stop growing strictly, and the contradiction to Artinian of V then occurs at $(\text{span}\{v_i \in V : i \geq n\})_n$ strictly decrease infinitely. ■

For usage in [section on Artin ring](#), we give a corollary.

Corollary 1.9.3. (Artinian is equivalent to Noetherian in the class of rings whose zero ideal is some finite product of maximal ideals) Let A be a ring with $0 = \mathfrak{m}_1 \cdots \mathfrak{m}_n$, where \mathfrak{m}_i are maximal. We have

$$A \text{ is Noetherian} \iff A \text{ is Artinian}$$

Proof. WLOG, we only prove (\implies). The proof is done by induction. Write $\mathfrak{a}_i \triangleq \mathfrak{m}_1 \cdots \mathfrak{m}_i$, where $\mathfrak{a}_0 \triangleq A$ and $\mathfrak{a}_n = 0$. Clearly, \mathfrak{a}_n is Artinian as an A -module. We now show \mathfrak{a}_{n-1} is also Artinian as an A -module. Consider the short exact sequence of A -module:

$$0 \longrightarrow \mathfrak{a}_n \longrightarrow \mathfrak{a}_{n-1} \longrightarrow \mathfrak{a}_{n-1}/\mathfrak{a}_n \longrightarrow 0$$

By [proposition 1.8.4](#), to prove \mathfrak{a}_{n-1} is Artinian as an A -module, we only have to show $\mathfrak{a}_{n-1}/\mathfrak{a}_n$ is Artinian as an A -module. Before such, we first have to make two remarks:

- (i) $\mathfrak{a}_{n-1}/\mathfrak{a}_n$ forms an A/\mathfrak{m}_n -vector space under obvious assignment of scalar product.
- (ii) For each $E \subseteq \mathfrak{a}_{n-1}/\mathfrak{a}_n$, E forms an A -submodule if and only if E forms an A/\mathfrak{m}_n -submodule.

Now, by [proposition 1.8.5](#) we know $\mathfrak{a}_n/\mathfrak{a}_{n-1}$ is Noetherian as an A -module, which with remark (ii) implies that $\mathfrak{a}_n/\mathfrak{a}_{n-1}$ is Noetherian as an A/\mathfrak{m}_n -module, which further implies by [theorem 1.9.2](#) that $\mathfrak{a}_n/\mathfrak{a}_{n-1}$ is Artinian as an A/\mathfrak{m}_n -module, which further further implies with remark (ii) that, indeed, $\mathfrak{a}_n/\mathfrak{a}_{n-1}$ is Artinian as an A -module.

We have shown \mathfrak{a}_{n-1} is Artinian as an A -module, and if we apply the same argument¹⁵ short exact sequence of A -module:

$$0 \longrightarrow \mathfrak{a}_{n-1} \longrightarrow \mathfrak{a}_{n-2} \longrightarrow \mathfrak{a}_{n-2}/\mathfrak{a}_{n-1} \longrightarrow 0$$

We see \mathfrak{a}_{n-2} is also Artinian as an A -module. Continuing the same process, we see that indeed $A = \mathfrak{a}_0$ is Artinian. (as an A -module) ■

¹⁵Replace A/\mathfrak{m}_n with A/\mathfrak{m}_{n-1}

Chapter 2

Valuation Ring and DVR

2.1 Localization of ideals

Let $I \subseteq A$ be some ideal, clearly its extension is the **localization of I by S** defined by $S^{-1}I = \{\frac{i}{s} \in S^{-1}A : i \in I\}$. We use the notation $S(I)$ to denote the contraction of $S^{-1}I$. For [the section on uniqueness of primary decomposition](#), we first prove some basic properties of localization of ideals.

Theorem 2.1.1. (Properties of localization of ideals) Let A be a ring, and let S be some multiplicatively closed subset of A .

(a) If I is an ideal in A , then

$$S(I) = \bigcup_{s \in S} (I : s)$$

(b) If I is an ideal in A , then

$$\sqrt{S^{-1}I} = S^{-1}\sqrt{I}$$

(c) If I_1, \dots, I_n are ideals in A , then

$$S^{-1}(I_1 \cap \dots \cap I_n) = S^{-1}I_1 \cap \dots \cap S^{-1}I_n$$

Proof. We first prove part (a). Let $t \in (I : s)$ for some s . Because $\frac{t}{1} = \frac{st}{s} \in S^{-1}I$, we see $t \in I^{ec}$. Let $t \in I^{ec}$, so $\frac{t}{1} = \frac{i}{s}$ for some $i \in I, s \in S$. Observe $tss' = is' \in I$ for some s' to conclude $t \in (I : ss')$, and we are done. We now prove part (b). It is clear that $S^{-1}\sqrt{I} \subseteq \sqrt{S^{-1}I}$. Let $\frac{a}{s} \in \sqrt{S^{-1}I}$, so $\frac{a^n}{s^n} = \frac{i}{s'}$ for some n, i, s' . Let s'' satisfies $a^n s' s'' = i s^n s'' \in I$. Observations of $\frac{a}{s} = \frac{a s' s''}{s s' s''}$ and $a s' s'' \in \sqrt{I}$ finish the proof. We now prove part (c). It is clear that $S^{-1}(I_1 \cap \dots \cap I_n) \subseteq S^{-1}I_1 \cap \dots \cap S^{-1}I_n$. Let

$\frac{a}{s} \in S^{-1}I_1 \cap \cdots \cap S^{-1}I_n$. For each $j \in \{1, \dots, n\}$, we may find $s_j, s'_j \in S, i_j \in I$ such that $as_js'_j = si_js'_j \in I_j$. Writing

$$\frac{a}{s} = \frac{as_1s'_1s_2s'_2 \cdots s_ns'_n}{ss_1s'_1s_2s'_2 \cdots s_ns'_n} \in S^{-1}(I_1 \cap \cdots \cap I_n)$$

and we are done. ■

2.2 Uniqueness of Primary Decomposition

Let A be a ring. We say a proper ideal \mathfrak{q} is **primary** if for each $xy \in \mathfrak{q}$, either $x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some $n > 0$.

Equivalent Definition 2.2.1. (Primary ideal) Let A be a ring and $\mathfrak{q} \subseteq A$ be an ideal. The followings are equivalent:

- (i) \mathfrak{q} is primary.
- (ii) Every zero divisor of A/\mathfrak{q} is nilpotent.

Proof. Unroll the definition. ■

Clearly, the radical $\mathfrak{p} = \sqrt{\mathfrak{q}}$ of a primary ideal \mathfrak{q} is prime. In such case, we say \mathfrak{q} is **\mathfrak{p} -primary**. A **primary decomposition** of an ideal \mathfrak{a} is an expression of \mathfrak{a} as a finite intersection of primary ideals:

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

Such primary decomposition is said to be **irredundant** if $\sqrt{\mathfrak{q}_i}$ are all distinct and no \mathfrak{q}_i is unnecessary in the sense that:

$$\bigcap_{j \neq i} \mathfrak{q}_j \not\subseteq \mathfrak{q}_i, \quad \text{for all } i.$$

An ideal \mathfrak{a} is said to be **decomposable** if there exists some primary decomposition of \mathfrak{a} . Because finite intersection of \mathfrak{p} -primary ideals is again \mathfrak{p} -primary¹, every decomposable ideal has an irredundant primary decomposition.

Theorem 2.2.2. (First uniqueness theorem for irredundant primary decomposition) Given some irredundant primary decomposition $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$, we have

$$\{\sqrt{\mathfrak{q}_i} : 1 \leq i \leq n\} = \text{Spec}(A) \cap \left\{ \sqrt{(\mathfrak{a} : x)} \subseteq A : x \in A \right\} \quad (2.1)$$

Proof. Before showing that both sides of **equation 2.1** are subsets of each other, we first make the following observation. For all $x \in A$, clearly:

$$(\mathfrak{a} : x) = \left(\bigcap \mathfrak{q}_i : x \right) = \bigcap (\mathfrak{q}_i : x)$$

¹In general, finite intersection of primary ideals need not be primary. To prove finite intersection of \mathfrak{p} -primary ideals are \mathfrak{p} -primary, the first step is to prove the radical of the finite intersection is \mathfrak{p} .

Therefore,

$$\sqrt{(\mathfrak{a} : x)} = \bigcap \sqrt{(\mathfrak{q}_i : x)} = \bigcap_{k: x \notin \mathfrak{q}_k} \sqrt{\mathfrak{q}_k} \quad (2.2)$$

where the last equality is justified by:

$$x \in \mathfrak{q}_i \implies (\mathfrak{q}_i : x) = A, \quad \text{and } x \notin \mathfrak{q}_i \implies \sqrt{(\mathfrak{q}_i : x)} = \sqrt{\mathfrak{q}_i}$$

We now prove that the left hand side of [equation 2.1](#) is a subset of the right hand side. Fix i . By irredundancy of the decomposition, there exists some $x \in A$ such that x belongs to all \mathfrak{q}_j except \mathfrak{q}_i . This x by [equation 2.2](#) must satisfies:

$$\sqrt{\mathfrak{q}_i} = \sqrt{(\mathfrak{a} : x)}$$

Noting that $\sqrt{\mathfrak{q}_i}$ must be prime due to \mathfrak{q}_i being primary, we have shown the left hand side of [equation 2.1](#) is a indeed a subset of the right hand side.

Now, suppose for some $x \in A$ that $\sqrt{(\mathfrak{a} : x)}$ is prime. Because prime ideal must be proper, we know there must exists some k such that $x \notin \mathfrak{q}_k$. By [equation 2.2](#), to finish the proof, we only need to show $\sqrt{\mathfrak{q}_k} \subseteq \sqrt{(\mathfrak{a} : x)}$ for some k such that $x \notin \mathfrak{q}_k$. Assume not for a contradiction. Then for all k such that $x \notin \mathfrak{q}_k$, there exists $y_k \in \sqrt{\mathfrak{q}_k} - \sqrt{(\mathfrak{a} : x)}$. The product of these y_k is an element of $\bigcap \sqrt{\mathfrak{q}_k}$, thus an element of $\sqrt{(\mathfrak{a} : x)}$. This with $\sqrt{(\mathfrak{a} : x)}$ being prime shows that $y_k \in \sqrt{(\mathfrak{a} : x)}$ for some k , a contradiction. ■

Let $\mathfrak{a} \subseteq A$ be an ideal. A **minimal prime ideal over \mathfrak{a}** is a minimal element in the set of prime ideals that contains \mathfrak{a} . Note that by [definition of radical](#), a minimal prime ideal over \mathfrak{a} is also is a minimal prime ideal over $\sqrt{\mathfrak{a}}$.

Equivalent Definition 2.2.3. (Minimal prime ideals over decomposable ideals)

Let A be a ring and $\mathfrak{a} \subseteq A$ be a decomposable ideal with irredundant primary decomposition $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$. Let $\{\sqrt{\mathfrak{q}_1}, \dots, \sqrt{\mathfrak{q}_n}\}$ be the collection of minimal elements of $\{\sqrt{\mathfrak{q}_1}, \dots, \sqrt{\mathfrak{q}_n}\}$. The followings are equivalent:

- (i) \mathfrak{p} is a minimal prime ideal over \mathfrak{a} .
- (ii) $\mathfrak{p} \in \{\sqrt{\mathfrak{q}_1}, \dots, \sqrt{\mathfrak{q}_n}\}$

Proof. (i) \implies (ii): Because \mathfrak{p} contains $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$, we know

$$\sqrt{\mathfrak{q}_1} \cap \cdots \cap \sqrt{\mathfrak{q}_n} \subseteq \sqrt{\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p}$$

If none of $\sqrt{\mathfrak{q}_i}$ is contained by \mathfrak{p} , then we can cause a contradiction by considering $\prod y_i$ where $y_i \in \sqrt{\mathfrak{q}_i} - \mathfrak{p}$.

(ii) \implies (i): Let $1 \leq i \leq m$. If $\sqrt{\mathfrak{q}_i}$ is not minimal, then by (i) \implies (ii), $\sqrt{\mathfrak{q}_i} \supseteq \sqrt{\mathfrak{q}_j}$ for some $1 \leq j \leq m$ that isn't i , contradicting to the construction that $\{\sqrt{\mathfrak{q}_1}, \dots, \sqrt{\mathfrak{q}_m}\}$ are minimal among $\{\sqrt{\mathfrak{q}_1}, \dots, \sqrt{\mathfrak{q}_n}\}$. \blacksquare

The followings have not been cleaned yet!!!!

Because of **the first uniqueness theorem**, we may well define the **inner spectrum** of decomposable ideal I , independent of choice of irredundant decomposition, to be

$$\{\sqrt{Q_1}, \dots, \sqrt{Q_n}\}$$

where

$$I = \bigcap_{i=1}^n Q_i \text{ is some irredundant primary decomposition.}$$

Given such irredundant primary decomposition, we say Q_i is an **isolated primary component** if $\sqrt{Q_i}$ is minimal in the inner spectrum.

Lemma 2.2.4. (preparation lemma for second uniqueness theorem) Let S be a multiplicatively closed subset of A , and let Q be a P -primary ideal. If S and P are disjoint, then $S^{-1}Q$ is $S^{-1}P$ -primary and $S(Q) = Q$. If S and P meet, then $S^{-1}Q = S^{-1}A$.

Proof. Suppose S and P are disjoint. Clearly we have $Q \subseteq S(Q)$, so to show $S(Q) = Q$, we only have to show $S(Q) \subseteq Q$. Let $a \in S(Q)$. The first part of **Theorem 2.1.1** states that $a \in (Q : s)$ for some $s \in S$. Because $Q \subseteq P$, this implies $a \in Q$. We have shown $S(Q) = Q$. Note that the second part of **Theorem 2.1.1** states that

$$\sqrt{S^{-1}Q} = S^{-1}\sqrt{Q} = S^{-1}P$$

so for the case when S and P are disjoint, it only remains to prove $S^{-1}Q$ is indeed primary, which is routine and even unnecessary for the **Second uniqueness theorem below**.

Suppose $s \in S \cap P$. Let $s^n \in Q$. The fact that $S^{-1}Q = S^{-1}A$ follows from the fact $\frac{s^n}{1}$ is a unit with inverse $\frac{1}{s^n}$. \blacksquare

Theorem 2.2.5. (Second uniqueness theorem for isolated primary component) The isolated primary components of a decomposable ideal I is uniquely determined by I , independent of the irredundant decomposition.

Proof. Let P be a minimal element of the inner spectrum of I , and let $I = \bigcap_{i=1}^n Q_i$ be an arbitrary irredundant primary decomposition, where $\sqrt{Q_1} = P$. Clearly $S \triangleq A \setminus P$ is multiplicatively closed. Because the definition of S is independent of the choice of the primary decomposition, we are only required to prove the goal

$$Q_1 = S(I)$$

Because S and P are disjoint, we may apply [Lemma 2.2.4](#) to reduce this goal into

$$S^{-1}Q_1 = S^{-1}I$$

Noting that $\sqrt{Q_i}$ meets $S = A \setminus \sqrt{Q_1}$ for every $i > 1$ due to the minimality of $\sqrt{Q_1}$, we conclude our proof using [Lemma 2.2.4](#) and the third part of [Theorem 2.1.1](#):

$$S^{-1}I = \bigcap_{i=1}^n S^{-1}Q_i = S^{-1}Q_1$$

■

2.3 Existence of Primary Decomposition in Noetherian ring

Let A be a ring, and let $I \subseteq A$ be some ideal. We say I is **irreducible** if whenever I is expressed as an intersection of two ideals, I equals to one of them. Clearly, to show every ideal in Noetherian ring is decomposable, we only need to show the following two lemmas.

Lemma 2.3.1. In Noetherian ring A , every ideal is a finite intersection of irreducible ideals.

Proof. Assume not for a contradiction. Let I be a maximal element of the collection Σ of all ideals that can not be expressed as finite intersections of irreducible ideals. Clearly, I must be reducible, so there exists some $I = J_1 \cap J_2$ such that $I \subset J_1$ and $I \subset J_2$. Because $J_1, J_2 \notin \Sigma$, we may express them both as finite intersection of irreducible ideals. This implies that we may express I as a finite intersection of irreducible ideals, a contradiction. ■

Lemma 2.3.2. In Noetherian ring A , every irreducible ideal is primary.

Proof. Let $I \subseteq A$ be irreducible. Clearly, the zero ideal in A/I is irreducible, and if the zero ideal in A/I is primary, then I is also primary. Because of such, we may WLOG suppose I is zero. Let $xy = 0$ and $y \neq 0$. We are required to show $x^n = 0$. Clearly we have the chain $\text{Ann}(x) \subseteq \text{Ann}(x^2) \subseteq \dots$, and by a.c.c., there exists some n such that $\text{Ann}(x^n) = \text{Ann}(x^{n+1}) = \dots$. We now show

$$\langle x^n \rangle \cap \langle y \rangle = 0 \tag{2.3}$$

Let $a \in \langle x^n \rangle \cap \langle y \rangle$. Because $a \in \langle y \rangle$ and $xy = 0$, we know $ax = 0$. Writing $a = bx^n$, we now see $b \in \text{Ann}(x^{n+1}) = \text{Ann}(x^n)$. This implies $a = bx^n = 0$. We have shown [Equation 2.3](#).

Finally, because the zero ideal is irreducible, we must have $\langle x^n \rangle = 0$ or $\langle y \rangle = 0$. Because $y \neq 0$, we may conclude $x^n = 0$. ■

2.4 Artin Rings

Set theoretically similar to **equivalent definition of Noetherian**, by axiom of choice, we have

Theorem 2.4.1. (Equivalent Definition of Artinian) Let M be a module. We have

- (a) M is Artinian.
- (b) Every nonempty collection of submodules of M has a minimal element.

From this definition, we see that Artin ring can only have finite number of maximal ideals.

Corollary 2.4.2. (Artin ring has only a finite number of maximal ideals) If A is an Artin ring, then

A only has a finite number of maximal ideals.

Proof. Let Σ be the collection of all finite intersection of maximal ideals of A , and let $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \in \Sigma$ be minimal. We claim that $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ are the only maximal ideals of A . To prove this, we only have to prove that for each maximal ideal \mathfrak{m} , there exist some i such that $\mathfrak{m}_i \subseteq \mathfrak{m}$, and it will follow that $\mathfrak{m} = \mathfrak{m}_i$.

Assume not for a contradiction. Let $x_i \in \mathfrak{m}_i - \mathfrak{m}$ for all i . We see $\prod x_i \in \prod \mathfrak{m}_i \subseteq \bigcap \mathfrak{m}_i \subseteq \mathfrak{m}$, where the last set inclusion follows from minimality of $\bigcap \mathfrak{m}_i \in \Sigma$. Because \mathfrak{m} is prime, we see $x_i \in \mathfrak{m}$ for some i , a contradiction to the construction of x_i . ■

Theorem 2.4.3. (Nilradical in Artin ring is nilpotent) If ring A is Artinian, then

$$(\text{Nil}(A))^k = 0 \text{ for some } k.$$

Proof. Let $\mathfrak{a} \triangleq (\text{Nil}(A))^k = (\text{Nil}(A))^{k+1} = \cdots$. Assume for a contradiction that $\mathfrak{a} \neq 0$. Letting Σ be the collection of all ideals \mathfrak{b} such that $\mathfrak{a}\mathfrak{b} \neq 0$, we see Σ is nonempty since $\mathfrak{a} \in \Sigma$, and therefore by **equivalent definition of Artinian** there exists minimal $\mathfrak{c} \in \Sigma$. Picking $x \in \mathfrak{c}$ such that $x\mathfrak{b} \neq 0$, we see by minimality of \mathfrak{c} that $\mathfrak{c} = \langle x \rangle$. Checking that $(x\mathfrak{a})\mathfrak{a} = x\mathfrak{a}^2 = x\mathfrak{a} \neq 0$ and $x\mathfrak{a} \subseteq \mathfrak{a}$, again by minimality of $\langle x \rangle$, we see $x\mathfrak{a} = \langle x \rangle$. This implies $x = xy$ for some $y \in \mathfrak{a} \supseteq \text{Nil}(A)$, and therefore $x = xy = xy^2 = \cdots = xy^n = 0$ for some large enough n , a contradiction to construction of x . ■

Given ring A , we define its **Krull dimension** to be the supremum of the length of all chains of prime ideals in A . Albeit tempting to treat Artinian a property symmetry to Noetherian, Artin rings is in fact a subclass of Noether rings.

Theorem 2.4.4. (Actual characterization of Artin Rings) Given some ring A ,

$$A \text{ is Artin} \iff A \text{ is Noetherian with } \text{Krudim}(A) = 0$$

Proof. (\implies): We first prove $\text{Krudim}(A) = 0$. Note that $\text{Krudim}(A) = 0$ means exactly that all prime ideal of A are maximal. Let $\mathfrak{p} \subseteq A$ be prime, and $x \neq 0 \in B \triangleq A/\mathfrak{p}$. Because B is Artinian, there exists some n such that $\langle x^n \rangle = \langle x^{n+1} \rangle$, which implies

$$x^n = x^{n+1}y, \quad \text{for some } y \in B$$

Because $x \neq 0$ and B is an integral domain, this tell us $xy = 1$. We have shown that B is a field, i.e., \mathfrak{p} is indeed maximal.

Let $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ be the maximal ideals of A . Because every maximal ideal in Artin ring is prime and $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ are the only maximal ideal of A , we see that $\prod \mathfrak{m}_i^k \subseteq (\bigcap \mathfrak{m}_i)^k = (\text{Nil}(A))^k = 0$ for some k by [Theorem 2.4.3](#). It then follows from [Corollary 1.9.3](#) that A is indeed Noetherian.

(\impliedby): Because A is Noetherian, we know the zero ideal of A has an irredundant primary decomposition $0 = \bigcap_{i=1}^n \mathfrak{q}_i$. Let \mathfrak{p} be a prime ideal. Because $\bigcap_{i=1}^n \mathfrak{q}_i \subseteq \mathfrak{p}$, we know $\mathfrak{q}_i \subseteq \mathfrak{p}$ for some i^2 , which by definition of radical implies that $\sqrt{\mathfrak{p}_i} \subseteq \mathfrak{p}$. We have shown $\text{Nil}(A) = \bigcap_{i=1}^n \sqrt{\mathfrak{q}_i}$. Letting $\mathfrak{a} = 0$ in [Corollary 1.8.2](#), we now see

$$\prod_{i=1}^n (\sqrt{\mathfrak{q}_i})^k \subseteq \left(\bigcap_{i=1}^n \sqrt{\mathfrak{q}_i} \right)^k = (\text{Nil}(A))^k = 0$$

Because $\text{Krudim}(A) = 0$, we know $\sqrt{\mathfrak{q}_i}$ are all maximal ideals. It then follows from [Corollary 1.9.3](#) that A is Artinian. ■

Having zero Krull dimension together with being local form a very lethal weapon. A ring A satisfies A local and $\text{Kudim}(A) = 0$ if and only if A contains exactly one prime ideal, i.e., its nilradical. From this point of view, [Theorem 2.4.4](#) is very strong, which you can already guess from its long proof. Indeed, [Theorem 2.4.4](#) give us the following two useful corollaries, which are all later used to establish the [equivalent characterization of DVR](#).

Corollary 2.4.5. (Powers of the maximal ideal of Noetherian local rings) Given Noetherian local ring (A, \mathfrak{m}) , exactly one of the following two statements is true:

- (a) $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ for all n .
- (b) $\mathfrak{m}^n = 0$ for some n , and A is an Artin ring.

Proof. Suppose $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ for some n . Because A is Noetherian and local, we may apply [Nakayama Lemma](#) to see $\mathfrak{m}^n = \mathfrak{m}^{n+1} = 0$. To show A is indeed Artinian, by [Theorem 2.4.4](#), we only have to prove that \mathfrak{m} is the only prime ideal of A . Too see thus, just observe $\mathfrak{m} \subseteq \sqrt{\mathfrak{m}^n} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p}$ if \mathfrak{p} is prime. ■

²Otherwise you may cause a contradiction by considering $\prod x_i$ where $x_i \in \mathfrak{q}_i - \mathfrak{p}$

Corollary 2.4.6. (Powers of the maximal ideal of Artin local ring) Consider the Artin local ring (A, \mathfrak{m}, k) . We have

A is a PID with every proper nonzero ideal being some power of \mathfrak{m} $\iff \dim_k(\mathfrak{m}/\mathfrak{m}^2) \leq 1$

Proof. (\implies) : This follows from noting that if we let x be the generator of \mathfrak{m} , then $[x]$ spans $\mathfrak{m}/\mathfrak{m}^2$ over k .

(\impliedby) : If $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 0$, then $\mathfrak{m} = \mathfrak{m}^2$, so by [Nakayama Lemma³](#), $\mathfrak{m} = 0$, implying A is a field. Suppose $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$ and $[x] \in \mathfrak{m}/\mathfrak{m}^2$ spans $\mathfrak{m}/\mathfrak{m}^2$ over k . We first show that indeed, \mathfrak{m} as an ideal of A is generated by just x .

Let $y \in \mathfrak{m}$. Because $[x] \in \mathfrak{m}/\mathfrak{m}^2$ spans $\mathfrak{m}/\mathfrak{m}^2$ over k . We know $[y] = [ax] \in \mathfrak{m}/\mathfrak{m}^2$ for some $a \in A$. This implies $y - ax = m_1 m'_1 + \dots + m_n m'_n$ for some $m_i, m'_i \in \mathfrak{m}$, which implies $[y] = [y - ax] \in \mathfrak{m}/\langle x \rangle$ is also an element of $\mathfrak{m}(\mathfrak{m}/\langle x \rangle)$. We have shown $\mathfrak{m}(\mathfrak{m}/\langle x \rangle) = \mathfrak{m}/\langle x \rangle$. It now follows from [Nakayama Lemma⁴](#) that $\mathfrak{m}/\langle x \rangle = 0$, i.e., $\mathfrak{m} = \langle x \rangle$ indeed.

Now, let $\mathfrak{a} \subset A$ be a proper nonzero ideal.⁵ [Theorem 2.4.4](#) tell us that $\text{Krudim}(A) = 0$, and so $\mathfrak{m}^n = \text{Nil}(A)^n = 0$ for some n by [Theorem 2.4.3](#). Let r satisfies $\mathfrak{a} \subseteq \mathfrak{m}^r, \mathfrak{a} \not\subseteq \mathfrak{m}^{r+1}$. By construction, there exist some $y \in \mathfrak{a}$ such that $y = ax^r$ for some $a \in A$ and $y \notin \langle x^{r+1} \rangle$. We now see this a satisfies $a \notin \langle x \rangle = \mathfrak{m}$, implying a is a unit. This shows $x^r = ya^{-1} \in \mathfrak{a}$. We have shown $\mathfrak{a} = \langle x^r \rangle$, as desired. ■

³Because A is [Noetherian](#), we know \mathfrak{m} is finitely generated.

⁴ $\mathfrak{m}/\langle x \rangle$ is finitely generated because A is [Noetherian](#).

⁵If $\mathfrak{a} = A$, then $\mathfrak{a} = \langle 1 \rangle$.

2.5 Equivalent Characterizations of DVR

Let K be a field. A **discrete valuation** $\nu : K \rightarrow \Gamma \cup \{\infty\}$ is a valuation such that $\Gamma \cong \mathbb{Z}$ as totally ordered abelian group. An integral domain D is a **discrete valuation ring** if $D = \{x \in \text{Frac}(D) : \nu(x) \geq 0\}$ for some nontrivial discrete valuation $\nu : \text{Frac}(D) \rightarrow \mathbb{Z} \cup \{\infty\}$. Because every ideal $\mathfrak{a} \subseteq D$ is of the form: ⁶

$$\mathfrak{a} = \{x \in D : \nu(x) \geq \min \nu(\mathfrak{a})\}$$

We see that the collection of the ideals in DVRs is exactly $\{\mathfrak{a}_k : k \in \mathbb{N}\}$ where

$$\mathfrak{a}_k = \{x \in D : \nu(x) \geq pk\} = \langle x^k \rangle \text{ for any } \nu(x) = p \triangleq \min \{\nu(d) \in \mathbb{N} : d^{-1} \notin D\} \quad (2.4)$$

In fact, we can conversely characterize DVRs using these good properties.

Theorem 2.5.1. (Equivalent Characterizations of DVR: part 1) Given an 1-Krull-dimensional Noetherian local domain (D, \mathfrak{m}, k) , the following are equivalent:

- (i) D is a DVR.
- (ii) D is integrally closed.
- (iii) \mathfrak{m} is principal.
- (iv) $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$.
- (v) Every proper nonzero ideal of D is a power of \mathfrak{m} .
- (vi) There exists $x \in D$ such that every nonzero ideal is of the form $\langle x^s \rangle$, $s \geq 0$.

Proof. Before we start going the rounds, we shall make the following remark

- (A) Because D is an 1-Krull-dimensional local domain, D has only two prime ideals, i.e., the zero ideal and \mathfrak{m} .
- (B) Because D is Noetherian, by remark (A) and **Corollary 1.8.2**, for every proper nonzero ideal $\mathfrak{a} \subseteq D$, we have some n that satisfies $\mathfrak{m}^n \subseteq \mathfrak{a}$ and $\mathfrak{m}^{n-1} \not\subseteq \mathfrak{a}$.
- (C) Because $\text{Krudim}(D) = 1$ and D is Noetherian local, $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ for all $n \geq 0$ by **Theorem 2.4.6**.

We may now start going rounds. (i) \implies (ii) follows from the fact **valuation ring are integrally closed**.

⁶To see the " \supseteq ", let $a \in \mathfrak{a}$ satisfies $\nu(a) = \min \nu(\mathfrak{a})$ and observe for all $x \in D$ such that $\nu(x) \geq \nu(a)$, we have $x = (xa^{-1})a \in \mathfrak{a}$ since $\nu(xa^{-1}) = \nu(x) - \nu(a) \geq 0 \implies xa^{-1} \in D$

(ii) \implies (iii): Let $a \neq 0 \in \mathfrak{m}$. By remark (B), there exists some n such that $\mathfrak{m}^n \subseteq \langle a \rangle$ and $\mathfrak{m}^{n-1} \not\subseteq \langle a \rangle$. Picking $b \in \mathfrak{m}^{n-1} - \langle a \rangle$, and defining $x \triangleq \frac{a}{b} \in \text{Frac}(D)$, clearly we have $x^{-1} \notin D$, so by premise, x^{-1} is not integral over D . Therefore, $x^{-1}\mathfrak{m} \not\subseteq \mathfrak{m}$ ⁷. This, together with the fact that $x^{-1}\mathfrak{m} = a^{-1}(b\mathfrak{m}) \subseteq \mathfrak{m}^n \subseteq a^{-1}\langle a \rangle \subseteq A$ by construction, implies $x^{-1}\mathfrak{m} = A$, since $\mathfrak{m} \neq 0$ is the only maximal ideal of A . In conclusion, one can now finish the proof by checking, indeed, $\mathfrak{m} = xA = \langle x \rangle$.

(iii) \implies (iv): If \mathfrak{m} is generated by x over D , then $\mathfrak{m}/\mathfrak{m}^2$ is spanned by $[x] \in \mathfrak{m}/\mathfrak{m}^2$ over k , and so by remark (C), we have $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$.

(iv) \implies (v): Let $\mathfrak{a} \subset D$ be some proper nonzero ideal. By remark (B), there exists some n that satisfies $\mathfrak{m}^n \subseteq \mathfrak{a}$. By [ring correspondence theorem](#) and [theorem 1.8.5](#), A/\mathfrak{m}^n is Noetherian local, and thus by [corollary 2.4.6](#) Artin. Now, checking that indeed the square of image of \mathfrak{m} is the image of \mathfrak{m}^2 under quotient map $A \longrightarrow A/\mathfrak{m}^n$, and checking that $\dim_{(A/\mathfrak{m}^n)/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$, we may apply [corollary 2.4.6](#) to conclude that \mathfrak{a} is a power of \mathfrak{m} in A/\mathfrak{m}^n . Now, says $\mathfrak{a} = \mathfrak{m}^r$ in A/\mathfrak{m}^n , because the quotient map $A \longrightarrow A/\mathfrak{m}^n$ maps \mathfrak{m}^r to the r -th power of image of \mathfrak{m} , we see by [ring correspondence theorem](#) that indeed $\mathfrak{a} = \mathfrak{m}^r$ in A .

(v) \implies (vi): By remark (C), there exists $x \in \mathfrak{m} - \mathfrak{m}^2$, and by premise, $\langle x \rangle = \mathfrak{m}^r$ for some r . Because if $r > 1$, then $x \in \mathfrak{m}^r \subseteq \mathfrak{m}^2$, we see $r = 1$. It is then easy to check $\mathfrak{m}^s = \langle x^s \rangle$ for all $s \in \mathbb{N}$.

(vi) \implies (i): Let $\mathfrak{m} \triangleq \langle x \rangle$. For all $y \in D$, one define $\nu(y) \triangleq n$ where $n \geq 0$ is the smallest nonnegative integer such that $y \notin \langle x^n \rangle$. To finish the proof one may check $\nu(yz^{-1}) \triangleq \nu(y) - \nu(z)$ well define a discrete valuation on $\text{Frac}(D)$. ■

⁷Otherwise, we may set $A \triangleq D$, $\mathfrak{a} \triangleq D$, $M \triangleq \mathfrak{m}$, and $\phi(m) \triangleq x^{-1}m$ in [Cayley-Hamilton Theorem for finitely generated module](#) to deduce x^{-1} is integral over D . Note that $\mathfrak{m} \neq 0$ because $\text{Krudim}(D) = 1$.

2.6 UFT for ideals in 1-Krull-dimensional Noetherian domain

Before the main course, we first develop some basic notion. We say two ideals are **coprime** if their sum equals to the whole ring. Note that two prime ideals need not be coprime. If K is a field, then $\langle x \rangle, \langle y \rangle$ are not coprime in $K[x, y]$.

Proposition 2.6.1. (Product of coprime ideals is the intersection) Let I_k be a finite collection of pairwise coprime ideals. We have $\prod I_k = \bigcap I_k$.

Proof. The proof relies on induction of total number of the pairwise coprime ideals. The base case is when there are only two, says, I and J . Clearly $IJ \subseteq I \cap J$. To prove the converse, observe for $c \in I \cap J$, there exists $1 = i + j$ so that $c = ci + cj$, where $ci, cj \in I \cap J$. ■

Theorem 2.6.2. (UFT for ideals in Noetherian domain of Krull Dimension 1) If A is a Noetherian domain of Krull dimension 1, then every nonzero ideal $I \subseteq A$ can be uniquely expressed as a product of primary ideals whose radicals are all distinct.

Proof. We first note that

- (i) Because $\text{Krudim}(A) = 1$, every prime ideal in A is maximal.
- (ii) Two distinct maximal ideals are always coprime.
- (iii) $\sqrt{J}, \sqrt{J'}$ coprime $\implies J, J'$ coprime.⁸

For existence, first observe that **because A is Noetherian, I has an irredundant primary decomposition $I = \bigcap Q_i$** . Then, by (i), (ii), (iii), and **Proposition 2.6.1**, we have

$$I = \bigcap Q_i = \prod Q_i$$

To see $\sqrt{Q_i}$ are indeed distinct, just note that the primary decomposition $I = \bigcap Q_i$ is irredundant. For uniqueness, suppose $I = \prod Q_i = \prod Q'_i$, where $\sqrt{Q_i}$, just like $\sqrt{Q_j}$, are distinct and prime. Again, by (i), (ii), (iii), and **Proposition 2.6.1**, we have

$$I = \prod Q_i = \bigcap Q_i = \prod Q'_i = \bigcap Q'_i$$

Because $\sqrt{Q_i}$ are distinct, by **first uniqueness theorem for primary decomposition**, we know none of Q_i are redundant, i.e., $I = \bigcap Q_i$ is an irredundant primary decomposition. Same argument shows that $I = \bigcap Q'_i$ is also an irredundant primary decomposition. The fact that these two primary decomposition are identical up to a renewal of index then follows from

⁸ $x + y = 1, x^n \in J, y^k \in J' \implies 1 = 1^{n+k} = (x + y)^{n+k} \in J + J'$.

second uniqueness theorem for primary decomposition and noting that every $\sqrt{Q_i}, \sqrt{Q'_i}$ are isolated because by (i) they are all maximal. ■

2.7 Fractional Ideal

Let A be an integral domain, and $K \triangleq \text{Frac}(A)$. Given two A -submodule $N, M \subseteq K$, we define their **product** and **quotient** and the same way we define product and quotient⁹ for ideals of a ring:

$$NM \triangleq \left\{ \sum_{\text{finite}} nm \in K : n \in N \text{ and } m \in M \right\} \text{ and } (N : M) \triangleq \{x \in K : xM \subseteq N\}$$

Clearly, A -submodules of K are indeed closed under these two binary operation, and moreover the product for A -submodule of K is associative, commutative, and has a unique identity A , forming a commutative monoid¹⁰.

A **fractional ideal** of A is an A -submodule $M \subseteq K$ such that $xM \subseteq A$ for some $x \neq 0 \in A$. Clearly, fractional ideals need not be subsets of A , so fractional ideals are not always ideals of A ¹¹. If there is need to talk about fractional ideal, some people use the term **integral ideal** to refer to an ordinary ideal. Clearly the set of fractional ideal is closed under product and contains A , so the set of fractional ideals of A is a sub-monoid of the commutative monoid of A -submodules of K .

An **invertible ideal** of A is an A -submodule of $M \subseteq A$ such that $NM = A$ for some A -submodule $N \subseteq K$. In other words, it is the set of all elements of the commutative monoid of A -submodule of K that has an inverse. From this point of view, it is clear that the set of invertible ideal is closed under product, and thus forms a group¹².

Proposition 2.7.1. (Form of the inverse of invertible ideal) Let A be an integral domain, and $K \triangleq \text{Frac}(A)$. If M is invertible with inverse N , then $N = (A : M)$.

Proof. Because $MN = A$ and the product is associative, we know $(A : M) \subseteq (A : M)A = (A : M)MN$, which give us the desired inequality:

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

finishing the proof. ■

⁹See Equation ?? and Equation ??

¹⁰You may google what is a monoid.

¹¹However unfortunate, the naming is "justified" in the sense that fractional ideals "act like" ordinary ideals with the twist that denominators are allowed, and moreover, if $xM \subseteq A$ for some x , then xM is indeed an ideal.

¹²which automatically implies the uniqueness of inverses of invertible ideals

Let M be an element of the group invertible ideals of A . From $M^{-1} = (A : M)$, we see that M as an A -module is finitely generated¹³ and thus a fractional ideal of A ¹⁴. We have shown that the group of invertible ideals is a sub-monoid of the monoid of fractional ideals of A .

For next theorem, note that given any A -submodule $N \subseteq K$ and prime $\mathfrak{p} \subseteq A$, we can and will identify $N_{\mathfrak{p}}$ as an $A_{\mathfrak{p}}$ -submodule of $\text{Frac}(A)$. This is because by universal property, we have the diagram

$$\begin{array}{ccccc}
 N & & A & \xrightarrow{\quad} & A_{\mathfrak{p}} \\
 \downarrow & \searrow & \downarrow & & \downarrow \\
 N_{\mathfrak{p}} & \hookrightarrow & \text{Frac}(A) & \longleftrightarrow & \text{Frac}(A_{\mathfrak{p}})
 \end{array}$$

Theorem 2.7.2. (Invertibility is a local property) Let A be an integral domain, $K \triangleq \text{Frac}(A)$, and $M \subseteq K$ a fractional ideal of A . We have

M is invertible $\iff M$ is finitely generated and $M_{\mathfrak{p}}$ invertible of $A_{\mathfrak{p}}$ for all prime $\mathfrak{p} \subseteq A$.

Proof. For the only if part, since we already know that $M_{\mathfrak{p}}$ is finitely generated, we only have to perform a routine check of:

$$M_{\mathfrak{p}}(A : M)_{\mathfrak{p}} = A_{\mathfrak{p}}.$$

For the if part, first observe that $M(A : M)$ is an integral ideal. Let \mathfrak{m} be an maximal integral ideal, and denote the integral ideal $M(A : M)$ by \mathfrak{a} . Check that

$$\mathfrak{a}_{\mathfrak{m}} = M_{\mathfrak{m}}(A : M)_{\mathfrak{m}} = M_{\mathfrak{m}}(A_{\mathfrak{m}} : M_{\mathfrak{m}}) = A_{\mathfrak{m}}$$

¹⁵ Let $x \in A - \mathfrak{m}$. Because $x \in A \subseteq A_{\mathfrak{m}} = \mathfrak{a}_{\mathfrak{m}}$, we know there exists $a \in \mathfrak{a}$ and $s \in A - \mathfrak{m}$ such that $x = as^{-1}$. Because maximal ideal is prime, we now see $a = xs \notin \mathfrak{m}$. In other words, $\mathfrak{a} \not\subseteq \mathfrak{m}$. This with maximality of \mathfrak{m} implies $\mathfrak{a} = A$, i.e., M is invertible. \blacksquare

¹³ $\sum x_i y_i = 1$ for some $x_i \in (A : M), y_i \in M \implies M = \langle y_i \rangle$

¹⁴ $(x_1 \cdots x_n) \langle \frac{y_1}{x_1}, \dots, \frac{y_n}{x_n} \rangle \subseteq A$.

¹⁵ $(A : M)_{\mathfrak{m}} = (A_{\mathfrak{m}} : M_{\mathfrak{m}})$ depends on the fact that M is finitely generated.

2.8 Dedekind domain

Theorem 2.8.1. (Local domain D is DVR if and only if every nonzero fractional ideal of D is invertible) Let D be a local domain.

D is a DVR \iff every nonzero fractional ideal of D is invertible.

Proof. We first prove (\implies). Let $\mathfrak{a}_1 = \langle x \rangle$ in Equation 2.4, and let M be a nonzero fractional ideal. Let $y \in D$ satisfies $yM \subseteq D$, so $yM = \langle x^k \rangle$ for some $k \in \mathbb{N}$. This implies M is a fractional principal ideal $M = \langle x^{k - \frac{\nu(y)}{p}} \rangle$, thus invertible.

We now prove (\impliedby). Because every integral ideal of D is invertible and **therefore finitely generated, we know D is Noetherian**. Let \mathfrak{m} be the unique maximal ideal of D . If every nonzero proper integral ideal is a power of \mathfrak{m} , then no nonzero proper ideal integral ideal that isn't \mathfrak{m} can be prime, since, says $0 \neq \mathfrak{m}^k \subset \mathfrak{m}$, we would have some $m_1, \dots, m_k \notin \mathfrak{m}^k$ that satisfy $m_1 \cdots m_k \in \mathfrak{m}^k$. Therefore, if we can prove that every nonzero proper integral ideal is a power of \mathfrak{m} , we can conclude $\text{Krudim}(D) = 1$ and use **Theorem 2.5.1** to conclude D is a DVR.

We have reduced the problem into proving every nonzero proper integral ideal is a power of \mathfrak{m} . Assume for a contradiction that this isn't true. Let Σ be the collection of nonzero ideals that are not powers of \mathfrak{m} . **Because D is Noetherian, there exists some maximal element $\mathfrak{a} \in \Sigma$** . We know $\mathfrak{a} \subset \mathfrak{m}$ from $\mathfrak{a} \neq \mathfrak{m}^1$. Let \mathfrak{m}^{-1} be the inverse of \mathfrak{m} in the group of invertible ideals. Because $\mathfrak{a} \neq \mathfrak{m}^1$, we know $\mathfrak{a} \subset \mathfrak{m}$, which implies $\mathfrak{m}^{-1}\mathfrak{a} \subset \mathfrak{m}^{-1}\mathfrak{m} = D$. We have shown that $\mathfrak{m}^{-1}\mathfrak{a}$ is a proper integral ideal. Also, note that $\mathfrak{m}^{-1}\mathfrak{a} \supseteq \mathfrak{a}$ because by **Proposition 2.7.1** $1 \in \mathfrak{m}^{-1}$.

We shall cause a contradiction using the fact $\mathfrak{a} \subseteq \mathfrak{m}^{-1}\mathfrak{a} \subset D$, which we have just proved. Clearly, there are only two possibilities: either $\mathfrak{m}^{-1}\mathfrak{a}$ strictly include \mathfrak{a} or not. If $\mathfrak{m}^{-1}\mathfrak{a}$ strictly include \mathfrak{a} , then $\mathfrak{m}^{-1}\mathfrak{a}$ is a power of \mathfrak{m} by maximality of \mathfrak{a} , which implies that \mathfrak{a} is a power of \mathfrak{m} , a contradiction. If not, then we may deduce $\mathfrak{a} = \mathfrak{m}\mathfrak{a}$, and use **Nakayama's Lemma**¹⁶ to deduce $\mathfrak{a} = 0$, also a contradiction. ■

A **Dedekind domain** is an integral domain D whose localizations at nonzero prime are always DVR.

Theorem 2.8.2. (An equivalent definition of Dedekind Domain) Let D be an

¹⁶To see \mathfrak{a} is finitely generated, observe that \mathfrak{a} is an D -submodule of the Noetherian D -module and use **Theorem 1.8.1**. To see $\mathfrak{m} \subseteq \text{Jacob}(D)$, just note that by definition \mathfrak{m} is the only maximal ideal of D .

integral domain.

D is a Dedekind domain \iff every nonzero fractional ideal of D is invertible.

Proof. We first prove (\implies). Let $M \neq 0$ be a fractional ideal. $\text{Frac}(D)$ is Noetherian because D is Noetherian. This implies M is finitely generated. Clearly for any prime $\mathfrak{p} \subseteq D$, $M_{\mathfrak{p}}$ is always nonzero fractional ideal of $D_{\mathfrak{p}}$. We have shown M is finitely generated and $M_{\mathfrak{p}}$ is always invertible ideal of $D_{\mathfrak{p}}$. Then because invertibility is a local property, M is also invertible.

We now prove (\impliedby). Fix nonzero prime $\mathfrak{p} \subseteq D$. By Theorem 2.8.1, we only have to prove every nonzero fractional ideal of $D_{\mathfrak{p}}$ is invertible. Let M be a nonzero fractional ideal of $D_{\mathfrak{p}}$, and $x \neq 0 \in \text{Frac}(D)$ satisfies $xM \subseteq D_{\mathfrak{p}}$. To prove M is invertible of $D_{\mathfrak{p}}$, we must first note that if there exists some fractional ideal N of $D_{\mathfrak{p}}$ such that $(xM)N = D_{\mathfrak{p}}$, then we will have $M(xN) = D_{\mathfrak{p}}$. Because xM is a nonzero integral ideal of $D_{\mathfrak{p}}$, this allow us to reduce the problem into proving all nonzero integral ideal of $D_{\mathfrak{p}}$ is invertible of $D_{\mathfrak{p}}$.

Let \mathfrak{b} be an integral ideal of $D_{\mathfrak{p}}$, and define $\mathfrak{a} \triangleq \mathfrak{b} \cap D$. Clearly \mathfrak{a} is an integral ideal of D , so by premise, \mathfrak{a} is invertible. It now follows from $\mathfrak{b} = \mathfrak{a}_{\mathfrak{p}}$ ¹⁷ and the fact invertibility is a local property that \mathfrak{b} is invertible of $D_{\mathfrak{p}}$. ■

¹⁷You may check this.

Chapter 3

Dimension and Completion

3.1 Completion

Let G be simultaneously a group and a topological space. We say G is a **topological group** if addition $(x, y) \mapsto x + y$ and negation $x \mapsto -x$ are both continuous.

Equivalent Definition 3.1.1. (Topological Group) Let G be simultaneously a group and a topological space. The followings are equivalent:

- (i) G is a topological group.
- (ii) $G \times G \rightarrow G; (x, y) \mapsto x - y$ is continuous.

Proof. (i) \implies (ii): Because subtraction is the composition:

$$G \times G \xrightarrow{(x,y) \mapsto (x,-y)} G \times G \xrightarrow{(x,y) \mapsto x+y} G$$

To see the first map is continuous, just observe both components of $(x, y) \mapsto (x, -y)$ are continuous.¹

(ii) \implies (i): Note that negation is the composition:

$$G \xrightarrow{x \mapsto (0,x)} G \times G \xrightarrow{(x,y) \mapsto (x,-y)} G$$

Again to see the first map is continuous, just observe that both components of $x \mapsto (0, x)$ are continuous. Note that addition is the composition:

$$G \times G \xrightarrow{(x,y) \mapsto (x,-y)} G \times G \xrightarrow{(x,y) \mapsto x+y} G$$

The fact that the second components of the first map is continuous follows from the fact that negation is continuous. ■

¹The universal property of product topology implies that $f : X \rightarrow \prod Y_i$ is continuous if and only if f_i are all continuous.

Recall that given topological space X and sequence $\{x_n\}$ in X , we say $x_n \rightarrow y$ if for all neighborhood U of y , there exists some $s(U)$ such that $x_n \in U$ for all $n \geq s(U)$. Let G be an abelian topological group². Because $U + x$ are open for any open $U \subseteq G$ and $x \in G$,³ we see that in G ,

$$x_n \rightarrow y \iff (x_n - y) \rightarrow 0.$$

Let G be an abelian topological group. We say a sequence $\{x_n\}$ in G is a **Cauchy sequence** if for all neighborhood U of 0, there exists some integer $s(U)$ such that

$$x_n - x_m \in U \text{ for all } n, m \geq s(U)$$

Clearly, we may define on the collection of Cauchy sequences in G an equivalence relation by saying two Cauchy sequences $\{x_n\}, \{y_n\}$ are equivalent if and only if $x_n - y_n \rightarrow 0$.⁴ We denote the equivalence class of Cauchy sequences in G by \widehat{G} . Clearly we may well-define the obvious group structure on \widehat{G} .⁵

Let G be an abelian topological group, and let N be a neighborhood of 0. We denote $\widehat{N} \subseteq \widehat{G}$ the collection of equivalence class $[x_n]$ such that for every $\{y_n\} \in [x_n]$, there exists integer M such that $y_n \in N$ for all $n \geq M$. Clearly, the collection of $U \subseteq \widehat{G}$ such that:

$$\text{For all } [x_n] \in U \text{ there exists neighborhood } N \subseteq G \text{ of } 0 \text{ such that } [x_n] + \widehat{N} \subseteq U$$

forms a topology on \widehat{G} .⁶

Suppose moreover that G has a **local basis** at 0 with the form:

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots, \quad \text{where } G_i \text{ are all subgroups of } G.$$

In other words, we have a descending chain of subgroups G_i such that G_i are all open and every neighborhood of 0 contains some G_i .

²We must require G to be abelian here, so that we don't have to talk about notions like "left converge", "right converge", "left Cauchy," and "right Cauchy". For more information, see comments of this MO post: <https://mathoverflow.net/questions/150703/completion-of-abelian-topological-groups> that give a reference to Bourbaki.

³You may check that the translation $z \mapsto z - x$ is continuous.

⁴Fix U , and let $f : G \rightarrow G$ be the negation. There exists N such that $x_n - y_n \in f^{-1}(U)$ for all $n \geq N$. Such N suffices to prove symmetry. Let $g : G \times G \rightarrow G$ be the addition. There exists open $O_1, O_2 \subseteq G$ such that $O_1 \times O_2 \subseteq g^{-1}(U)$, and there exists N such that $x_n - y_n \in O_1$ and $y_n - z_n \in O_2$. Such N suffices to prove transitivity.

⁵The argument for well-definedness of group structure is the same as that for well-definedness of equivalence class.

⁶To see that this topology is indeed closed under finite intersection, show $\widehat{N_1 \cap N_2} \subseteq \widehat{N_1} \cap \widehat{N_2}$

3.2 Filtrations

3.3 Graded rings and modules

Given some ring A , a **grading on A** is an assignment of each $n \in \mathbb{Z}$ a subgroup $A_n \subseteq A$ such that $A = \bigoplus A_n$ and $A_n A_t \subseteq A_{n+t}$ ⁷ for all $n, t \in \mathbb{Z}$. If we say graded ring A is **\mathbb{N} -graded**, we mean that $A_n = 0$ for all $n < 0$. Fix $a \in A$. If $a = a_{n_1} + \cdots + a_{n_s}$ for $a_{n_i} \in A_{n_i}$, we say a_{n_i} are the **homogeneous components of a** , and if $s = 1$ we say a is a **homogeneous element**. Note that there is ambiguity whether 0 should be considered homogeneous. If one consider 0 homogeneous, then 0 should have arbitrary degree.

Theorem 3.3.1. (Properties of graded rings) If A is a graded ring, then:

- (i) A_0 forms a subring of A .
- (ii) For each $n \in \mathbb{Z}$, A_n forms a A_0 -modules where the scalar product is the multiplication of A_0 .

Proof. (i): A_0 is clearly closed under addition and multiplication. To see $1 \in A$, consider the highest graded component of 1 and $1 = 1 \cdot 1$. (ii) is clear. ■

An ideal $\mathfrak{a} \subseteq A$ is **homogeneous** if \mathfrak{a} have a set of generators that are all homogeneous.

Equivalent Definition 3.3.2. (Homogeneous ideals) Given a graded ring A and an ideal \mathfrak{a} in A , the followings are equivalent:

- (i) \mathfrak{a} is homogeneous.
- (ii) $\mathfrak{a} = \bigoplus \mathfrak{a} \cap A_n$

Proof. (i) \implies (ii): The sum $\sum (\mathfrak{a} \cap A_n)$ is clearly direct. We only have to prove $\sum (\mathfrak{a} \cap A_n) = \mathfrak{a}$. Fix $a \in \mathfrak{a}$. By premise, there exists some $a_1, \dots, a_s, x_1, \dots, x_s \in A$ such that:

- (a) $a = \sum x_i a_i$.
- (b) For all i , $a_i \in \mathfrak{a} \cap A_{j_i}$ for some $j_i \in \mathbb{Z}$.

The proof then follows from expressing x_i as the sum of its homogeneous components. Note that (ii) \implies (i) is clear. ■

Theorem 3.3.3. (Homogeneous ideals are closed under common operations) Given a graded ring A and two homogeneous ideals $\mathfrak{a}, \mathfrak{b}$ in A , the sum, the product, and the intersection of $\mathfrak{a}, \mathfrak{b}$ all remain homogeneous. The radical of \mathfrak{a} is also homogeneous.

⁷You may interpret $A_t A_n$ as $\{a_t a_n \in A : a_t \in A_t, a_n \in A_n\}$ here.

Proof. Let S_a, S_b contain only homogeneous elements and generate $\mathfrak{a}, \mathfrak{b}$. The sum $\mathfrak{a} + \mathfrak{b}$ is then generated by $S_a \cup S_b$.

If $(x_1 + \cdots + x_r)^l \in I$ with x_r highest grade and I homogeneous, then since the highest grade term of $(x_1 + \cdots + x_r)^l$ is x_r^l , we have $x_r \in \sqrt{I}$, which implies $x_1 + \cdots + x_{r-1} \in \sqrt{I}$. ■

Given graded ring A and homogeneous ideal I , one may check that $(A/I)_d \triangleq \pi(A_d)$ for all d where $\pi : A \twoheadrightarrow A/I$ is the quotient map forms a grading and satisfies the universal property of quotient in the category of graded rings.

Given a graded ring A and an A -module M , a **grading on M** is an assignment of each $n \in \mathbb{Z}$ a submodule $M_n \subseteq M$ such that $M = \bigoplus M_n$ and $A_n M_t \subseteq M_{n+t}$ for all $n, t \in \mathbb{Z}$. **Twisted module $M(l)$** as an A -module is the same as M , but its grading are shifted by $M(l)_d \triangleq M_{d+l}$. Given some map $f : M \rightarrow N$ between two graded A -modules, we say f is a **graded A -module homomorphism** if f is a A -module homomorphism and f respect the grading in the sense that $f(M_n) \subseteq N_n$ for all $n \in \mathbb{Z}$. Let $N \subseteq M$ be an A -submodule. We say N is a **graded A -submodule of M** if the inclusion map is an graded A -module homomorphism.

Equivalent Definition 3.3.4. (Graded submodules) Let A be a graded ring, M a graded A -module, and $N \subseteq M$ a A -submodule. The followings are equivalent:

- (i) N is a graded A -submodule of M .
- (ii) $N = \bigoplus (N \cap M_n)$.
- (iii) N have a set of generator consisting of homogeneous elements.⁸

Proof. ■

⁸You haven't define homogeneous elements for graded modules yet.

3.4 Dimension

Theorem 3.4.1. (Krull dimension of polynomial rings) Let A be a Noetherian ring, and let $A[x_1, \dots, x_n]$ be the formal polynomial ring. Then:

$$\text{Krudim}(A[x_1, \dots, x_n]) = \text{Krudim } A + n$$

Proof. Because of **Hilbert basis theorem**, it is enough to prove the case $n = 1$. Let \mathfrak{p} be a prime ideal in A and P a prime ideal in $A[x]$ that makes $\text{ht}(P/\mathfrak{p})$ ■

Theorem 3.4.2. (Krull's principal ideal theorem) Given Noetherian A , if $x \in A$ is neither a unit nor a zero-divisor, then the minimal prime ideals over $\langle x \rangle$ all have height 1.

Theorem 3.4.3. (Dimension Theorem) Let k be a field, B a finitely generated k -algebra and also an integral domain, and $\mathfrak{p} \subseteq B$ be prime. We have:

- (i) $\text{Krudim}(B) = \text{trdeg}_k \text{Frac}(B)$.
- (ii) $\text{height } \mathfrak{p} + \text{Krudim}(B/\mathfrak{p}) = \text{Krudim}(B)$.

3.5 Hilbert function

Chapter 4

The Classical

4.1 Topology of Zariski

Let X be a topological space. We say X is **irreducible** if X can not be written as union of two proper closed subset of X . If we say a subset of some topological space is **irreducible**, we mean that that subset when given the subspace topology is irreducible. Let X be some arbitrary topological space. In other words, $Y \subseteq X$ is irreducible if and only if Y can not be written as $Y = (F_1 \cap Y) \cup (F_2 \cap Y)$ where $F_1, F_2 \subseteq X$ are closed and don't contain Y .

Theorem 4.1.1. (Irreducibility and closure) Given topological spaces $Y \subseteq X$, the topological space Y is irreducible if and only if \overline{Y} is irreducible.

Proof. Just observe that given any two closed sets $F_1, F_2 \subseteq X$, the statement that $\overline{Y} = (F_1 \cap \overline{Y}) \cup (F_2 \cap \overline{Y})$ where $F_1 \cup F_2$ doesn't cover \overline{Y} is equivalent to the statement that $Y = (F_1 \cap Y) \cup (F_2 \cap Y)$ where $F_1 \cup F_2$ doesn't cover Y . ■

Equivalent Definition 4.1.2. (Irreducible topology) Given topological space X , the followings are equivalent:

- (i) X is irreducible.
- (ii) Every nonempty open subset of X is dense.
- (iii) Every two nonempty open subset of X have nonempty intersection.
- (iv) Every open subspace of X is irreducible.

Proof. (i) \implies (ii): If nonempty open $Y \subseteq X$ is not dense, then \overline{Y} is proper closed and $X = \overline{Y} \cup (X - Y)$.

(ii) \implies (iii): Assume for a contradiction $Y_1, Y_2 \subseteq X$ are nonempty open that have empty intersection. One get a contradiction from $\overline{Y_1} = X$ and $Y_1 \subseteq X - Y_2$.

(iii) \implies (i): Assume for a contradiction X is reducible, says, $X = Y_1 \cup Y_2$. One get a contradiction from noting $X - Y_1$ and $X - Y_2$ have empty intersection.

(i) \implies (iv) follows from (i) \implies (ii) and [Theorem 4.1.1](#). ■

By Zorn's Lemma¹, every $x \in X$ has some not necessarily unique maximal irreducible set Y containing x . We call these maximal irreducible sets **irreducible components of X** . Because [closure of an irreducible set is also irreducible](#), irreducible components are closed. For ease in [future section on quasi variety morphism](#), we note that:

Equivalent Definition 4.1.3. (Quasi variety) If $V \subseteq X$ is irreducible closed and $Y \subseteq V$ is open in V , then $\overline{Y} = V$.

Proof. Clearly $\overline{Y} \subseteq V$. The converse $V \subseteq \overline{Y}$ follows from $\overline{Y} \cap V = \text{cl}_V(Y) = V$, where the last equality holds true due to [equivalent definition of irreducibility](#). ■

Let X be a topological space. We say X is **Noetherian** if its closed sets satisfy descending chain condition. Clearly, subspace Y of Noetherian space X is also Noetherian².

Equivalent Definition 4.1.4. (Noetherian topology) Given topological space X , the followings are equivalent:

- (i) X is Noetherian
- (ii) Open sets of X satisfy ascending chain condition.
- (iii) Every subset of X is compact.

Proof. (i) \implies (ii) is clear.

(ii) \implies (iii): Assume for a contradiction $Y \subseteq X$ has an open cover \mathcal{U} that has no finite subcover. Fix $E_1 \in \mathcal{U}$. Because \mathcal{U} has no finite subcover, there exists $E_2 \in \mathcal{U}$ such that $E_2 \cap Y - (E_1 \cap Y)$ is nonempty, i.e., $E_1 \cup E_2$ strictly contain E_1 . Again, because \mathcal{U} has no finite subcover, there exists $E_3 \in \mathcal{U}$ such that $E_3 \cap Y - ((E_1 \cup E_2) \cap Y)$ is nonempty. Repeating the same process, we construct a non-stopping ascending chain of open sets: $E_1 \subset E_1 \cup E_2 \subset E_1 \cup E_2 \cup E_3 \subset \dots$, a contradiction.

(iii) \implies (i): Let F_n be a descending chain of closed subsets of X . Clearly $X - F_n$ is an ascending chain and forms an open cover of $X - \bigcap F_n$. It follows from compactness of $X - \bigcap F_n$ that descending chain F_n must stops permanently at some point. ■

¹Clearly $\{x\}$ is irreducible. Let E_n be an ascending chain of irreducible set containing x . To see its upper bound is also irreducible, assume it isn't and cause a contradiction by showing E_n are reducible for large n .

²Given $X_1 \cap Y \supseteq X_2 \cap Y \supseteq \dots$, we have $X_n \cap Y = X_1 \cap \dots \cap X_n \cap Y$, and the descending chain $X_1 \supseteq X_1 \cap X_2 \supseteq \dots$ must stop.

As we shall see, most of the topologies studied in this note are Noetherian, and indeed they have nice relationship with irreducibility.

Theorem 4.1.5. (Topological form of Lasker-Noether Theorem) If topological space X is Noetherian, then for every nonempty closed $V \subseteq X$, there always exists unique irreducible closed $V_1, \dots, V_m \subseteq X$ such that

$$V = V_1 \cup \dots \cup V_m \quad (4.1)$$

and every V_i is necessary in the sense that $\bigcup_{j \neq i} V_j \neq V$.

Proof. Note that if V can be written as some finite union of irreducible closed subsets, then we may delete the unnecessary terms so that every term in the union is necessary. We now prove that every V can be written as a finite union of irreducible closed subset.

Let \mathcal{S} be the collection of nonempty closed subset of X that can not be written as finite union of irreducible closed subsets. Assume for a contradiction that \mathcal{S} is nonempty. Because X is Noetherian, \mathcal{S} have some minimal element, say Y . Because Y is reducible, we may write $Y = Y_1 \cup Y_2$, where Y_1 and Y_2 are both closed and contained strictly by Y . By minimality of $Y \in \mathcal{S}$, Y_1 and Y_2 can both be written as finite union of irreducible closed subset, a contradiction³.

It remains to prove the uniqueness of expression of V , so suppose

$$V = V_1 \cup \dots \cup V_m = W_1 \cup \dots \cup W_r$$

where V_i, W_j are all irreducible closed and "necessary". For each i , because V_i is irreducible and $V_i = \bigcup (W_j \cap V_i)$, we have $V_i \subseteq W_j$ for some fixed j . The same argument yields $W_j \subseteq V_p$ for some fixed p . It then follows from the "necessity" that $V_i = W_j$. This implies uniqueness. ■

Let X be a Noetherian topological space. **Topological form of Lasker-Noether Theorem** tell us that X , uniquely, can be written as $X = V_1 \cup \dots \cup V_m$ where V_i are all irreducible closed and necessary in this union. One may conjecture that these V_i are exactly the irreducible components of X . This is true indeed. Fix j . To see V_j is an irreducible component, let W be some irreducible component containing V_j . We are required to show $W = V_j$. Because $W = \bigcup (W \cap V_i)$ and W is an irreducible component⁴, we must have $W \subseteq V_l$ for some l . It then follows from the "necessity: that $j = l$ and $V_j = W$. Conversely, let W be some irreducible component of X . We are required to show W is one of V_i . Because W is irreducible

³Because $Y = Y_1 \cup Y_2$.

⁴So $W \cap V_i$ are all closed. Recall that irreducible components are closed, since closure of irreducible set is also irreducible.

and $W = \bigcup (W \cap V_i)$, we have $W \subseteq V_i$ for some i , which by maximality of W implies $W = V_i$.

We close this section by introducing the idea of variety dimension in a purely topological setting. Let X be a topological space. We define the **dimension of X** to be the supremum of all integers n such that there exists a chain $\emptyset = Z_0 \subset Z_1 \subset \cdots \subset Z_n$ of distinct irreducible closed subsets of X . Immediately we see same wanted property of our definition for dimension: Given subspace $Y \subseteq X$, we have $\text{topdim}(Y) \leq \text{topdim}(X)$.⁵

⁵To prove this, you will need: Y_i closed in $Y \implies Y_i = \overline{Y_i} \cap Y$.

4.2 Affine variety

Let k be some field. We use \mathbb{A}^n to denote the **affine n -space** over k , the Cartesian product k^n . Given some collection $S \subseteq k[x_1, \dots, x_n]$ of polynomials, we use $V(S) = \{a \in \mathbb{A}^n : F(a) = 0 \text{ for all } F \in S\}$ to denote its **vanishing set**, and given $X \subseteq \mathbb{A}^n$, we use notation $I(X)$ to denote the ideal of polynomials that vanish on X . If $X \subseteq \mathbb{A}^n$ is the vanishing set of some $S \subseteq k[x_1, \dots, x_n]$, we say X is **algebraic**. Clearly this give rise to a topology on \mathbb{A}^n , the **Zariski topology**, in which $X \subseteq \mathbb{A}^n$ is closed if and only if X is algebraic⁶. We call irreducible closed subset of \mathbb{A}^n **affine variety**. Clearly, we have:

$$\overline{X} = V(I(X)), \quad \text{for all } X \subseteq \mathbb{A}^n \quad (4.2)$$

and

$$I(X) = I(\overline{X}), \quad \text{for all } X \subseteq \mathbb{A}^n$$

Even without putting any restriction on the ground fields, we see from **Hilbert Basis Theorem** and **Equation 4.2** that \mathbb{A}^n are always Noetherian, and we have the prime-irreducibility correspondence:

Theorem 4.2.1. (Prime-irreducibility correspondence) For all $X \subseteq \mathbb{A}^n$,

$$X \text{ is irreducible} \iff I(X) \text{ is prime} \quad (4.3)$$

Proof. Before the proof, we first make the remark that clearly for all $F, G \in k[x_1, \dots, x_n]$, we have:

$$FG \in I(X) \iff X = (X \cap V(F)) \cup (X \cap V(G)) \quad (4.4)$$

(\implies) in **Equation 4.3** is then an immediate consequence of (\implies) in **Equation 4.4**.

We now prove (\impliedby) in **Equation 4.3**. Assume for a contradiction that $X = (X \cap V_1) \cup (X \cap V_2)$ for some V_1, V_2 such that neither of them covers X . Clearly, there exists some $F \in I(V_1) - I(X)$. This F satisfies $I(V_1) - I(X)$. Similar argument gives us some $G \in I(V_2) - I(X)$, but $FG \in I(X)$, a contradiction to $I(X)$ being prime. ■

Because **Hilbert's Basis Theorem** only require the underlying ring of polynomials to be Noetherian, which all fields are, we can already deduce some important properties from the hypothesis (as weak as this hypothesis is) that k is a field. For example, one may show \mathbb{A}^n as

⁶Note that $V(S_1) \cup V(S_2) = V(\{f_1 f_2 : f_1 \in S_1, f_2 \in S_2\})$ and $\bigcap V(S_\alpha) = V(\bigcup S_\alpha)$

a topological space is Noetherian⁷, every closed $X \subseteq \mathbb{A}^n$ is of the form $X = V(F_1, \dots, F_m)$ for some $F_1, \dots, F_m \in k[x_1, \dots, x_n]$,⁸ and \mathbb{A}^n is irreducible if, moreover, k is infinite:

Theorem 4.2.2. (Polynomial Identity Principal) Let k be an infinite field and $F \neq 0 \in k[x_1, \dots, x_n]$. There exists some nonzero $\mathbf{a} \in \mathbb{A}^n$ such that $F(\mathbf{a}) \neq 0$.

Proof. We prove by induction on n . Base case $n = 1$ follows from fundamental theorem of algebra and taking algebraic closure \bar{k} . Suppose the assertion hold true for $n - 1$, and write

$$F(x_1, \dots, x_n) = \sum_{i=0}^d G_i(x_1, \dots, x_{n-1})x_n^i, \quad \text{where } d = \deg_{x_n} F$$

By inductive hypothesis, there exists some nonzero $(a_1, \dots, a_{n-1}) \in \mathbb{A}^{n-1}$ such that

$$G_d(a_1, \dots, a_{n-1}) \neq 0$$

It then follows from the base case that there exists some nonzero $x_n \in k$ such that $F(x_1, \dots, x_n) \neq 0$. ■

Corollary 4.2.3. (Affine space is irreducible if the underlying field is infinite) If field k is infinite, then \mathbb{A}^n as a topological space is irreducible.

Proof. Suppose $\mathbb{A}^n = V(F_1, \dots, F_r) \cup V(G_1, \dots, G_m)$. Clearly $F_1 \cdots F_r G_1 \cdots G_m$ vanishes on \mathbb{A}^n . This implies $F_1 \cdots F_r G_1 \cdots G_m = 0 \in k[x_1, \dots, x_n]$, which implies one of them is zero. Says, $F_1 = 0$. In such case, we see $V(F_1, \dots, F_r) = V(F_2, \dots, F_r)$ and

$$\mathbb{A}^n = V(F_2, \dots, F_r) \cup V(G_1, \dots, G_m)$$

Repeating the same argument, we see that either F_1, \dots, F_r are all zeros or G_1, \dots, G_m are all zeros. ■

Corollary 4.2.3 proves that affine spaces over infinite field are irreducible, and their every of its open set is a quasi variety. The situation of affine spaces over finite field is in fact even simpler: If k is finite and nontrivial, then \mathbb{A}^n all have discrete topology⁹, thus reducible. Therefore, whenever we use the term variety, its ground field must be infinite.

Theorem 4.2.4. (Relationship between topological form and algebraic form of Lasker-Noether Theorem) Let $X \subseteq \mathbb{A}^n$ be nonempty closed, C_1, \dots, C_t be its irreducible components and $\mathfrak{p}_1, \dots, \mathfrak{p}_r \subseteq k[\mathbf{x}]$ minimal prime ideals over $I(X)$. We have $r = t$ and by switching order, $C_i = V(\mathfrak{p}_i)$.

⁷Given descending chain of closed subset $X_0 \supset X_1 \supset \cdots \supset X_m$ of \mathbb{A}^n , we must have $I(X_0) \subset I(X_1) \subset \cdots \subset I(X_m)$ where the inequalities hold true because of **Equation 4.2**. Now recall that **Hilbert's Basis Theorem** guarantees $k[x_1, \dots, x_n]$ is Noetherian.

⁸For its reason, consider **the third equivalent definition of Noetherian module**.

⁹Every singleton is closed. $\{\mathbf{a}\}$ is the vanishing set of $\{x_1 - a_1, \dots, x_n - a_n\}$.

Proof. Observing that the ideal of any irreducible closed subsets of X is a prime ideal over $I(X)$, we see that the
Clearly, $V(\mathfrak{p}_i)$ are irreducible closed subset of X . ■

If k is closed, we have the powerful **Nullstellensatz**:

$$I(V(I)) = \sqrt{I}, \quad \text{for all ideal } I \subseteq k[x_1, \dots, x_n]$$

As **Equation 4.2** have already shown, functor:

$$\{X \subseteq \mathbb{A}^n : X \text{ is a variety.}\} \xrightarrow{I} \text{Spec}(k[x_1, \dots, x_n])$$

is injective. **Nullstellensatz** moreover shows that this functor is surjective. In particular, I forms a bijection between points in \mathbb{A}^n with $\text{Max}(k[x_1, \dots, x_n])$ ¹⁰.

Theorem 4.2.5. (Hypersurface of affine space must be cutout by a single polynomial) Let k be closed. $X \subseteq \mathbb{A}^n$ has dimension $n - 1$ if and only if $X = V(F)$ for some nonconstant irreducible $F \in k[\mathbf{x}]$.

Proof. ■

¹⁰Using **the weak form of Nullstellensatz**, if $\mathfrak{m} \subseteq k[x_1, \dots, x_n]$ is maximal, then one construct isomorphism $\phi : k[x_1, \dots, x_n]/\mathfrak{m} \rightarrow k$ and set $a_i \triangleq x_i$ to see $\phi([f]) = f(a)$ and $\{a\} = V(\mathfrak{m})$

4.3 Projective variety

Let k be some field. Clearly, we may define on $k^{n+1} - \{0\}$ an equivalence relation by setting

$$a \sim b \iff a = \lambda b, \quad \text{for some } \lambda \in k$$

Similar to the affine n -space, we use the notation \mathbb{P}^n to represent the set of equivalence classes, and we use the notation $[x_0 : \cdots : x_n]$ to denote the equivalence class that contains (x_0, \dots, x_n) . Clearly, we may give the polynomial ring $k[x_0, \dots, x_n]$ the obvious grading. Let $F \in k[x_0, \dots, x_n]$ be homogeneous. Even though the value of F on \mathbb{P}^n is not well-defined, if F is homogeneous then indeed it is well-defined whether $F(p) = 0$ for fixed $p \in \mathbb{P}^n$, so it make sense for us to talk about the **(projective) algebraic set** $V(S) = \{p \in \mathbb{P}^n : F(p) = 0 \text{ for all } F \in S\}$ for every collection $S \subseteq k[x_1, \dots, x_{n+1}]$ of homogeneous polynomial. Again this give rise to **Zariski topology** on \mathbb{P}^n where $E \subseteq \mathbb{P}^n$ is closed if and only if E is algebraic, and again we say $X \subseteq \mathbb{P}^n$ is a **projective variety** if X is irreducible closed.

Let S_1 and $S_2 \subseteq k[x_0, \dots, x_n]$ be two collections of homogeneous polynomials that generate the same ideal. Clearly we have $V(S_1) = V(S_2)$. Therefore, given some homogeneous ideal $J \subseteq k[x_0, \dots, x_n]$, we may well define algebraic $V(J)$. Trivially, for each $X \subseteq \mathbb{P}^n$, the ideal generated by homogeneous $F \in k[x_0, \dots, x_n]$ that vanishes on X is homogeneous. We denote such ideal $I(X)$ and call it **defining ideal of X** if X is closed.

Immediately, we see that projective space have lots of similar property with affine space. For example, \mathbb{P}^n is Noetherian, and similar to [Equation 4.2](#), we have:

$$\overline{X} = V(I(X)), \quad \text{for all } X \subseteq \mathbb{P}^n$$

And similar to the [fact that if the underlying field is infinite, the affine space is irreducible](#), we have:

Theorem 4.3.1. (Projective space is irreducible if the underlying field is infinite)
If field k is infinite, then \mathbb{P}^n is irreducible.

Proof. Suppose $\mathbb{P}^n = V(F_1, \dots, F_r) \cup V(G_1, \dots, G_m)$. Clearly $F_1 \cdots F_r G_1 \cdots G_m$ vanishes on \mathbb{P}^n . This implies $F_1 \cdots F_r G_1 \cdots G_m$ vanishes on $\mathbb{A}^{n+1} - \{0\}$. Now, if we were able to prove $F_1 \cdots F_r G_1 \cdots G_m$ also vanishes 0 , thus whole \mathbb{A}^{n+1} , then we may use the same argument in [Corollary 4.2.3](#). To see that $F_1 \cdots F_r G_1 \cdots G_m$ also vanishes at 0 , just observe that because $F_1 \cdots F_r G_1 \cdots G_m$ is homogeneous, if it doesn't vanish at 0 , then $F_1, \dots, F_r, G_1, \dots, G_m$ are all nonzero constant, which is clearly impossible. ■

Also we have the prime-irreducibility correspondence, whose proof in the projective setting requires some more algebraic effort.

Theorem 4.3.2. (Projective prime-irreducibility correspondence) For all $X \subseteq \mathbb{P}^n$,

$$X \text{ is irreducible} \iff I(X) \text{ is prime}$$

Proof. (\implies): Let $F, G \in k[x_0, \dots, x_n]$ satisfy $FG \in I(X)$. We are required to prove one of them belongs to $I(X)$. Let F_1, \dots, F_d and G_1, \dots, G_r be the (nonzero) homogeneous component of F and G with $\deg(F_i) < \deg(F_{i+1}), \deg(G_i) < \deg(G_{i+1})$ for all i . Because $F_d G_r$ is exactly the highest degree term of $FG \in I(X)$ and because $I(X)$ is homogeneous, we know $F_d G_r \in I(X)$. Because X is irreducible and because $X = (X \cap V(F_d)) \cup (X \cap V(G_r))$, we now see $F_d \in I(X)$ or $G_r \in I(X)$.

WLOG, let $F_d \in I(X)$. There are two cases: either G_r is in $I(X)$ or not. We first prove the case when G_r isn't in $I(X)$.

Because $F_{d-1}G_r + F_d G_{r-1}$ is either zero or the second higher degree term of $FG \in I(X)$, we know $F_{d-1}G_r + F_d G_{r-1} \in I(X)$. This together with $F_d \in I(X)$ implies $F_{d-1}G_r \in I(X)$. It then follows from the irreducibility of X and $X = (X \cap V(F_{d-1})) \cup (X \cap V(G_r))$ that $F_{d-1} \in I(X)$. Similar arguments applies to show in order that $F_{d-2}, \dots, F_1 \in I(X)$, finishing the proof of the case $G_r \notin I(X)$.

For the case of $G_r \in I(X)$, just observe that $G_r \in I(X) \implies (F - F_d)(G - G_r) \in I(X)$, and repeat the arguments all over again.

(\impliedby): Assume for a contradiction that $X = (X \cap V_1) \cup (X \cap V_2)$ for some V_1, V_2 such that neither of them covers X . Clearly, there exists some homogeneous $F \in I(V_1)$ that doesn't vanish on the whole X . This F satisfies $I(V_1) - I(X)$. Similar argument gives us some homogeneous $G \in I(V_2) - I(X)$, but $FG \in I(X)$, a contradiction to $I(X)$ being prime. ■

Let $S \subseteq k[x_0, \dots, x_n]$ be some homogeneous ideal or collection of homogeneous polynomials. If necessary, we often distinguish the two vanishing sets in affine and projective setting by writing:

$$V_{\mathbb{P}}(S) \triangleq \{[x_0 : \dots : x_n] \in \mathbb{P}^n : F(x_0, \dots, x_n) = 0 \text{ for all } F \in S\}$$

and writing:

$$V_{\mathbb{A}}(S) \triangleq \{(x_0, \dots, x_n) \in \mathbb{A}^{n+1} : F(x_0, \dots, x_n) = 0 \text{ for all } F \in S\}.$$

Theorem 4.3.3. (Vanishing sets of collections of homogeneous polynomials are cones) Let $\pi : (\mathbb{A}^{n+1} - \{0\}) \rightarrow \mathbb{P}^n$ be the quotient map. Given any collection $S \subseteq k[x_0, \dots, x_n]$ of homogeneous polynomials, $V_{\mathbb{A}}(S)$ equals to either $\pi^{-1}(V_{\mathbb{P}}(S))$ or $\pi^{-1}(V_{\mathbb{P}}(S)) \cup \{0\}$.

Proof. It is trivial to check:

$$\pi(V_{\mathbb{A}}(S)) = V_{\mathbb{P}}(S) \quad (4.5)$$

Equation 4.5 finishes the proof because it implies $V_{\mathbb{A}}(S) - \{\mathbf{0}\} \subseteq \pi^{-1}(V_{\mathbb{P}}(S))$ and implies $\pi^{-1}(V_{\mathbb{P}}(S)) \subseteq V_{\mathbb{A}}(S)$. ■

Let $S \subseteq k[x_0, \dots, x_n]$ be a collection of homogeneous polynomials. We often call $V_{\mathbb{A}}(S)$ **cone**. This notion helps us prove the following result.

Theorem 4.3.4. (Zariski topology on projective space is the quotient topology)
The quotient map $\pi : (\mathbb{A}^{n+1} - \{\mathbf{0}\}) \rightarrow \mathbb{P}^n$ is a topological quotient map.

Proof. To prove that π is a topological quotient, we need to show that π is surjective, continuous, and every subset of \mathbb{P}^n that has closed preimage is closed. Clearly π is surjective. To see π is continuous, just observe for every collection S of homogeneous polynomials, we have

$$\pi(V_{\mathbb{A}}(S)) = V_{\mathbb{P}}(S) \quad (4.6)$$

Note that if the underlying field is finite, then the Zariski topologies are discrete so the assertion holds trivially. We from now suppose the underlying field k is infinite. Suppose $E \subseteq \mathbb{P}^n$ have closed preimage $\pi^{-1}(E) = V_{\mathbb{A}}(T) - \{\mathbf{0}\}$, where $T \subseteq k[x_0, \dots, x_n]$. We show

$$E = V_{\mathbb{P}}(\{F_i \in k[x_0, \dots, x_n] : F_i \text{ is the homogeneous component of some } F \in T.\})$$

The " \supseteq " holds true trivially. We now show the " \subseteq ". Fix $F \in T$ with homogeneous decomposition $F = \sum F_i$. We are required to prove F_i all vanish on E . Fix $[x_0 : \dots : x_n] \in E$. We are required to prove all F_i vanish at $[x_0 : \dots : x_n]$. Define formal polynomial $p(y) \in k[y]$ by:

$$p(y) \triangleq \sum F_i(x_0, \dots, x_n)y^i = \sum F_i(yx_0, \dots, yx_n)$$

Assume for a contradiction that there exists some F_i such that $F_i(x_0, \dots, x_n) \neq 0$. Because k is infinite, by **polynomial identity principal**, there exists nonzero $y' \in k$ such that $p(y') \neq 0$. However, because by definition $(y'x_0, \dots, y'x_n) \in \pi^{-1}(E)$ and because F vanish on $\pi^{-1}(E)$, we also have:

$$0 = F(y'x_0, \dots, y'x_n) = \sum F_i(y'x_0, \dots, y'x_n) = p(y')$$

a contradiction. ■

We now enter the better behaved and smaller category: when the underlying field is algebraically closed. In particular, we prove the famous **projective Nullstellensatz**:

Theorem 4.3.5. (Homogeneous or Projective Nullstellensatz) Given algebraically closed field k and homogeneous ideal $\mathfrak{a} \subseteq k[x_0, \dots, x_n]$, if $V(\mathfrak{a})$ is nonempty¹¹, then

$$I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$$

Proof. Clearly we have:

$$\sqrt{\mathfrak{a}} \subseteq I(V(\mathfrak{a}))$$

We now prove $I(V(\mathfrak{a})) \subseteq \sqrt{\mathfrak{a}}$. Because **affine Nullstellensatz** said that $\sqrt{\mathfrak{a}} = I(V_{\mathbb{A}}(\mathfrak{a}))$, we only have to prove $I(V_{\mathbb{P}}(\mathfrak{a})) \subseteq I(V_{\mathbb{A}}(\mathfrak{a}))$. Fixing homogeneous $F \in I(V_{\mathbb{P}}(\mathfrak{a}))$ and $\mathbf{x} \in V_{\mathbb{A}}(\mathfrak{a})$, we are required to prove F vanishes at \mathbf{x} . If F is zero, there is nothing to prove, so we from now on suppose F is nonzero. Because by premise $V_{\mathbb{P}}(\mathfrak{a})$ is nonempty, we know F can not be nonzero constant. In other words, homogeneous F have positive degree. **Theorem 4.3.3** said that $V_{\mathbb{A}}(\mathfrak{a})$ either equals to $\pi^{-1}(V_{\mathbb{P}}(\mathfrak{a}))$ or $\pi^{-1}(V_{\mathbb{P}}(\mathfrak{a})) \cup \{0\}$. If $\mathbf{x} = \mathbf{0}$, then F vanishes at \mathbf{x} because F is homogeneous with positive degree. If $\mathbf{x} \in \pi^{-1}(V_{\mathbb{P}}(\mathfrak{a}))$, then F vanishes at \mathbf{x} because it vanishes at $\pi(\mathbf{x})$. ■

Theorem 4.3.6. (Special case of projective Nullstellensatz) Given algebraically closed field k and homogeneous ideal $\mathfrak{a} \subseteq k[x_0, \dots, x_n]$, the followings are equivalents:

- (i) $V_{\mathbb{P}}(\mathfrak{a})$ is empty.
- (ii) $\sqrt{\mathfrak{a}} = k[x_0, \dots, x_n]$ or $\sqrt{\mathfrak{a}} = \{F \in k[x_0, \dots, x_n] : F(0) = 0\}$.

Proof. (i) \implies (ii): **Theorem 4.3.3** implies $V_{\mathbb{A}}(\mathfrak{a})$ either is empty or contains only the origin. This together with **affine Nullstellensatz** proves (ii).

(ii) \implies (i): **Affine Nullstellensatz** said that $I(V_{\mathbb{A}}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$. No matter which one $\sqrt{\mathfrak{a}}$ actually is, it must contains $\{x_0, \dots, x_n\}$. This implies $V_{\mathbb{A}}(\mathfrak{a}) \subseteq \{0\}$, which proves (i) by **Theorem 4.3.3**. ■

¹¹This implies \mathfrak{a} contains no nonzero constant.

4.4 Quasi variety morphism

By a **quasi affine (or projective) variety** $X \subseteq \mathbb{A}^n$ (resp. \mathbb{P}^n), we mean X is a subset of some variety $V \subseteq \mathbb{A}^n$ (resp. \mathbb{P}^n) and X is open in V , or equivalently¹² that X is irreducible and open in its closure.

A **normal variety** is a variety whose local ring at each point is regular. Because regular local rings are integrally closed domain¹³, smooth varieties are normal.

Equivalent Definition 4.4.1. (Normal variety in \mathbb{CP}^n) Let $X \subseteq \mathbb{CP}^n$ be a variety. X is normal if and only if there exists some collection of open $U_\alpha \subseteq X$ such that:

- (i) $X = \bigcup U_\alpha$.
- (ii) U_α are quasi-variety isomorphic to some affine variety.
- (iii) Coordinate rings $A(U_\alpha)$ of U_α are integrally closed domain.

Proof. ■

Equivalent Definition 4.4.2. (Serre's criteria for normality) Let A be an Noetherian ring. A is integrally closed domain if and only if for each $\mathfrak{p} \in \text{Spec}(A)$, we have $\text{ht}(\mathfrak{p}) \leq 1$, $A_{\mathfrak{p}}$ is regular, and $\text{depth}(A_{\mathfrak{p}}) \geq \inf \{2, \text{ht}(\mathfrak{p})\}$.

Proof. ■

Given some quasi affine variety $X \subseteq \mathbb{A}^n$ and $f : X \rightarrow k$, we say f is **regular at** $p \in X$ if there exist $U \subseteq X$ open in X containing p and exist $G, H \in k[x_1, \dots, x_n]$ such that H nonzero on U and $f = G/H$ on U . In the projective setting, says $X \subseteq \mathbb{P}^n$ is a quasi projective variety and f maps X into k , we say f is **regular at** $p \in X$ if there exists $U \subseteq X$ containing p and open in X such that there exists homogeneous $G, H \in k[x_0, \dots, x_n]$ such that H nonzero on U , $f = G/H$ on U , and G, H have same degree. Given a quasi variety X , we say $f : X \rightarrow k$ is **regular** if it is regular at each points of X . Here, we make the important remark that the set of regular functions $f : X \rightarrow k$ always form a ring. ¹⁴

Theorem 4.4.3. (Regular functions are continuous) Given quasi variety $X \subseteq \mathbb{A}^n$ (or \mathbb{P}^n), if $f : X \rightarrow k$ is regular, then f is continuous.

¹²See [Equivalent Definition 4.1.3](#) and [Corollary 4.1.1](#)

¹³This is highly nontrivial.

¹⁴It is IMPORTANT to deduce that regular functions indeed forms a ring here, since it is impossible to later check transitivity of [equivalence 4.7](#) purely topologically, without using the algebraic result of one regular functions minus another is still regular, thus continuous. I guess the moral of the story here is that one must remember \mathbb{A}^1 is a field, and thus have a field structure, which shall be used when topological method doesn't work; or that if something forms an algebraic structure, then utilize that structure as much as possible. Indeed, we are talking about ALGEBRAIC geometry here.

Proof. Because every closed set in k is either finite or the whole space¹⁵, we only have to show $f^{-1}(a)$ is closed for fixed $a \in k$. Let $(U_i, G_i, H_i)_{i \in I}$ cover X , where H_i nonzero and $f = G_i/H_i$ on U_i . Because X is coherent¹⁶ with $(U_i)_I$, we only have to show $U_i \cap f^{-1}(a)$ is closed in U_i for fixed $i \in I$, which follows from noting $U_i \cap f^{-1}(a) = V(G_i - aH_i) \cap U_i$. ■

Let X be a quasi variety with $p \in X$. Consider the collection of all $(U \subseteq X, f : U \rightarrow k)$, where U is nonempty open and f is regular, because **regular functions are continuous** and **nonempty open subset of irreducible space is always dense**, we may well define an equivalence relation by:

$$(U, f) \sim (O, g) \iff f = g \text{ on } U \cap O \quad (4.7)$$

to form the **function field** $K(X)$ of X . The germ-based (equivalence class) approach to defining function fields provides a way to collect all possible regular "functions" on a variety X . These regular functions need not be defined on all of X , but only on some nonempty open subset of it. Given any $[(U, f)] \in K(X)$, there exists a unique representative (U_{\max}, f_{\max}) such that f_{\max} is defined on the largest open subset of X where all representatives agree. We refer to this representative when writing $f \in K(X)$, implicitly identifying the element of the function field with its maximal domain. We say that a function $f \in K(X)$ is **defined at** a point $x \in X$ if the maximal representative of f is defined at x .

Let $f \in K(X)$. If f is defined and doesn't vanish at p , then clearly there exists $g \in K(X)$ such that $fg = 1$ on some neighborhood of p . This implies that indeed $K(X)$ is a field. Clearly, the collection of all $f \in K(X)$ that are defined at p forms a ring, which we denote as $\mathcal{O}_{p,X}$. Moreover, clearly the units of $\mathcal{O}_{p,X}$ are exactly those who doesn't vanish at p , which implies the non-units, those vanish at p , forms an ideal of $\mathcal{O}_{p,X}$, justifying the convention of calling $\mathcal{O}_{p,X}$ the **local ring of X at p** ¹⁷. Moreover, clearly the collection of all $f \in K(X)$ that are globally defined also forms a ring, which we denote by $\mathcal{O}(X)$. Note that the three structures are all k -algebras.

Let X be some quasi variety, and let $U \subseteq X$ be open nonempty. Given $u \in U$, we identify $K(U) = K(X)$ and $\mathcal{O}_{u,U} = \mathcal{O}_{u,X}$ as k -algebras the obvious way¹⁸. Let Y be another quasi variety. We say $\varphi : U \rightarrow Y$ is a **quasi variety morphism** if φ is continuous and for

¹⁵To see such, consider **Hilbert Basis Theorem** and fundamental theorem of algebra.

¹⁶You may Google what does **coherent topology** mean. To see that every topological space X and any of its open cover U_i are always coherent, just observe for any $Z \subseteq X$, we have $Z = \bigcup (U_i \cap Z)$ and $X - Z = \bigcup (U_i - Z)$.

¹⁷Recall that if the set of non-units forms an ideal, then the ring is local.

¹⁸Every element of $K(U)$ is a subset of some unique element of $K(X)$.

every $f \in K(Y)$, the function $f \circ \varphi : \varphi^{-1}(\text{Dom } f) \rightarrow k$ is regular. Clearly, this induces a k -algebra homomorphism $\varphi^* : K(Y) \rightarrow K(U) = K(X)$ defined by

$$[(W, f)] \mapsto [(\varphi^{-1}(W), f \circ \varphi)]$$

which we call **the dual map of φ** , and clearly it always map $\mathcal{O}_{y,Y}$ into $\bigcap_{x \in \varphi^{-1}(y)} \mathcal{O}_{x,X}$.

If we say $\varphi : X \rightarrow Y$ is a **quasi variety isomorphism**, we mean that φ is bijective with its inverse being also a quasi variety morphism. Clearly, if X, Y are quasi variety isomorphic, then we have three pairs of isomorphic k -algebras. Because of such, we often say $\mathcal{O}(X)$, $\mathcal{O}_{p,X}$, and $K(X)$ are **invariant up to quasi variety isomorphisms**. As we shall show later in **the section on rational map**, unlike ring of globally defined regular function, $K(X)$ is in fact invariant up to a even weaker condition if we consider only varieties.

Theorem 4.4.4. (If and only if test for quasi variety mapping whose target is affine) Given quasi variety mapping $\varphi : X \rightarrow Y \subseteq \mathbb{A}^n$,

$$\varphi \text{ is a quasi variety morphism.} \iff x_i \circ \varphi : X \rightarrow k \text{ are all regular.}$$

Proof. (\implies) follows from definition. We now prove (\impliedby). Clearly, because regular function on X is closed under addition and multiplication **as noted before**, for all $F \in k[x_1, \dots, x_n]$, the function $F \circ \varphi$ must be regular. It then follows from **continuity of regular functions** and

$$\varphi^{-1}(V(S) \cap Y) = \bigcap_{F \in S} (F \circ \varphi)^{-1}(0), \quad \text{for any } S \subseteq k[x_1, \dots, x_n]$$

that φ is continuous. Fix $(U, g) \in K(Y)$ and $p \in \varphi^{-1}(U)$. It remains to prove $g \circ \varphi : \varphi^{-1}(U) \rightarrow k$ is regular at p . Because $U \xrightarrow{g} k$ is regular, there exists open $O \subseteq U$ containing $\varphi(p)$ such that $g = \frac{H_1}{H_2}$ on O for some $H_1, H_2 \in k[x_1, \dots, x_n]$ where H_2 nonzero on whole O and degree of them being the same if X is projective. Clearly,

$$g \circ \varphi = \frac{H_1 \circ \varphi}{H_2 \circ \varphi}, \quad \text{on } \varphi^{-1}(O).$$

Because $H_1 \circ \varphi$ and $H_2 \circ \varphi$ are regular as function from X to k as we proved in the first paragraph of this proof, we know there exists open $V \subseteq \varphi^{-1}(O)$ containing p such that

$$H_1 \circ \varphi = \frac{F_1}{F_2} \text{ and } H_2 \circ \varphi = \frac{F_3}{F_4}, \quad \text{on } V$$

for some polynomials F_1, F_2, F_3, F_4 , with F_2, F_4 nonzero on V and the pairs having the same degree if X projective. This give us

$$g \circ \varphi = \frac{F_1 F_4}{F_2 F_3}, \quad \text{on } V$$

where $\deg(F_1F_4) = \deg(F_2F_3)$ if X is projective. We have shown that indeed $g \circ \varphi$ is regular at p . ■

Corollary 4.4.5. (Quasi variety embedding of complement of hypersurface in infinite affine space into one-higher dimensional affine space as a hypersurface)

Let k be infinite and $F \in k[x_1, \dots, x_n]$. The projection $\pi : \mathbb{A}^{n+1} \rightarrow \mathbb{A}^n$

$$(x_1, \dots, x_{n+1}) \rightarrow (x_1, \dots, x_n)$$

when restricted onto $V(x_{n+1}F - 1)$ is a quasi variety isomorphism from $V(x_{n+1}F - 1)$ to $\mathbb{A}^n - V(F)$.

Proof. It is easy to check that π restrict to a bijection between $V(x_{n+1}F - 1)$ and $\mathbb{A}^n - V(F)$ with the inverse being $(\mathbf{a}) \mapsto (\mathbf{a}, F^{-1}(\mathbf{a}))$. It then follows from [Theorem 4.4.4](#) that indeed the restriction of π forms a quasi variety isomorphism. ■

One particular key observation on [Theorem 4.4.4](#) is that it proves the continuity of a given map WITHOUT constructing pullbacks of polynomials, but simply claim the preimage of vanishing set is closed via [continuity of regular functions](#). A nontrivial technique indeed, go on to show the importance of [continuity of regular functions](#). We close this section by proving [Theorem 4.4.6](#), which will prove pivotal in later development, as it reduce lots of argument in the projective setting back to affine space. For ease in its proof, we first introduce two notions. Let S be the collection of homogeneous elements of $k[x_0, \dots, x_n]$. Clearly, we may well-define mappings $\alpha : S \rightarrow k[x_1, \dots, x_n]$ and $\beta : k[x_1, \dots, x_n] \rightarrow S$ by

$$\alpha(F) \triangleq F(1, x_1, \dots, x_n) \text{ and } \beta(G) \triangleq x_0^{\deg(G)} g\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right)$$

Let $F \in S$ and $G \in k[x_1, \dots, x_n]$. We refer to $\alpha(F)$ as the **dehomogenization** of F , and we refer to $\beta(G)$ as the **homogenization** of G . Actions of homogenization are actually easy to memorize. For example, homogenization send $x_2 - x_1^2$ to $x_0x_2 - x_1^2$, and send $x_2 - x_1^3$ to $x_2x_0^2 - x_1^3$. Dehomogenization sends $x_0x_2^2 + x_1^3$ to $x_2^2 + x_1^3$.

Theorem 4.4.6. (Standard embedding of \mathbb{A}^n into \mathbb{P}^n) Let $U \triangleq \mathbb{P}^n - V(x_0)$. The map $\varphi : U \rightarrow \mathbb{A}^n$ defined by

$$\varphi([x_0 : \dots : x_n]) \triangleq \left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right)$$

is a well-defined homeomorphism, and moreover a quasi variety isomorphism if the underlying field k is infinite.

Proof. It is routine to check φ is well-defined and bijective. We now prove it is indeed bi-continuous. Let $Y \subseteq U$ be closed in U , and let \overline{Y} be the closure of Y in \mathbb{P}^n . By definition,

there exists some collection T of homogeneous polynomials $F \in k[x_0, \dots, x_n]$ whose locus is exactly \bar{Y} . To see $\varphi(Y)$ is closed, just check $\varphi(Y)$ is the locus of the dehomogenizations of T . Conversely, given closed $W \subseteq \mathbb{A}^n$, we know there exists $T \subseteq k[x_1, \dots, x_n]$ whose locus is exactly W . To see $\varphi^{-1}(W)$ is closed, just check that $\varphi^{-1}(W)$ is the intersection between U and the locus of the homogenization of T . We have shown φ is indeed a homeomorphism.

From now on suppose k is infinite, and we wish to prove φ is moreover a quasi-variety isomorphism. To see U is indeed a quasi variety, note that **projective space is irreducible when underlying field is infinite** and that **nonempty subset of irreducible space is dense**.

Fix $(O, f) \in K(\mathbb{A}^n)$, where, WLOG, $f = F/G$ on O for some $F, G \in k[x_1, \dots, x_n]$ such that G nonzero on O . To see φ is indeed a morphism, just check $f \circ \varphi|_{\varphi^{-1}(O)} = (x_0^{\deg(G)} \tilde{F}) / (x_0^{\deg(F)} \tilde{G})$, where \tilde{F} and \tilde{G} are the homogenization of F and G . Fix $(O, f) \in K(U)$, where, WLOG, $f = F/G$ on O for some same degree homogeneous $F, G \in k[x_0, \dots, x_n]$ such that G nonzero on O . To see φ^{-1} is indeed a morphism, just check $f \circ \varphi^{-1}|_{\varphi(O)} = F_0/G_0$, where F_0 and G_0 are the dehomogenization of F and G . ■

4.5 Coordinate ring and function field

Given an affine quasi variety $X \subseteq \mathbb{A}^n$, its **coordinate ring** $A(X)$ is $A/I(X)$, which is clearly isomorphic to the ring of function $f : X \rightarrow k$ such that $f = F|_X$ for some $F \in k[x_1, \dots, x_n]$ ¹⁹. Because of the **prime-irreducibility correspondence in affine setting**, the coordinate of affine quasi variety is an integral domain. Later we will see more usage of the realization of $\Gamma(X)$ as ring of polynomial functions in the proof of **Theorem 4.5.1**.

Theorem 4.5.1. (Algebraic structure of global ring, local ring, and function field of affine quasi variety) If $X \subseteq \mathbb{A}^n$ is an affine quasi variety, then

- (i) $\mathcal{O}(X) \cong \Gamma(X)$.
- (ii) For all $p \in X$, if we let $\mathfrak{m}_p \subseteq \Gamma(X)$ be the maximal ideal corresponding to p , then $\mathcal{O}_{p,X} \cong \Gamma(X)_{\mathfrak{m}_p}$.
- (iii) $K(X) \cong \text{Frac}(\Gamma X)$.

Proof. Before the proof, we first remark that: If we fix p , regarding $\Gamma(X)$ either as the ring of polynomial function $f : X \rightarrow k$ or as the quotient $k[x_1, \dots, x_n]/I(X)$ makes no mathematical differences. In the former, $I(p) \subseteq \Gamma(X)$ is the ring of polynomial functions that vanishes at p , and in the latter, $I(p) \subseteq \Gamma(X)$ is the image of $I(p) \subseteq k[x_1, \dots, x_n]$ under the quotient map $k[x_1, \dots, x_n] \twoheadrightarrow k[x_1, \dots, x_n]/I(X)$. Either way, the $I(p) \subseteq \Gamma(X)$ is what we meant by \mathfrak{m}_p in (ii), and using the latter point of view with the bijection between \mathbb{A}^n and $\text{Max}(k[x_1, \dots, x_n])$, we have a bijection between X and $\text{Max}(\Gamma X)$: $p \leftrightarrow \mathfrak{m}_p = I(p)$.

Fix p . Let $\beta : \Gamma(X)_{\mathfrak{m}_p} \rightarrow \mathcal{O}_{p,X}$ be the obvious mapping²⁰: $F/G \mapsto [(U, F/G)]$ where $F, G : X \rightarrow k$ are polynomial function and $U = \{x \in X : G(x) \neq 0\}$. Clearly β is an injective ring homomorphism²¹. To see β is surjective, just recall the definition of regular function. We have constructed isomorphism $\beta : \Gamma(X)_{\mathfrak{m}_p} \rightarrow \mathcal{O}_{p,X}$, proving (ii). The same argument works for constructing isomorphism $\text{Frac}(\Gamma X) \cong K(X)$, proving (iii).

Let $\alpha : \Gamma(X) \rightarrow \mathcal{O}(X)$ be the obvious mapping, which is clearly an injective ring homo-

¹⁹We call these functions **polynomial functions**.

²⁰From β you can see that the done localization $\Gamma(X)_{\mathfrak{m}_p}$ is of geometrical nature, not algebraic.

²¹Note that $[(U, f)] = 0 \in \mathcal{O}_{p,X}$ if and only if $f = 0$ on U , since if $f \neq 0$ on U , then $f + f \neq f$. This implies injectivity of β since $f^{-1}(0) \subseteq X$ is closed in X , containing $g^{-1}(k^\times) \subseteq X$, whose closure in X are X . ($\because Z \subseteq Y \subseteq X \implies \text{cl}_Z(Y) = \text{cl}_X(X) \cap Y$)

morphism. It remains to prove α is surjective, which follows from checking the diagram:

$$\begin{array}{ccc}
\Gamma(X) & \xrightarrow{\alpha} & \mathcal{O}(X) \\
\updownarrow & & \updownarrow \\
\bigcap_{\mathfrak{m} \in \text{Max}(\Gamma X)} (\Gamma X)_{\mathfrak{m}} & \longleftrightarrow & \bigcap_{p \in X} \mathcal{O}_{p,X}
\end{array}$$

²²is indeed commutative, where the left and right sides are, respectively, subrings of $\text{Frac}(\Gamma X)$ and $K(X)$. ■

It may seem surprising that $\mathcal{O}(X) \cong \Gamma(X)$, since one might expect the former to be a localization of the latter, given that regular functions are defined locally as quotients of global polynomial functions. However, this apparent tension is actually a valuable opportunity to distinguish between the local and global perspectives: regularity is inherently a local notion. Indeed, by definition, a function $f : X \rightarrow k$ is regular if, locally, it can be written as a fraction G/H with $G, H \in \Gamma(X)$.

In fact, if one attempts to show that $\mathcal{O}_{p,X}$ is the localization $(f \in \mathcal{O}(X) : f(p) \neq 0)^{-1} \mathcal{O}(X)$ —that is, to verify that the obvious map $\mathcal{O}(X) \rightarrow \mathcal{O}_{p,X}$ satisfies the universal property—without invoking [Theorem 4.5.1](#), one quickly encounters difficulties and will be forced to use isomorphism $\mathcal{O}(X) \cong \Gamma(X)$ ²³.

Now, let X, Y be two quasi varieties with Y affine. It is clear that the three structures $\mathcal{O}(X)$, $\mathcal{O}_{p,X}$, and $K(X)$ all admit obvious k -algebra structures, and from the proof of [Theorem 4.5.1](#), the ring isomorphism $\mathcal{O}(Y) \cong \Gamma(Y)$ is also a k -algebra isomorphism.

Theorem 4.5.2. (Induction forms a bijection between set of quasi varieties of morphism and set of k -algebra homomorphism from target's coordinate ring to source's global ring if target is affine) Let X, Y be two quasi varieties with $Y \subseteq \mathbb{A}^n$. Denoting the collection of quasi variety morphisms $X \rightarrow Y$ by $\text{Hom}(X, Y)$ and the collection of k -algebra homomorphism $\Gamma(Y) \rightarrow \mathcal{O}(X)$ by $\text{Hom}(\mathcal{O}(X), \Gamma(Y))$, clearly we can well define a map $\text{Hom}(X, Y) \xrightarrow{\alpha} \text{Hom}(\Gamma(Y), \mathcal{O}(X))$ by

$$\varphi \mapsto (\tilde{\varphi} : \Gamma(Y) \rightarrow \mathcal{O}(X)), \quad \text{where } \tilde{\varphi}(F) \triangleq F \circ \varphi.$$

Such α is bijective.

²²The left isomorphism is explained in [this paragraph](#) of [Section 1.4](#), the bottom isomorphism is from (ii), and the right injective homomorphism is from this paragraph of this section.

²³As the action of isomorphism α in [Theorem 4.5.1](#) suggest, one can really just write $\mathcal{O}(X) = \Gamma(X)$

Proof. Fix $h \in \text{Hom}(\Gamma(Y), \mathcal{O}(X))$. Consider $x_i \in \Gamma(Y)$, $\xi_i \triangleq h(x_i) \in \mathcal{O}(X)$, and $\psi : X \rightarrow \mathbb{A}^n$ defined by $\psi(p) \triangleq (\xi_1(p), \dots, \xi_n(p))$. Because α is clearly injective²⁴, our end goal here is to show that $\psi \in \text{Hom}(X, Y)$ and $h = \tilde{\psi}$.

Because $Y = V(I(Y))$, to show that ψ at least forms a map from X to Y , we only have to show $F \circ \psi = 0$ for any fixed $F \in I(Y)$. Because h is a k -algebra homomorphism and F in k -algebra $\Gamma(Y)$ can be appropriately (See footnote) generated by x_i , we have $h(F) = F(h(x_1), \dots, h(x_n))$ ²⁵. This by definition of ξ and ψ give us

$$h(F) = F(\xi_1, \dots, \xi_n) = F \circ \psi \quad (4.8)$$

This together with the fact F as an element of $\Gamma(Y)$ is zero implies, indeed, $F \circ \psi = 0$.

Noticing that Equation 4.8 also holds true for any $F \in \Gamma(Y)$ ²⁶ that's not in $I(Y)$, we conclude that if ψ really is a morphism, then we will have $h = \tilde{\psi}$. Therefore, it only remains to show ψ is indeed a morphism, which follows from $x_i \circ \psi = \xi_i \in \mathcal{O}(X)$ for all $x_i \in k[x_1, \dots, x_n]$ and Test 4.4.4. ■

Corollary 4.5.3. (Quasi affine varieties are isomorphic if and only if their coordinate ring are isomorphic as k -algebra) Let X, Y be two quasi affine variety. We have

$$X, Y \text{ isomorphic as quasi variety} \iff \Gamma(Y), \Gamma(X) \text{ isomorphic as } k\text{-algebra}.$$

Proof. If $\varphi : X \rightarrow Y$ is a quasi variety isomorphism, then $\tilde{\varphi} : \Gamma(Y) \rightarrow \Gamma(X)$ is a k -algebra isomorphism with inverse $\tilde{\varphi}^{-1} : \Gamma(X) \rightarrow \Gamma(Y)$. If $\phi : \Gamma(Y) \rightarrow \Gamma(X)$ is a k -algebra isomorphism, then the unique morphism $\varphi : X \rightarrow Y$ that satisfies $\tilde{\varphi} = \phi$ is an isomorphism with the obvious inverse. ■

Given a projective quasi variety $X \subseteq \mathbb{P}^n$, we also use notation $\Gamma(X)$ to denote its **homogeneous coordinate ring** $k[x_0, \dots, x_n]/I(X)$, where $I(X)$ are the defining ideal of X , the ideal generated by homogeneous polynomials vanishing on X . We have shown that coordinate rings of affine quasi varieties are invariant up to isomorphisms, and we are going to show coordinate rings of projective quasi varieties are not.

Theorem 4.5.4. (Obvious grading of the quotient of graded ring) Given \mathbb{Z}_0^+ -graded ring A , homogeneous ideal $I \subseteq A$, and quotient ring $\pi : A \rightarrow A/I$, we have a well defined

²⁴A direct proof suffices. It is easy to construct $F \in k[x_1, \dots, x_n]$ for arbitrary $p_1 \neq p_2 \in \mathbb{A}^n$ that satisfies $F(p_1) \neq F(p_2)$.

²⁵For example, $h(x_1^2 + x_2) = (h(x_1))^2 + h(x_2)$. Note that the F on the left hand side is an element of $\Gamma(Y)$, and that the F on the right hand side is an actual polynomial.

²⁶Perhaps here it will be better to write $k[x_1, \dots, x_n]$ in place of $\Gamma(Y)$.

\mathbb{Z}_0^+ -grading on A/I :

$$A/I = \bigoplus_{n \geq 0} \pi(A_n)$$

Proof. Clearly $\pi(A_n)$ all form groups, and $A/I = \sum \pi(A_n)$. It remains to show the sum is direct. Suppose

$$\pi(a_{n_r}) = \sum_{i=1}^{r-1} \pi(a_{n_i}), \quad \text{where } n_i \text{ distinct and } a_{n_i} \in A_{n_i}$$

We are required to show $a_{n_r} \in I$. Clearly, we have $n_r > n_i$ for all $i < r$ and

$$a_{n_r} - \sum_{i=1}^{r-1} a_{n_i} \in I$$

This implies

$$a_{n_r} = \sum_{i=1}^{r-1} a_{n_i} + b, \quad \text{for some } b \in I$$

Note that I is homogeneous, so there exists unique decomposition of $b = a_{n_r} - \sum_{i=1}^{r-1} a_{n_i}$ as elements of $A_n \cap I$. By comparing the degrees of the elements of the unique decomposition of b and $a_{n_r} - \sum_{i=1}^{r-1} a_{n_i}$, we see that the unique decomposition of b is exactly $a_{n_r} - \sum_{i=1}^{r-1} a_{n_i}$, i.e., $a_{n_i} \in I$ for all $i \leq r$. ■

Let X be a projective quasi variety. From now on, we regard $\Gamma(X)$ as a \mathbb{Z}_0^+ -graded ring, whose grading come from [Theorem 4.5.4](#).

Let A be a graded ring, and $\mathfrak{p} \subseteq A$ a homogeneous prime ideal. Clearly the set S of homogeneous elements not in \mathfrak{p} forms a multiplicatively closed subset.

Theorem 4.5.5. (Obvious grading on homogeneous localizations: What we mean by $A_{(\mathfrak{p})}$) Given a \mathbb{Z}_0^+ -graded ring A , if $\mathfrak{p} \subseteq A$ is homogeneous prime and we denote S the set of homogeneous element not in \mathfrak{p} , then we may well define a \mathbb{Z} -grading on $S^{-1}A$ by letting

$$(S^{-1}A)_n \triangleq \{f/g \in S^{-1}A : f \text{ homogeneous and } n = \deg f - \deg g\} \cup \{0\}$$

Proof. To check that $(S^{-1}A)_n$ are well-defined as sets, we are required to show

$$\frac{a_1}{s_1} = \frac{a_2}{s_2} \in S^{-1}A \text{ and } a_1 \text{ homo} \implies a_2 \text{ homo and } \deg a_1 - \deg s_1 = \deg a_2 - \deg s_2$$

Because $a_1/s_1 = a_2/s_2 \in S^{-1}A$, we know $a_1s_2u = a_2s_1u$ for some $u \in S$. By definition and premise, a_1, s_2, s_2 , and u are all homogeneous, which with $a_1s_2u = a_2s_1u$ implies a_2 is indeed homogeneous with $\deg a_1 - \deg s_1 = \deg a_2 - \deg s_2$. Clearly $(S^{-1}A)_n$ all form groups, $S^{-1}A = \sum (S^{-1}A)_n$, and $(S^{-1}A)_n(S^{-1}A)_m \subseteq (S^{-1}A)_{n+m}$. It remains to prove the sum is direct. Suppose

$$\frac{a}{s} = \frac{a_0}{s_0} + \cdots + \frac{a_n}{s_n}$$

where $a/s \in (S^{-1}A)_m$ and $a_i/s_i \in (S^{-1}A)_{n_i}$ such that n_i all distinct and not equal to m . We are required to show $\frac{a}{s} = 0$. From

$$\frac{a}{s} = \frac{a_0s_1 \cdots s_n + \cdots + a_ns_0 \cdots s_{n-1}}{s_0 \cdots s_n}$$

We know that either

$$\frac{a_0s_1 \cdots s_n + \cdots + a_ns_0 \cdots s_{n-1}}{s_0 \cdots s_n} = 0$$

or $(a_0s_1 \cdots s_n + \cdots + a_ns_0 \cdots s_{n-1})$ homogeneous with

$$\deg(a) + \deg(s_0 \cdots s_n) = \deg(a_0s_1 \cdots s_n + \cdots + a_ns_0 \cdots s_{n-1}) + \deg(s).$$

Assume for a contradiction that $a_0s_1 \cdots s_n + \cdots + a_ns_0 \cdots s_{n-1}$ is homogeneous. WLOG, we have

$$\deg(a) + \deg(s_0 \cdots s_n) = \deg(a_0s_1 \cdots s_n) + \deg(s).$$

which implies

$$\deg(a) + \deg(s_0) = \deg(a_0) + \deg(s)$$

a contradiction to the definition of a_0/s_0 . ■

We use the notation $A_{(\mathfrak{p})}$ to denote the $(S^{-1}A)_0$ in [Theorem 4.5.5](#). Clearly $A_{(\mathfrak{p})}$ is also a local ring with maximal ideal $\{a/s \in A_{(\mathfrak{p})} : a \in \mathfrak{p}\}$ ²⁷. In particular, this local ring becomes a field when $\mathfrak{p} = 0$, and in such case we write $A_{(\mathfrak{p})} = A_{(\langle 0 \rangle)}$.

Theorem 4.5.6. (Obvious grading on homogeneous localizations: What we mean by $A_{(f)}$) Given some \mathbb{Z}_0^+ -graded ring A and homogeneous $f \in A$, we may well define a \mathbb{Z} -grading on A_f by letting

$$(A_f)_n \triangleq \left\{ \frac{g}{f^l} \in A_f : g \text{ homogeneous and } n = \deg(g) - l \deg(f) \right\} \cup \{0\}$$

²⁷This set is clearly the set of non units of $A_{(\mathfrak{p})}$, and it clearly forms an ideal of $A_{(\mathfrak{p})}$

Proof. To check that $(A_f)_n$ are well defined as sets, we are required to show

$$\frac{g_1}{f^{l_1}} = \frac{g_2}{f^{l_2}} \in A_f \text{ and } g_1 \text{ homo} \implies g_2 \text{ homo and } \deg(g_1) - \deg(f^{l_1}) = \deg(g_2) - \deg(f^{l_2})$$

whose proof is similar to the one in [Theorem 4.5.5](#). Again, clearly $(A_f)_n$ all form groups, $A_f = \sum (A_f)_n$, and $(A_f)_n(A_f)_m \subseteq (A_f)_{n+m}$. It remains to prove the sum is direct. Suppose

$$\frac{g_0}{f^{l_0}} = \frac{g_1}{f^{l_1}} + \dots + \frac{g_n}{f^{l_n}}$$

where $g_i/f^{l_i} \in (A_f)_{r_i}$ and r_i are all distinct. We are required to show $\frac{g_0}{f^{l_0}} = 0$. From

$$\frac{g_0}{f^{l_0}} = \frac{g_1 f^{l_2+\dots+l_n} + \dots + g_n f^{l_1+\dots+l_{n-1}}}{f^{l_1+\dots+l_n}}$$

We know that either

$$\frac{g_1 f^{l_2+\dots+l_n} + \dots + g_n f^{l_1+\dots+l_{n-1}}}{f^{l_1+\dots+l_n}} = 0$$

or $(g_1 f^{l_2+\dots+l_n} + \dots + g_n f^{l_1+\dots+l_{n-1}})$ homogeneous with

$$\deg(g_0) - \deg(f^{l_0}) = \deg(g_1 f^{l_2+\dots+l_n} + \dots + g_n f^{l_1+\dots+l_{n-1}}) - \deg(f^{l_1+\dots+l_n})$$

Assume for a contradiction that $g_1 f^{l_2+\dots+l_n} + \dots + g_n f^{l_1+\dots+l_{n-1}}$ is homogeneous. WLOG, we have

$$\deg(g_0) - \deg(f^{l_0}) = \deg(g_1 f^{l_2+\dots+l_n}) - \deg(f^{l_1+\dots+l_n})$$

which implies

$$\deg(g_0) - \deg(f^{l_0}) = \deg(g_1) - \deg(f^{l_1})$$

a contradiction to the premise $r_0 \neq r_1$. ■

Again, we use the notation $A_{(f)}$ to denote the $(A_f)_0$ in [Theorem 4.5.6](#).

4.6 Category of quasi varieties

Theorem 4.6.1. ()

4.7 Segre embedding

Theorem 4.7.1. ()

Fix n and m . In this section, the underlying field k is always infinite, and we express elements of $\mathbb{P}^{(n+1)(m+1)-1}$ (not uniquely, of course) as matrices:

$$\begin{bmatrix} z_{0,0} & \cdots & z_{0,m} \\ \vdots & \ddots & \vdots \\ z_{n,0} & \cdots & z_{n,m} \end{bmatrix}$$

and use $k[z_{i,j}]$ to denote "the" polynomial ring. Now, consider the **Segre embedding** $\psi : \mathbb{P}^n \times \mathbb{P}^m \rightarrow \mathbb{P}^{(n+1)(m+1)-1}$ defined by

$$[x_0 : \cdots : x_n] \times [y_0 : \cdots : y_m] \mapsto \begin{bmatrix} x_0 y_0 & \cdots & x_0 y_m \\ \vdots & \ddots & \vdots \\ x_n y_0 & \cdots & x_n y_m \end{bmatrix}$$

It is clear that ψ is well-defined and injective. We shall show that the image of ψ is indeed irreducible closed to justify calling ψ an embedding.

Theorem 4.7.2. (Image of Segre embedding is closed) Let $\psi : \mathbb{P}^n \times \mathbb{P}^m \rightarrow \mathbb{P}^{(n+1)(m+1)-1}$ be the Segre embedding, and consider

$$S \triangleq \left\{ z_{i,j} z_{p,l} - z_{p,j} z_{i,l} \in k[z_{i,j}] : i, p \in \{0, \dots, n\} \text{ and } j, l \in \{0, \dots, m\} \right\}.$$

We have

$$\text{Im}(\psi) = V(S)$$

Proof. Clearly, we have $\text{Im}(\psi) \subseteq V(S)$. Suppose

$$\alpha \triangleq \begin{bmatrix} z_{0,0} & \cdots & z_{0,m} \\ \vdots & \ddots & \vdots \\ z_{n,0} & \cdots & z_{n,m} \end{bmatrix} \in V(S)$$

By definition, there exists some column of α that is nonzero. WLOG, let that column be the first one. To show $\alpha \in \text{Im}(\psi)$, we are required to show there exists some $\lambda_1, \dots, \lambda_m \in k$ such that

$$z_{i,j} = \lambda_j z_{i,0}, \quad \text{for all } i, j$$

then the proof will follow from noting α is the image of $[z_{0,0} : \cdots : z_{n,0}] \times [1 : \lambda_1 : \cdots : \lambda_m]$. WLOG, let $z_{0,0} \neq 0$. One may now check $\lambda_j \triangleq z_{0,j} z_{0,0}^{-1}$ suffices, using the premise $\alpha \in V(S)$. ■

Theorem 4.7.3. (Basic Property) Identifying $\mathbb{P}^n \times \mathbb{P}^m$ as a subspace of $\mathbb{P}^{(n+1)(m+1)-1}$ via Segre embedding ψ . If $C_1 \subseteq \mathbb{P}^n, C_2 \subseteq \mathbb{P}^m$ are closed, then $C_1 \times C_2 \subseteq \mathbb{P}^n \times \mathbb{P}^m$ is also closed.

Proof. Let $C_1 \triangleq V(P_1, \dots, P_r)$ and $C_2 \triangleq V(Q_1, \dots, Q_l)$. The proof follows from checking that the image of $C_1 \times C_2 \subseteq \mathbb{P}^{(n+1)(m+1)-1}$ is the intersection of image of $\mathbb{P}^n \times \mathbb{P}^m$ with:

$$\bigcap_{i,j} V(P_1(z_{0j}, \dots, z_{mj}), \dots, P_r(z_{0j}, \dots, z_{mj}), Q_1(z_{i0}, \dots, z_{in}), \dots, Q_l(z_{i0}, \dots, z_{in}))$$

■

Theorem 4.7.4. (Projection is indeed a close map) Identifying $\mathbb{P}^n \times \mathbb{P}^m$ as a subspace of $\mathbb{P}^{(n+1)(m+1)-1}$, the projection $\pi : \mathbb{P}^n \times \mathbb{P}^m \rightarrow \mathbb{P}^m$ is a closed map.

Proof. Let $C \subseteq \mathbb{P}^n \times \mathbb{P}^m$ be closed. We are required to prove $\pi(C)$ is closed. Let $\varphi_i : \mathbb{P}_{(i)}^m \rightarrow \mathbb{A}^m$ be the **standard open affine covering** of \mathbb{P}^m , where i runs through $\{0, \dots, m\}$. Because the topology of \mathbb{P}^m is coherent with the topologies of $\mathbb{P}_{(i)}^m$, to prove $\pi(C)$ is closed, we only have to prove $\pi(C) \cap \mathbb{P}_{(i)}^m$ are closed in $\mathbb{P}_{(i)}^m$. In other words, we wish to show $\varphi_i \circ \pi(C)$ is closed in \mathbb{A}^m .

Let $u_i : \mathbb{A}^n \rightarrow \mathbb{P}_{(i)}^n$ be the **standard quasi variety isomorphisms**.

■

Theorem 4.7.5. (Image of Segre embedding is irreducible) The image of the Segre embedding $\psi : \mathbb{P}^n \times \mathbb{P}^m \rightarrow \mathbb{P}^{(n+1)(m+1)-1}$ is irreducible.

Proof. Suppose $\mathbb{P}^n \times \mathbb{P}^m = A \cup B$ where A, B are closed. We are required to show $\mathbb{P}^n \times \mathbb{P}^m$ is covered either by A or by B . For each $[\mathbf{x}] \in \mathbb{P}^n$, let $X_{[\mathbf{x}]} \triangleq \{[\mathbf{x}]\} \times \mathbb{P}^m$. Because $X_{[\mathbf{x}]}$ is a subset of $\mathbb{P}^n \times \mathbb{P}^m$, we have:

$$X_{[\mathbf{x}]} = (A \cap X_{[\mathbf{x}]}) \cup (B \cap X_{[\mathbf{x}]})$$

This implies by irreducibility of $X_{[\mathbf{x}]}$ that either A or B covers $X_{[\mathbf{x}]}$. Define X_A to be the collection of $[\mathbf{x}] \in \mathbb{P}^n$ that makes A cover $X_{[\mathbf{x}]}$, and define X_B similarly. By construction, if $X_A = \mathbb{P}^n$, then A cover $\mathbb{P}^n \times \mathbb{P}^m$. A routine check shows that:

$$X_A = \bigcap_{[\mathbf{y}] \in \mathbb{P}^m} \pi_1((\mathbb{P}^n \times \{[\mathbf{y}]\}) \cap A)$$

Because \mathbb{P}^n is irreducible and we have shown $\mathbb{P}^n = X_A \cup X_B$, the proof moreover boils downs to proving X_A and X_B are closed.

So it remains to show projection $\pi_1 : \mathbb{P}^n \times \mathbb{P}^m \rightarrow \mathbb{P}^n$ is a closed map.

■

Consider formal polynomial $F \in k[x_0, \dots, x_n, y_0, \dots, y_m]$, and write $F = F_1 + \dots + F_r$ where F_i are all monomials of the forms $cx_0^{e_0} \dots x_n^{e_n} y_0^{e_{n+1}} y_m^{e_{n+m}}$. If for all i , **the degree of F_i in x** , the numbers $e_0 + \dots + e_n$, are the same, then we say F is **x -homogeneous**. We say F is **bi-homogeneous** if F is both **x -homogeneous** and **y -homogeneous**.

Clearly, if $F \in k[x_0, \dots, x_n, y_0, \dots, y_m]$ is bi-homogeneous, then we may well define its **vanishing set** on $\mathbb{P}^n \times \mathbb{P}^m$ the obvious way.

Theorem 4.7.6. (Zariski Topology on $\mathbb{P}^n \times \mathbb{P}^m$) Identifying $\mathbb{P}^n \times \mathbb{P}^m$ as a closed subset of $\mathbb{P}^{(n+1)(m+1)-1}$ via Segre embedding, not only every closed set $X \subseteq \mathbb{P}^n \times \mathbb{P}^m$ have the form

$$\{([x_0 : \dots : x_n], [y_0 : \dots : y_m]) \in \mathbb{P}^n \times \mathbb{P}^m : F(\mathbf{x}, \mathbf{y}) = 0 \text{ for all } F \in S\} \quad (4.9)$$

for some collection S of bi-homogeneous polynomials whose **x -degree** equals to its **y -degree**, but also for any collection S of bi-homogeneous polynomial, **Set 4.9** is closed.

Nontrivial. $F(\mathbf{y}) \mapsto \mathbf{x}F(\mathbf{y})$ won't work.

Proof. The "not only" part follows from checking given any $V(F_1, \dots, F_r) \subseteq \mathbb{P}^{(n+1)(m+1)-1}$, its preimage under Segre embedding equals to $V(\widetilde{F}_1, \dots, \widetilde{F}_r)$, where each $\widetilde{F}_i \in k[\mathbf{x}, \mathbf{y}]$ comes from substituting the $z_{i,j}$ in F_i with $x_i y_j$.

■

A routine check shows that every closed subset of $\mathbb{P}^n \times \mathbb{P}^m$ have the form where $S \subseteq k[x_0, \dots, x_n, y_0, \dots, y_m]$ is some collection of bi-homogeneous polynomials. Moreover, for each closed $X \subseteq \mathbb{P}^n \times \mathbb{P}^m$, there always exists bi-homogeneous polynomial collection S such that X equal to **Set 4.9** and such that for each $F \in S$, the degree of F in x equals to the degree of F in y .

Lemma 4.7.7. (Expected Behavior of Product) Identifying $\mathbb{P}^n \times \mathbb{P}^m$ as a closed subset of $\mathbb{P}^{(n+1)(m+1)-1}$ via Segre embedding, for all fixed $[x'_0 : \dots : x'_n] \in \mathbb{P}^n$, the set $[x'_0 : \dots : x'_n] \times \mathbb{P}^m$ is homeomorphic to \mathbb{P}^m .

Proof. Define $\varphi : \mathbb{P}^m \rightarrow [x'_0 : \dots : x'_n] \times \mathbb{P}^m$ by

$$[y_0 : \dots : y_m] \mapsto [x'_0 : \dots : x'_n] \times [y_0 : \dots : y_m]$$

We first prove that φ is a closed map. Fix $V(F_1, \dots, F_l) \in \mathbb{P}^m$. Define

$$\widetilde{S} \triangleq \left\{ x_j^{\deg(F_i)} F_i : 0 \leq j \leq n, 1 \leq i \leq l \right\}$$

Observe

$$\varphi(V(F_1, \dots, F_l)) = V(\widetilde{S})|_{[x'_0 : \dots : x'_n] \times \mathbb{P}^m}$$

We now prove that φ is continuous. Let $\{F_1, \dots, F_t\} \subseteq k[\mathbf{x}, \mathbf{y}]$ be some collection of bi-homogeneous polynomials whose \mathbf{x} -degree equal to its \mathbf{y} -degree. Observe

$$\varphi^{-1}(V(F_1, \dots, F_t)|_{[x'_0: \dots: x'_n] \times \mathbb{P}^m}) = V(\widetilde{F}_1, \dots, \widetilde{F}_t), \quad \text{where } \widetilde{F}_i(\mathbf{y}) \triangleq F_i(x'_0, \dots, x'_n, \mathbf{y})$$

■

Theorem 4.7.8. (Image of Segre embedding is irreducible)

As it turned out, to prove the image of Segre embedding is irreducible is extremely nontrivial and is often overlooked by people who are not careful enough²⁸.

Theorem 4.7.9. (Closed set of Segre embedding) Identifying the Cartesian product $\mathbb{P}^n \times \mathbb{P}^m$ as a subvariety of $\mathbb{P}^{(n+1)(m+1)-1}$ using Segre embedding,

Proof. Let $S \subseteq k[z_{i,j}]$ be some collection of homogeneous polynomial. For each homogeneous $F \in k[z_{i,j}]$, define \widetilde{F} by replacing $z_{i,j}$ with $x_i y_j$. Clearly,

$$\widetilde{S} \triangleq \left\{ \widetilde{F} \in k[x_0, \dots, x_n, y_0, \dots, y_m] : F \in S \right\}$$

is a collection of bi-homogeneous polynomial. Let $\psi : \mathbb{P}^n \times \mathbb{P}^m \rightarrow \mathbb{P}^{(n+1)(m+1)-1}$ be the Segre embedding. We claim preimage of $V(S) \cap \text{Im}(\psi)$ under Segre embedding indeed has the form [Set 4.9](#). ■

Theorem 4.7.10. (A part of universal property) If $\varphi : X \rightarrow \mathbb{P}^n, \psi : X \rightarrow \mathbb{P}^m$ are two quasi variety morphism, then $\varphi \times \psi : X \rightarrow \mathbb{P}^n \times \mathbb{P}^m$ defined in the obvious way is also a quasi variety morphism.

²⁸See these two MSE post:

<https://math.stackexchange.com/questions/984340/the-ideal-for-image-of-segre-embedding?noredirect=1&q=1>

<https://math.stackexchange.com/questions/139531/is-this-quotient-ring-mathbbcz-ij-ker-phi-integrally-closed>

for an outline of the proof. It is by nature combinatorial.

4.8 Rational map

Theorem 4.8.1. (Rational map is well-defined) Let X and Y be two quasi varieties, and let φ and ψ be two quasi varieties from X to Y . If there exists non empty open subset $U \subseteq X$ on which φ and ψ agree, then $\varphi = \psi$.

Proof. WLOG²⁹, let $Y = \mathbb{P}^n$. By **universal property**, $\varphi \times \psi : X \rightarrow \mathbb{P}^n \times \mathbb{P}^n$ is a quasi variety morphism. Clearly, the diagonal set $\Delta \triangleq \{[\mathbf{x}] \times [\mathbf{x}] \in \mathbb{P}^n \times \mathbb{P}^n : [\mathbf{x}] \in \mathbb{P}^n\}$ equals to the vanishing set $V(\{x_i y_j - x_j y_i : 0 \leq i, j \leq n\})$, and is thus closed. By premise, $\varphi \times \psi(U) \subseteq \Delta$. It then follows from continuity³⁰ of $\varphi \times \psi$, U being dense in X , and Δ being closed that $\varphi \times \psi(X) \subseteq \Delta$, which implies $\varphi = \psi$. ■

Let X and Y be two varieties. Because of **Theorem 4.8.1**, we may well-define **rational map** $\varphi : X \dashrightarrow Y$ to be equivalence³¹ class of pairs (U, φ_U) where U is a nonempty open subset of X and $\varphi_U : U \rightarrow Y$ is a quasi variety morphism. Again, this equivalence-class-based approach to defining rational map provides a way to collect all possible quasi varieties morphisms from nonempty open subset of X to Y . Given any $\varphi : X \dashrightarrow Y$, there exists a unique representative $(U_{\max}, \varphi_{U_{\max}}) \in \varphi$ such that $\varphi_{U_{\max}}$ is defined on the largest open subset of X where all representatives agree.³² Therefore, it make sense for us to say whether $\varphi : X \dashrightarrow Y$ is **defined at** $x \in X$.

Given a rational map $\varphi : X \dashrightarrow Y$, we say φ is **dominant** if for some and hence every³³ pair (U, φ_U) , the image of φ_U is dense in Y . We care much more about dominant rational map than non dominant rational map for following reasons:

- (i) We may well define composition of dominant rational maps.
- (ii) The composition of dominant rational is also dominant.³⁴

²⁹If Y is affine, by **Theorem 4.4.6**, there exists quasi variety isomorphism $Y \xrightarrow{\phi} Y' \subseteq \mathbb{P}^n$. If $\phi \circ \varphi : X \rightarrow Y'$ and $\phi \circ \psi : X \rightarrow Y'$ agree, then $\varphi = \phi^{-1} \circ \phi \circ \varphi$ and $\psi = \phi^{-1} \circ \phi \circ \psi$ also agree. In other words, we may WLOG let Y be projective. Let $j : Y \rightarrow \mathbb{P}^n$ be the inclusion. Because j is injective, if $j \circ \varphi$ and $j \circ \psi$ agree, then φ and ψ must agree. This allow us to WLOG suppose $Y = \mathbb{P}^n$.

³⁰Recall that one of the equivalent definition for function between two topological space to be continuous is that the functions maps closure of any subset A of domain into the closure of image of A .

³¹The relation is that two quasi varieties morphism agrees on the intersection on their domains.

³²To see such, note that X must be Noetherian **so any subspace is compact**, "union" of these morphism is continuous then follows from paste lemma, and the finite "union" of these morphism clearly pullback regular functions.

³³Let $U, V \subseteq X$ be open, and $\varphi(U)$ be dense in Y . Because U is irreducible, we know $U = \text{cl}_U(U \cap V)$, and because $\varphi : U \rightarrow Y$ is continuous, we know $\varphi(\text{cl}_U(U \cap V)) \subseteq \overline{\varphi(U \cap V)}$. Together, we have $Y = \overline{\varphi(U)} = \overline{\varphi(\text{cl}_U(U \cap V))} \subseteq \overline{\varphi(U \cap V)} \subseteq \overline{\varphi(V)}$.

³⁴Let $W \subseteq Z$ be open. We are required to show W intersect with $\psi_V(V \cap \varphi_U(U))$. Because $\psi_V(V) \subseteq Z$ is

(iii) Because for each open $U \subseteq X$, we have the identification $K(U) = K(X)$, we can well define dual map $\varphi^* : K(Y) \rightarrow K(X)$.

Moreover, the dual map of dominant rational map behave the way we all wish:

$$(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$$

If we say $\varphi : X \dashrightarrow Y$ is a **birational map**, we mean φ is dominant and there exists some dominant $\psi : Y \dashrightarrow X$ such that $\psi \circ \varphi : X \dashrightarrow X$ contains (X, id) and $\varphi \circ \psi : Y \dashrightarrow Y$ contains (Y, id) . Clearly, inverse of any birational map is unique and also a birational map. Two quasi varieties are said to be **birational equivalent** if there exists a birational map between them. Quasi varieties are always birational equivalent to their open subsets.

The reason we care about birational equivalence stemmed from that we care about the function field on varieties: One always study first about the functions on the object to make interesting conclusion of the object. As we have promise earlier, see the almighty **equivalent definition for birational equivalence**.

Theorem 4.8.2. (Basis consisting of "affine" variety) Each variety X has a basis whose elements are all quasi variety isomorphic to some affine variety.

Proof. Fix $p \in X$ and open $U \subseteq X$ containing p . We are required to find open $W \subseteq U$ containing p and quasi variety isomorphic to some affine variety.

For the affine case $X \subseteq \mathbb{A}^n$, first observe that because $\mathbb{A}^n - U$ is closed, there exists $F \in I(\mathbb{A}^n - U)$ such that $p \notin V(F)$. Clearly $W \triangleq X \cap (\mathbb{A}^n - V(F))$ is open in X , contains p , and is contained by U . It remains to show that W is quasi variety isomorphic to some affine variety.

By **Theorem 4.4.5**, there exists a quasi variety isomorphism $\psi : \mathbb{A}^n - V(F) \rightarrow V(x_{n+1}F - 1) \subseteq \mathbb{A}^{n+1}$. To show such ψ when restricted onto W suffices, we only have to show $\psi(W)$ is closed, which follows from W being closed in $\mathbb{A}^n - V(F)$, which follows from X being closed in \mathbb{A}^n .

Let $X \subseteq \mathbb{P}^n$, let $p \in \mathbb{A}_{(0)} \triangleq \{[\mathbf{x}] \in \mathbb{P}^n : x_0 \neq 0\}$, and let $\varphi : \mathbb{A}_{(0)} \rightarrow \mathbb{A}^n$ be the **standard quasi variety isomorphism**. Because X is closed, we know $\varphi(X \cap \mathbb{A}_{(0)}) \subseteq \mathbb{A}^n$ is closed. Clearly, $U \cap \mathbb{A}_{(0)}$ is open in $X \cap \mathbb{A}_{(0)}$. It then follows from the affine case that there exists some W' , containing $\varphi(p)$, contained by $\varphi(U \cap \mathbb{A}_{(0)})$, open in $\varphi(X \cap \mathbb{A}_{(0)})$, and quasi variety isomorphic to some affine variety. By construction, $W \triangleq \varphi^{-1}(W')$ suffices. ■

dense and ψ_V is continuous, we know $\psi_V^{-1}(W) \subseteq Y$ is nonempty and open. It then follows from dominance of φ that $\varphi_U^{-1}(\psi_V^{-1}(W))$ is nonempty.

Theorem 4.8.3. (Category of varieties and dominant rational map is "equivalent" to the finitely generated field extension) Let X, Y be two varieties. The map $\varphi \mapsto \varphi^*$ forms a bijection between

- (i) the set of dominant rational maps from X to Y .
- (ii) the set of k -algebra homomorphism from $K(Y)$ to $K(X)$.

Proof. Let $\theta : K(Y) \rightarrow K(X)$ be a k -algebra homomorphism. We are required to show the existence and uniqueness of dominant $\varphi : X \dashrightarrow Y$ that satisfies $\varphi^* = \theta$. Suppose for now Y is projective. By [Theorem 4.8.2](#), there exists some nonempty open $U \subseteq Y$ and quasi variety isomorphism $\phi : U \rightarrow Z \subseteq \mathbb{A}^n$ where Z is closed. Let $\beta : U \dashrightarrow Y, \phi : Z \dashrightarrow U$ be the obvious birational maps.

$$\begin{array}{ccc}
 X & \xrightarrow{\quad \quad \quad} & Y \\
 & \searrow & \uparrow \beta \\
 & & U \\
 & & \downarrow \phi \\
 & \searrow & Z
 \end{array}$$

Clearly, the unique existence of $\psi : X \dashrightarrow Z$ that satisfies $\psi^* = \theta \circ (\beta^{-1})^* \circ (\phi^{-1})^*$ implies the unique existence of $\alpha : X \dashrightarrow Y$ that satisfies $\alpha^* = \theta$. This allows us to suppose Y is affine.

Let $\{y_1, \dots, y_n\}$ generate $\Gamma(Y)$ as k -algebra. Because X is irreducible, we know the intersection of domains of $\theta(y_i)$ is nonempty open. Denoting that intersection by U , clearly θ maps $\Gamma(Y)$ into $\mathcal{O}(U)$. By [Theorem 4.5.2](#), there exists a unique quasi variety morphism $\varphi_U : U \rightarrow Y$ such that $\theta(F) = F \circ \varphi_U$ for all $F \in \Gamma(Y)$. Let $\varphi : X \dashrightarrow Y$ be the rational map induced by φ_U . It remains to show that

- (i) φ is dominant with $\varphi^* = \theta$.
- (ii) φ is the only dominant rational map from X to Y whose dual map is θ .

To see that φ is dominant, observe that if $\varphi_U(U) \subseteq V(F_1, \dots, F_m)$, then $\theta(F_i) = 0$, which by injectivity of the field homomorphism θ implies $F_i = 0$.

We now show $\varphi^* = \theta$. Let $f \in K(Y)$ and $x \in \varphi_U^{-1}(\text{Dom } f)$. Because by irreducibility, $\varphi_U^{-1}(\text{Dom } f)$ is nonempty open, to show $\theta(f) = \varphi^*(f)$, we only have to show $\theta(f)(x) = \varphi^*(f)(x)$, which is done by verifying the computation:

$$\varphi^*(f)(x) = \varphi^*(F/G)(x) = \frac{\varphi^*(F)(x)}{\varphi^*(G)(x)} = \frac{\theta(F)(x)}{\theta(G)(x)} = \theta(f)(x)$$

86

where $f = F/G$.³⁵ Note that $\varphi^*(f)$ is defined at x because $x \in \varphi_U^{-1}(\text{Dom } f)$, that $\varphi^*(F) = \theta(F)$ are defined at x by construction of U , and that $\theta(G)(x) = \varphi^*(G)(x) \neq 0$ by definition.

Lastly, let $\psi : X \dashrightarrow Y$ be another dominant rational map such that $\psi^* = \theta$. We are required to show $\psi = \varphi$. By irreducibility, there exists some open $V \subseteq U$ on which ψ is defined. By construction, $F \circ \psi_V = \theta(F)$ for all $F \in \Gamma(Y)$. **Theorem 4.5.2** states that such ψ_V is unique. On the other hands, φ_V also satisfies $F \circ \varphi_V = \theta(F)$. We have shown φ, ψ agree on V , which implies $\varphi = \psi$. ■

Equivalent Definition 4.8.4. (Birational Equivalence) Let X, Y be two varieties. The followings are equivalent:

- (i) X and Y are birationally equivalent.
- (ii) There exists $U \subseteq X$ and $V \subseteq Y$ such that U is open in X , V is open in Y , and U, V are quasi variety isomorphic.
- (iii) $K(X)$ and $K(Y)$ are isomorphic as k -algebras.

Proof. (i) \implies (ii): Consider birational map $\varphi : X \dashrightarrow Y$ with inverse $\psi : Y \dashrightarrow X$. Let $W \triangleq \text{Dom}(\varphi)$ and $O \triangleq \text{Dom}(\psi)$. The proof then follows from checking $U \triangleq \varphi_W^{-1}(\psi_O^{-1}(W))$ and $V \triangleq \psi_O^{-1}(\varphi_W^{-1}(O))$ suffices.

(ii) \implies (iii): This follows from $K(X) \cong K(U) \cong K(V) \cong K(Y)$ as k -algebras.

(iii) \implies (i): This follows from **Theorem 4.8.3**. ■

³⁵Such F, G are not only guaranteed to exist so that locally $f = F/G$, but also globally $f = F/G$. See **Theorem 4.5.1**.

4.9 Singularity

Let X be a quasi variety. We say X is **nonsingular at** $\mathbf{a} \in X$ if the local ring $\mathcal{O}_{\mathbf{a},X}$ is moreover regular, and we say X is **smooth** or **nonsingular** if X contains no singular point.

Equivalent Definition 4.9.1. (Jacobian criteria for singularities of affine varieties) Given algebraically closed field k , affine variety $X \subseteq \mathbb{A}_k^n$, $\mathbf{a} \in X$, and some set $\{F_1, \dots, F_t\} \subseteq k[x_1, \dots, x_n]$ of generators of $I(X)$, the followings are equivalent:

- (i) X is nonsingular at \mathbf{a} .
- (ii) The rank of the $t \times n$ **Jacobian matrix** $(\partial F_i / \partial x_j)|_{\mathbf{a}}$, equals to $n - \text{topdim}(X)$.

Note that basic linear algebra told us the rank of the Jacobian matrix $(\partial F_i / \partial x_j)$ is invariant under the choice of generators and t .

Proof. Define k -linear map $\theta : A \triangleq k[x_1, \dots, x_n] \rightarrow k^n$ by

$$\theta(G) \triangleq \left(\frac{\partial G}{\partial x_1} \Big|_{\mathbf{a}}, \dots, \frac{\partial G}{\partial x_n} \Big|_{\mathbf{a}} \right)$$

Let $\mathfrak{a} \triangleq \langle x_1 - a_1, \dots, x_n - a_n \rangle \subseteq A$ be the maximal ideal correspond to \mathbf{a} . Unrolling the definitions shows that:

- (i) θ is surjective because $\theta(x_i - a_i)$ forms a basis for k^n .
- (ii) $\mathfrak{a}^2 \subseteq \text{Ker } \theta \cap \mathfrak{a}$
- (iii) Fix $F \in \text{Ker } \theta \cap \mathfrak{a}^2$. Because $F \in \mathfrak{a}$, we may write $F = G_1(x_1 - a_1) + \dots + G_n(x_n - a_n)$. Because $\theta(F) = 0$, we know by computation that $G_i(a) = 0$ for all i , that is, $G_i \in \mathfrak{a}$ and $F \in \mathfrak{a}^2$. Together with (ii), we have shown $\mathfrak{a}^2 = \text{Ker } \theta \cap \mathfrak{a}$.

Therefore, θ induces a k -linear isomorphism $\theta' : \mathfrak{a} / \mathfrak{a}^2 \rightarrow k^n$. Again, unrolling the definitions shows that dimension of $\theta(I(X))$ equals to the rank r of the Jacobian matrix. Now, because we have the commutative diagram:

$$\begin{array}{ccc} \mathfrak{a} & \xrightarrow{\theta|_{\mathfrak{a}}} & k^n \\ \downarrow & \nearrow \theta' & \\ \mathfrak{a} / \mathfrak{a}^2 & & \end{array}$$

we see that $\theta' : \mathfrak{a}/\mathfrak{a}^2 \rightarrow k^n$ forms a k -vector space isomorphism between $\mathfrak{a}^2 + I(X)/\mathfrak{a}^2$ and $\theta(I(X))$, which implies $\mathfrak{a}^2 + I(X)/\mathfrak{a}^2$ have dimension r as a k -vectors space.

Let $\mathfrak{m} \subseteq \mathcal{O}_{\mathfrak{a}}$ be the maximal ideal. **Theorem 4.5.1** stated that $\mathcal{O}_{\mathfrak{a}} \cong (A/I(X))_{\mathfrak{a}}$. Because the set \mathfrak{m} of non-units in $\mathcal{O}_{\mathfrak{a}}$ are exactly rational functions whose nominator vanish at \mathfrak{a} , we know $\mathfrak{m} = (\mathfrak{a}/I(X))_{\mathfrak{a}}$, which implies $\mathfrak{m}^2 = (\mathfrak{a}^2 + I(X)/I(X))_{\mathfrak{a}}$, which moreover implies³⁶:

$$\mathfrak{m}/\mathfrak{m}^2 \cong (\mathfrak{a}/\mathfrak{a}^2 + I(X))_{\mathfrak{a}} \cong \mathfrak{a}/\mathfrak{a}^2 + I(X), \quad \text{as } k\text{-vector space}$$

Now, because $\dim_k(\mathfrak{a}/\mathfrak{a}^2) = n$, we know:

$$\dim_k(\mathfrak{m}/\mathfrak{m}^2) = \dim_k(\mathfrak{a}/\mathfrak{a}^2 + I(X)) = n - \dim_k(\mathfrak{a}^2 + I(X)/\mathfrak{a}^2) = n - r$$

³⁷ As desired, we now see:

$$\dim_k(\mathfrak{m}/\mathfrak{m}^2) = \text{Topdim}(X) \iff r = n - \text{Topdim}(X)$$

■

Theorem 4.9.2. (Rank of Jacobian matrix is invariant under choice of homogeneous coordinate) Let field k be algebraically closed, $F_1, \dots, F_t \in k[x_0, \dots, x_n]$ each be homogeneous with degree d_i , for each $\lambda \neq 0 \in k$ and $\mathbf{x} \neq \mathbf{0} \in \mathbb{A}^{n+1}$, the rank of the two $(n+1) \times t$ -matrices:

$$\begin{pmatrix} \frac{\partial F_1}{\partial x_0}(\mathbf{x}) & \cdots & \frac{\partial F_1}{\partial x_n}(\mathbf{x}) \\ \vdots & \ddots & \vdots \\ \frac{\partial F_t}{\partial x_0}(\mathbf{x}) & \cdots & \frac{\partial F_t}{\partial x_n}(\mathbf{x}) \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \frac{\partial F_1}{\partial x_0}(\lambda\mathbf{x}) & \cdots & \frac{\partial F_1}{\partial x_n}(\lambda\mathbf{x}) \\ \vdots & \ddots & \vdots \\ \frac{\partial F_t}{\partial x_0}(\lambda\mathbf{x}) & \cdots & \frac{\partial F_t}{\partial x_n}(\lambda\mathbf{x}) \end{pmatrix}$$

are the same.

Proof. Note that $\frac{\partial F_i}{\partial x_j} \in k[x_0, \dots, x_n]$ is either 0 or homogeneous with degree $d_i - 1$. Therefore,

$$\begin{pmatrix} \frac{\partial F_i}{\partial x_0}(\lambda\mathbf{x}) & \cdots & \frac{\partial F_i}{\partial x_n}(\lambda\mathbf{x}) \end{pmatrix} = \lambda^{d_i-1} \begin{pmatrix} \frac{\partial F_i}{\partial x_0}(\mathbf{x}) & \cdots & \frac{\partial F_i}{\partial x_n}(\mathbf{x}) \end{pmatrix}$$

This renders the desired result an easy consequences of basic linear algebra. ■

³⁶Note that Hartshorne never really proved that his way of defining local ring indeed makes residue field isomorphic to ground field. Such hold true because of the assumption that the ground field k is algebraically closed. Here we give a proof: Because the image of usual embedding $k \hookrightarrow \mathcal{O}_{\mathfrak{a}}$ clearly has element lying outside of \mathfrak{m} , we know the field homomorphism $k \rightarrow \mathcal{O}_{\mathfrak{a}}/\mathfrak{m}$ obtained by composing $k \hookrightarrow \mathcal{O}_{\mathfrak{a}}$ and $\mathcal{O}_{\mathfrak{a}} \rightarrow \mathcal{O}_{\mathfrak{a}}/\mathfrak{m}$ is nonzero. In other words, the residue field $\mathcal{O}_{\mathfrak{a}}/\mathfrak{m}$ is an extension of k . Now, because $\mathcal{O}_{\mathfrak{a}}/\mathfrak{m}$ is clearly a finitely generated k -algebra, we may conclude using Zariski's Lemma that that $\mathcal{O}_{\mathfrak{a}}/\mathfrak{m}$ is a finite extension of k , which by algebraically closedness of k implies $k \cong \mathcal{O}_{\mathfrak{a}}/\mathfrak{m}$ as field, as desired.

³⁷You may think about this later.

Equivalent Definition 4.9.3. (Jacobian criteria for singularities of projective varieties) Let field k be algebraically closed, $X \subseteq \mathbb{P}^n$ a projective variety, $[\mathbf{y}] \in X$, and homogeneous $\{F_1, \dots, F_t\} \subseteq k[x_0, \dots, x_n]$ generate $I(X)$. The followings are equivalent:³⁸

- (i) X is nonsingular at $[\mathbf{y}]$.
- (ii) The rank of the $t \times (n+1)$ Jacobian matrix $(\partial F_i / \partial x_j)|_{[\mathbf{y}]}$, equals to $n - \text{topdim}(X)$.

Proof. Let $0 \leq l \leq n$. Recall that the map:

$$X \cap \{[\mathbf{x}] \in \mathbb{P}^n : x_l \neq 0\} \rightarrow \mathbb{A}^n; \quad [\mathbf{x}] \mapsto \left(\frac{x_0}{x_l}, \dots, \frac{x_{l-1}}{x_l}, \frac{x_{l+1}}{x_l}, \dots, \frac{x_n}{x_l} \right)$$

forms a quasi variety isomorphism from the projective quasi variety $X \cap \{[\mathbf{x}] \in \mathbb{P}^n : x_l \neq 0\}$ to the affine variety $V(f_1, \dots, f_t) \subseteq \mathbb{A}^n$, where $f_i \in k[x_0, \dots, \hat{x}_l, \dots, x_n]$ are the dehomogenizations of $F_i \in k[x_0, \dots, x_n]$.

Because both quasi variety isomorphism and talking closure preserves both topological dimension and local rings, to finish the proof, we only have to establish the existence of an $l \in \{0, \dots, n\}$ that makes:

- (i) $y_l \neq 0$.
- (ii) the rank of the $t \times n$ Jacobian matrix $(\partial f_i / \partial x_j)|_{(\frac{y_0}{y_l}, \dots, \frac{y_{l-1}}{y_l}, \frac{y_{l+1}}{y_l}, \dots, \frac{y_n}{y_l})}$ equals to that of the $t \times (n+1)$ Jacobian matrix $(\partial F_i / \partial x_j)|_{\mathbf{y}}$.

and then the rest will follow from **Jacobian criteria for singularities of affine varieties**.

We now establish such l . Using **Euler's Lemma**, one may compute:³⁹

$$\begin{bmatrix} \frac{\partial F_1}{\partial x_0}(\mathbf{y}) & \cdots & \frac{\partial F_1}{\partial x_n}(\mathbf{y}) \\ \vdots & \ddots & \vdots \\ \frac{\partial F_t}{\partial x_0}(\mathbf{y}) & \cdots & \frac{\partial F_t}{\partial x_n}(\mathbf{y}) \end{bmatrix} \begin{bmatrix} y_0 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} F_1(\mathbf{y}) \cdot \deg F_1 \\ \vdots \\ F_t(\mathbf{y}) \cdot \deg F_t \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \quad (4.10)$$

where the second inequality hold true by construction of \mathbf{y} and F_i . For each $j \in \{0, \dots, n\}$, let v_j be the j -th column of the $t \times (n+1)$ matrix $(\partial F_i / \partial x_j)|_{\mathbf{y}}$. In other words:

$$v_j = \begin{bmatrix} \frac{\partial F_1}{\partial x_j}(\mathbf{y}) \\ \vdots \\ \frac{\partial F_t}{\partial x_j}(\mathbf{y}) \end{bmatrix}, \quad \text{for all } 0 \leq j \leq n$$

³⁸Note that the rank of the Jacobian matrix is well-defined up to choices of generators and homogeneous coordinates. We have discussed them in **Jacobian criteria for singularities of affine varieties** and **theorem 4.9.2**.

³⁹**Euler's Lemma** stated that if $F \in k[x_0, \dots, x_n]$ is homogeneous, then $\sum x_i (\frac{\partial F}{\partial x_i}) = F \cdot \deg(F)$.

Because $(y_0, \dots, y_n) \in k^{n+1}$ is nonzero, [equation 4.10](#) implies that, after rearranging the indexes of coordinates, we may let:

- (i) $m \leq n$.
- (ii) $\{v_1, \dots, v_m\}$ be a basis for the columns space: $\text{span}(v_0, \dots, v_n)$.
- (iii) $y_0 \neq 0$.^{[40](#)}

Finally, we claim $l \triangleq 0$ suffice, which follows from noting:

$$\left(\begin{array}{ccc} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_t}{\partial x_1} & \cdots & \frac{\partial f_t}{\partial x_n} \end{array} \right) \bigg|_{\left(\frac{y_1}{y_0}, \dots, \frac{y_n}{y_0} \right)} = \begin{bmatrix} y_0^{\deg(F_1)-1} \frac{\partial F_1}{\partial x_1}(\mathbf{y}) & \cdots & y_0^{\deg(F_1)-1} \frac{\partial F_1}{\partial x_n}(\mathbf{y}) \\ \vdots & \ddots & \vdots \\ y_0^{\deg(F_t)-1} \frac{\partial F_t}{\partial x_1}(\mathbf{y}) & \cdots & y_0^{\deg(F_t)-1} \frac{\partial F_t}{\partial x_n}(\mathbf{y}) \end{bmatrix} \quad (4.11)$$

■

⁴⁰If $y_j = 0$ for all $j \in \{0, \dots, m+1, \dots, n\}$, then the linearly independence of $\{v_1, \dots, v_m\}$ together with [equation 4.10](#) implies $\mathbf{y} = 0$, which is impossible.

4.10 Intersection

Theorem 4.10.1. (Affine Dimension Theorem) Let k be closed, Y, Z be two varieties of dimensions r, s in \mathbb{A}^n . Every irreducible component of $Y \cap Z$ has dimension $\geq r + s - n$.

Proof. We first prove the case when Z is a hypersurface, says $Z = V(F)$ for some irreducible $F \in k[\mathbf{x}]$. We are required to prove irreducible components of $Y \cap Z$ have dimension $\geq r - 1$. Because $A(Y)$ is Noetherian, by **primary decomposition theorem**, we know $\langle [F] \rangle \subseteq A(Y)$ has finite number of minimal prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_m \subseteq A(Y)$. By **correspondence theorem**, preimage of \mathfrak{p}_i under quotient map $k[\mathbf{x}] \twoheadrightarrow A(Y)$ are exactly minimal prime ideals over $I(Y) + \langle F \rangle$. Moreover, because:

$$\sqrt{I(Y) + \langle F \rangle} = I(V(I(Y) + \langle F \rangle)) = I(Y \cap Z)$$

We see preimages of \mathfrak{p}_i are furthermore exactly the minimal prime ideals over $I(Y \cap Z)$. Therefore, the images of ideals of irreducible components of $Y \cap Z$ under quotient map $k[\mathbf{x}] \twoheadrightarrow A(Y)$ are exactly \mathfrak{p}_i . Let C be an irreducible component of $Y \cap Z$ correspond to \mathfrak{p}_i . It now follows from third isomorphism theorem of ring that

$$A(C) = \frac{k[\mathbf{x}]}{I(C)} = \frac{\frac{k[\mathbf{x}]}{I(Y)}}{\frac{I(C)}{I(Y)}} = \frac{A(Y)}{\mathfrak{p}_i}$$

Because \mathfrak{p}_i is of height one by **Krull's principal ideal theorem**, by **Theorem 3.4.3**, we know $\text{Krudim}(A(C)) = \text{Krudim}(A(Y)) - \text{height } \mathfrak{p}_i = r - 1$. We have proved the special case when Z is a hypersurface. We now prove the general case.

Denote the diagonal in \mathbb{A}^{2n} by:

$$\Delta \triangleq \{(\mathbf{a}, \mathbf{a}) \in \mathbb{A}^{2n} : \mathbf{a} \in \mathbb{A}^n\}$$

Clearly, $\varphi : \mathbb{A}^n \rightarrow \Delta$ defined by $\mathbf{a} \mapsto (\mathbf{a}, \mathbf{a})$ forms a homeomorphism between $Y \cap Z \subseteq \mathbb{A}^n$ and $(Y \times Z) \cap \Delta \subseteq \mathbb{A}^{2n}$. Because of such, we only have to prove the irreducible components of $(Y \times Z) \cap \Delta$ has dimension $\geq r + s - n$. We now prove such using the special case above.

Note that

(i) $\text{Topdim}(Y \times Z) = r + s$.

(ii) $\Delta = V(x_1 - y_1) \cap \dots \cap V(x_n - y_n)$ is the intersection of n numbers of hyper surfaces.

By applying the special case n times, we see the irreducible components of $(Y \times Z) \cap \Delta$ has dimension $r + s - 1 \cdot n$. ■

41

⁴¹I don't understand:

Theorem 4.10.2. (Projective Dimension Theorem) Let k be closed, Y, Z be two varieties of dimension r, s in \mathbb{P}^n . Every irreducible component of $Y \cap Z$ has dimension $\geq r + s - n$. Moreover, if $r + s - n \geq 0$, then $Y \cap Z$ is nonempty.

Proof. ■

A single variable rational coefficient polynomial P is said to be **numerical** if $P(z)$ is an integer for all $z \in \mathbb{Z}$.

Equivalent Definition 4.10.3. (Numerical polynomial) For all $z \in \mathbb{C}$ and $r \in \mathbb{Z}_0^+$, we define

$$\binom{z}{r} \triangleq \frac{z(z-1)\cdots(z-r+1)}{r!}$$

Given $P \in \mathbb{Q}[z]$, the followings are equivalent:

- (i) $P(z) \in \mathbb{Z}$ for all $z \gg 0 \in \mathbb{Z}$.
- (ii) There exists $c_0, \dots, c_r \in \mathbb{Z}$ such that

$$P(z) = c_0 \binom{z}{r} + c_1 \binom{z}{r-1} + \cdots + c_r$$

- (iii) P is numerical.

Proof. (i) \implies (ii): The proof is done by induction on degree of P . If P is a constant then there is nothing to prove. Suppose $\deg(P) = r$ and the assertion hold true when $\deg(P) < r$. Clearly, there exists some $c_0, \dots, c_r \in \mathbb{Q}$ such that

$$P(z) = c_0 \binom{z}{r} + c_1 \binom{z}{r-1} + \cdots + c_r$$

-
- (i) Do we need primary decomposition theorem to deduce about the number or existence of minimal prime ideals in $A(Y)$ over $\langle [F] \rangle$? Doesn't the finite existence of irreducible components of $Y \cap Z$ with correspondence theorem already implies this?
 - (ii) Why $I(Y) + \langle F \rangle = I(Y \cap Z)$?
 - (iii) How to write third isomorphism theorem better? Remember to write it formally in chapter 1.
 - (iv) Why is φ a homeomorphism?
 - (v) Why is $\text{Topdim}(Y \times Z) = r + s$?
 - (vi) Why can we apply the special case n times?

Define $\Delta P \in \mathbb{Q}[z]$ by $\Delta P(z) \triangleq P(z+1) - P(z)$. Computing

$$\binom{z+1}{r} - \binom{z}{r} = \binom{z}{r-1}$$

We see

$$\Delta P(z) = c_0 \binom{z}{r-1} + c_1 \binom{z}{r-2} + \cdots + c_{r-1}$$

Clearly, $\Delta P(z) \in \mathbb{Z}$ for all $z \gg 0 \in \mathbb{Z}$ by construction, and there exists only one $(b_0, \dots, b_{r-1}) \in \mathbb{Q}^r$ such that

$$\Delta P(z) = b_0 \binom{z}{r-1} + b_1 \binom{z}{r-2} + \cdots + b_{r-1}$$

Therefore, we may apply inductive hypothesis to conclude $c_0, \dots, c_{r-1} \in \mathbb{Z}$. It then follows from $P(z) \in \mathbb{Z}$ for all $z \gg 0 \in \mathbb{Z}$ that $c_r \in \mathbb{Z}$, as desired.

(ii) \implies (iii): This follows from $\binom{z}{r} \in \mathbb{Z}$ for all $z \in \mathbb{Z}$, which can be checked by induction.

(iii) \implies (i) is clear. ■

Corollary 4.10.4. (Properties of numerical polynomials) Given two numerical $P_1, P_2 \in \mathbb{Q}[z]$, if $P_1(z) = P_2(z)$ for all $z \gg 0 \in \mathbb{Z}$, then $P_1 = P_2$.

Proof. Clearly, $P_1 - P_2 \in \mathbb{Q}[z]$ is numerical and maps large integers to 0. Therefore, by [definition of numerical polynomial](#), we have:

$$(P_1 - P_2)(z) = c_0 \binom{z}{r} + c_1 \binom{z}{r-1} + \cdots + c_r$$

Letting $z \rightarrow \infty$, we see c_0 must be 0. Letting $z \rightarrow \infty$ again, we see c_1 also must be 0. Repeating the same process, we see $P_1 - P_2 = 0 \in \mathbb{Q}[z]$. ■

Theorem 4.10.5. (Filtration to compute Hilbert polynomial) Let S be a \mathbb{N} -graded Noetherian ring and M a graded S -module of finite type. There exists some ascending filtration $0 = M^0 \subseteq M^1 \subseteq \cdots \subseteq M^r = M$ consisting of graded submodules together with a tuple $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ of homogeneous prime ideal in S and a tuple of integer $\{l_1, \dots, l_r\}$ such that

$$M^i / M^{i-1} \cong (S / \mathfrak{p}_i)(l_i), \quad \text{as graded } S\text{-module for all } i.$$

Even though such ascending filtration consisting of graded submodules aren't unique, every such filtration satisfies:

(i) If $\mathfrak{p} \subseteq S$ is homogeneous prime, then

$$\mathfrak{p} \supseteq \text{Ann } M \iff \mathfrak{p} \supseteq \mathfrak{p}_i \text{ for some } i$$

Moreover, the set of minimal elements of the set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ is exactly the set of minimal prime ideals over $\text{Ann}(M)$.⁴²

(ii) For each minimal prime \mathfrak{p} over $\text{Ann}(M)$, the number of times which \mathfrak{p} occur in the set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ equals to $\mu_{\mathfrak{p}}(M)$, the length of the $S_{\mathfrak{p}}$ -module $M_{\mathfrak{p}}$.

Proof. We first prove the existence of such filtration. Consider the set of graded submodule of M which admit such a filtration. Clearly, the zero module is in this set, so this set is nonempty. Because M is Noetherian, we know this set has a maximal element M' .⁴³

Consider $M'' \triangleq M/M'$. If $M'' = 0$, we are done. If not, consider the set of ideals $\{\text{Ann}(m) \subseteq M'' : m \in M'' \text{ is homogeneous and nonzero}\}$ ■

Let M be a graded module over polynomial ring $k[x_0, \dots, x_n]$. Its **Hilbert function** $\varphi_M : \mathbb{Z} \rightarrow \mathbb{N} \cup \{0\}$ is defined by

$$\varphi_M(l) \triangleq \dim_k(M_l)$$

Theorem 4.10.6. (Hilbert-Serre Theorem) Let k be an algebraically closed field and M a graded module of finite type over $k[x_0, \dots, x_n]$. There exists unique $P_M \in \mathbb{Q}[z]$ such that

$$\varphi_M(l) = P_M(l), \quad \text{for all } l \gg 0$$

Moreover, the degree of this P_M is the topological dimension of $Z(\text{Ann } M) \subseteq \mathbb{P}^n$.

Proof. ■

Given closed $Y \subseteq \mathbb{P}^n$, its **Hilbert polynomial** is $P_{S(Y)}$ from **Hilbert-Serre Theorem**. The **degree** of Y is the $\text{Topdim}(Y)!$ times the leading coefficient of $P_{S(Y)}$.

Theorem 4.10.7. (Degrees of simple objects are expected) Let k be closed. Denote S the coordinate ring of \mathbb{P}^n and denote φ the Hilbert function. If $F \in S$ is an irreducible homogeneous polynomial of degree d , H is the zero set of F , and $X \subseteq \mathbb{P}^n$ is singleton, then:

(i) $\varphi_S(l) = \binom{l+n}{n}$ for all $l \geq 0$. Therefore, $\deg(\mathbb{P}^n) = 1$.

⁴²This statement implies the statement that minimal prime ideals over $\text{Ann}(M)$ is always homogeneous, which I believe can be proved by showing $\text{Ann}(M)$ is always homogeneous and minimal prime over homogeneous ideals are always homogeneous.

⁴³**Theorem 1.8.5** implies M is Noetherian. **equivalent definition of Noetherian module** implies existence of M'

(ii) $\varphi_{S(H)}(l) = \binom{l+n}{n} - \binom{l-d+n}{n}$ for all $l \geq d$. Therefore, $\deg(H) = d$.

(iii) $\varphi_{S(X)}(l) = 1$ for all $l \geq 0$. Therefore, $\deg(X) = 1$.

Proof. (i): The proof follows from noting that for all $l \geq 0$, S_l has basis:

$$\left\{ x_0^{d_0} \cdots x_n^{d_n} \in S : d_0 + \cdots + d_n = l \right\}$$

(ii): Fix $l \in \mathbb{Z}$. Check that $G \mapsto GF$ forms a graded S -module homomorphism $S(-d) \rightarrow S$ that give us a short exact sequence of graded S -modules:

$$0 \longrightarrow S(-d) \xrightarrow{F} S \twoheadrightarrow S/\langle F \rangle \longrightarrow 0$$

Clearly, its restriction is a short exact sequence of k -vector spaces: ⁴⁴⁴⁵

$$0 \longrightarrow S(-d)_l \longrightarrow S_l \longrightarrow S(H)_l \longrightarrow 0$$

It then follows from **dimension of vector space is additive** and (i) that:

$$\varphi_{S(H)}(l) = \varphi_S(l) - \varphi_S(l-d) = \binom{l+n}{n} - \binom{l-d+n}{n}, \quad \text{for all } l \geq d.$$

(iii): Fix $l \geq 0$. Check that:⁴⁶

$$S(X)_l \cong S_l / I(X) \cap S_l, \quad \text{as } k\text{-vector space.}$$

We are then required to show $\dim_k(I(X) \cap S_l) = \binom{l+n}{n} - 1$. Under a projective change of coordinate⁴⁷, WLOG, we may let $X = \{[1 : 0 : \cdots : 0]\}$. The proof then follows from checking $I(X) \cap S_l$ has basis:

$$\left\{ x_0^{d_0} \cdots x_n^{d_n} \in S : d_0 + \cdots + d_n = l \text{ and } d_0 \neq l \right\}$$

■

Let S be a \mathbb{N} -graded Noetherian ring, M a graded S -module, and $\mathfrak{p} \subseteq S$ be a minimal prime ideal over $\text{Ann}(M)$. The **multiplicity** of M at \mathfrak{p} , denoted by $\mu_{\mathfrak{p}}(M)$ is the length of $M_{\mathfrak{p}}$ over $S_{\mathfrak{p}}$. Let $Y \subseteq \mathbb{P}^n$ be a projective variety and $H \subseteq \mathbb{P}^n$ a hypersurface not containing Y . Clearly,

$$\text{Ann}(S/I(Y) + I(H)) = I(Y) + I(H)$$

⁴⁴I want to check this again later.

⁴⁵A S -module isomorphism is a k -vector space isomorphism. Category of S -module is a subcategory of k -vector space. Record this in early chapter.

⁴⁶I haven't checked it yet, and I think there is a good generalization of it.

⁴⁷I don't know how to perform this yet.

Let C_1, \dots, C_s be the irreducible components of $Y \cap H$, so $\{I(C_1), \dots, I(C_s)\}$ is exactly the set of minimal prime ideals over:⁴⁸⁴⁹

$$I(Y \cap H) = I(Z(I(Y) + I(H))) = \sqrt{I(Y) + I(H)} \quad (4.12)$$

This implies that $\{I(C_1), \dots, I(C_s)\}$ is exactly the set of minimal prime ideals over $I(Y) + I(H) = \text{Ann}(S/I(Y) + I(H))$. Because of such, we may now well define the **intersection multiplicity (number) of Y and H along C_j** to be

$$i(Y, H; C_j) \triangleq \mu_{I(C_j)}(S/I(Y) + I(H))$$

Theorem 4.10.8. (Bezout Theorem for a variety and a hypersurface in \mathbb{P}^n) Let Y be a variety of dimension ≥ 1 in \mathbb{P}^n , and let H be a hypersurface not containing Y . Let C_1, \dots, C_s be the irreducible components of $Y \cap H$. We have

$$\sum_{j=1}^s i(Y, H; C_j) \cdot \deg C_j = (\deg Y)(\deg H)$$

Proof. Let H be defined by irreducible homogeneous F of degree d . We have an exact sequence of graded S -modules:

$$0 \longrightarrow (S/I(Y))(-d) \xrightarrow{F} S/I(Y) \longrightarrow S/(I(Y) + I(H)) \longrightarrow 0$$

Clearly, its restriction is a short exact sequence of k -vector spaces:

$$0 \longrightarrow (S(Y))(-d)_l \longrightarrow S(Y)_l \longrightarrow (S/(I(Y) + I(H)))_l \longrightarrow 0$$

Denoting $M \triangleq S/(I(Y) + I(H))$, because **dimension of vector space is additive**, this give us:

$$P_M(z) = P_{S(Y)}(z) - P_{S(Y)}(z - d), \quad \text{for all } z \gg 0 \quad (4.13)$$

Let r and e respectively be the dimension and degree of Y . It is clear that $\text{Ann}(S(Y)) = I(Y)$, which by closedness of Y implies $Z(\text{Ann}(S(Y))) = Y$. It now follows from **Hilbert-Serre Theorem** that $P_{S(Y)}(z)$ has degree r . This implies the leading term of $P_{S(Y)}(z)$ is $\frac{\deg Y}{r!} z^r$. This with **Equation 4.13** implies:

$$\text{The leading term of } P_M(z) \text{ is } \frac{(\deg Y)(\deg H)}{(r-1)!} z^{r-1}. \quad (4.14)$$

Let the ascending filtration $0 = M^0 \subseteq M^1 \subseteq \dots \subseteq M^q = M$ consisting of graded S -submodules and the tuples $\{\mathfrak{p}_1, \dots, \mathfrak{p}_q\}, \{l_1, \dots, l_q\}$ be from **Theorem 4.10.5**. In other words, we have:

⁴⁸The first equality follows from $Z(I(Y) + I(H)) = Y \cap H$, the second is just Nullstellensatz.

⁴⁹Write the minimal prime share with radical in Chapter 1.1

(I) For each i

$$M^i / M^{i-1} \cong (S / \mathfrak{p}_i)(l_i), \quad \text{as graded } S\text{-module} \quad (4.15)$$

(II) The set of minimal elements of the set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_q\}$ is exactly the set of minimal prime ideals over $\text{Ann}(M)$.

(III) For each minimal prime \mathfrak{p} over $\text{Ann}(M)$, the number of times which \mathfrak{p} occur in the set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_q\}$ equals to $\mu_{\mathfrak{p}}(M)$.

Because for each $1 \leq i \leq q$ we have short exact sequence of graded S -modules:

$$0 \longrightarrow M^{i-1} \longrightarrow M^i \longrightarrow M^i / M^{i-1} \longrightarrow 0$$

We have $\varphi_{M^i} = \varphi_{M^{i-1}} + \varphi_{M^i / M^{i-1}}$, which by [Corollary 4.10.4](#) give us $P_{M^i} = P_{M^{i-1}} + P_{M^i / M^{i-1}}$. It now follows from induction and [Equation 4.15](#) that $P_M = \sum_{i=1}^q P_{(S/\mathfrak{p}_i)(l_i)}$. Because shifting doesn't effect leading coefficients of Hilbert polynomial⁵⁰ and because of [Equation 4.14](#), it only remains to prove:

$$\text{The leading coefficient of polynomial } \sum_{i=1}^q P_{S/\mathfrak{p}_i} \text{ equals to } \frac{\sum_{j=1}^s i(Y, H; C_j) \cdot \deg C_j}{(r-1)!}$$

Denote $r_i \triangleq \text{Topdim}(Z(\mathfrak{p}_i)) = \text{Krudim}(S/\mathfrak{p}_i)$, and denote $f_i \triangleq \deg(Z(\mathfrak{p}_i))$. Recall that

(i) Because $\{I(C_1), \dots, I(C_s)\}$ is exactly the set of minimal prime ideals over $I(Y) + I(H) = \text{Ann}(M)$ as shown in the paragraph before this theorem, by construction, $\{I(C_1), \dots, I(C_s)\}$ is exactly the set of minimal elements of the set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_q\}$.

(ii) By [projective dimension theorem](#), $\text{Topdim}(C_j) = r - 1$.

Therefore, by [fake dimension theorem](#), $\mathfrak{p}_i \in \{I(C_1), \dots, I(C_s)\} \iff r_i = r - 1$. By [Hilbert-Serre Theorem](#), P_{S/\mathfrak{p}_i} have degree r_i and therefore have leading term $\frac{f_i}{r_i!} z^{r_i}$. We now see conclude by (III) that indeed, the leading coefficient of $\sum_{i=1}^q P_{S/\mathfrak{p}_i}$ equals to

$$\frac{\sum_{r_i=r-1} f_i}{(r-1)!} = \frac{\sum_{\mathfrak{p}_i \in \{I(C_1), \dots, I(C_s)\}} f_i}{(r-1)!} = \frac{\sum_{j=1}^q \mu_{I(C_j)}(M) \cdot \deg(C_j)}{(r-1)!}$$

■

Corollary 4.10.9. (Bezout's Theorem for \mathbb{P}^2) Let k be algebraically closed and $H_1 \triangleq Z(F_1), H_2 \triangleq Z(F_2)$ be two hypersurfaces in \mathbb{P}^2 . If $H_1 \cap H_2$ is finite, says, $H_1 \cap H_2 = \{P_1, \dots, P_s\}$, then:

$$\sum i(H_1, H_2; P_j) = (\deg F_1)(\deg F_2)$$

Proof. This follows from [Bezout theorem for a variety and a hypersurface in \$\mathbb{P}^n\$](#) and the fact $\deg(P_i) = 1$ and $\deg(H_j) = \deg(F_j)$. ■

⁵⁰This can be easily check by computing $G(z) \triangleq F(l+z)$.

Chapter 5

Schemes

5.1 Direct limit

We say that a pair (X, \leq) forms a **preordered set** if the relation \leq is reflexive and transitive. Given a preordered set (X, \leq) , an element $x \in X$ is called an **upper bound** of a subset $Y \subseteq X$ if $y \leq x$ for all $y \in Y$. If every finite subset of X has an upper bound, then (X, \leq) is called a **directed set**.

Let (I, \leq) be a directed set, \mathfrak{C} a category, and $\{A_i \in \mathfrak{C} : i \in I\}$ a family of objects in \mathfrak{C} . If for each pair $i \leq j$, there exists a morphism $f_{ij} : A_i \rightarrow A_j$, satisfying:

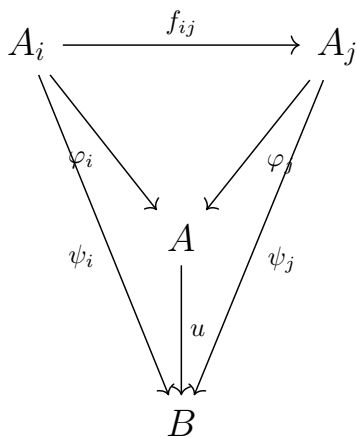
- (i) For all $i \in I$, f_{ii} is the identity morphism.
- (ii) For all $i \leq j \leq k$, we have $f_{ik} = f_{jk} \circ f_{ij}$.

then we say (A_i, f_{ij}) forms a **direct system** over I . Given a direct system (A_i, f_{ij}) , an object $B \in \mathfrak{C}$, together with morphisms $\varphi_i : A_i \rightarrow B$ for each $i \in I$, is called a **target** if for all $i \leq j$, the compatibility condition

$$\varphi_i = \varphi_j \circ f_{ji}$$

holds. The **direct limit** of the system, denoted $A \triangleq \varinjlim A_i$, is a target (A, φ_i) that satisfies the following **universal property**: For any target (\bar{B}, ψ_i) , there exists a unique morphism

$u : A \rightarrow B$ that makes the diagram:



commute for each $i \leq j$.

As one might expect, direct limits are indeed unique up to a unique isomorphism. In the remainder of this note, we refer to a category as a **good category** if it is the category of groups, rings, modules over a fixed ring, or algebras over a fixed ring. In such good categories, the existence of direct limits can be established by explicitly constructing:

$$A \triangleq \left(\bigsqcup A_i \right) / \sim, \quad \text{where } x_i \sim x_j \iff f_{ki}(x_i) = f_{kj}(x_j) \text{ for some } k \geq i, j.$$

5.2 Sheaves

Let X be a topological space and \mathfrak{C} a category. A **presheaf** \mathcal{F} of \mathfrak{C} -objects on X consists of the following data:

- (i) For each open subset $U \subseteq X$, an object $\mathcal{F}(U) \in \mathfrak{C}$. We call elements of $\mathcal{F}(U)$ **sections of \mathcal{F} over U** .
- (ii) For each inclusion of open sets $V \subseteq U$, a morphism (called the **restriction map**) $\text{Res}_V^U : \mathcal{F}(U) \rightarrow \mathcal{F}(V)$ in \mathfrak{C} . For obvious reason, we write $\text{Res}_V^U(s) \triangleq s|_V$.

subject to the following conditions:

- (a) $\mathcal{F}(\emptyset)$ is a final object of \mathfrak{C} .
- (b) **(Identity Law)** For every open set $U \subseteq X$, the restriction map Res_U^U is the identity morphism on $\mathcal{F}(U)$.
- (c) **(Composition Law)** For all open sets $W \subseteq V \subseteq U$, the composition law holds:

$$\text{Res}_W^U = \text{Res}_W^V \circ \text{Res}_V^U$$

For example, if we say that \mathcal{F} is a **presheaf of sets** on X , we mean that for each open subset $U \subseteq X$, $\mathcal{F}(U)$ is a set, each restriction map $\text{Res}_V^U : \mathcal{F}(U) \rightarrow \mathcal{F}(V)$ is a function between sets, the identity and composition laws hold, and $\mathcal{F}(\emptyset) = \{\emptyset\}$. Similarly, if \mathcal{F} is a **presheaf of rings** on X , then each $\mathcal{F}(U)$ is a ring, each restriction map Res_V^U is a ring homomorphism, and $\mathcal{F}(\emptyset) = \mathbb{Z}_1$. Likewise, a **presheaf of groups** consists of group-valued assignments: each $\mathcal{F}(U)$ is a group, the restriction maps are group homomorphisms, and $\mathcal{F}(\emptyset) = \mathbb{Z}_1$.

Fix \mathfrak{C} and X . One may check that a \mathfrak{C} -valued presheaf on X forms a category if we define a **morphism** φ from \mathcal{F} to \mathcal{G} to be an assignment of each open $U \subseteq X$ a \mathfrak{C} -morphism $\varphi(U) : \mathcal{F}(U) \rightarrow \mathcal{G}(U)$ such that for every inclusion $V \subseteq U$, the diagram:

$$\begin{array}{ccc} \mathcal{F}(U) & \xrightarrow{\varphi_U} & \mathcal{G}(U) \\ \text{Res}_{UV}^{\mathcal{F}} \downarrow & & \downarrow \text{Res}_{UV}^{\mathcal{G}} \\ \mathcal{F}(V) & \xrightarrow{\varphi_V} & \mathcal{G}(V) \end{array} \quad (5.1)$$

commutes. We denote the category of \mathfrak{C} -valued presheaves on X by $\mathbf{PSh}_{\mathfrak{C}}(X)$. Let $\mathcal{F} \in \mathbf{PSh}_{\mathfrak{C}}(X)$. A **subpresheaf** \mathcal{G} of \mathcal{F} consists of the assignment to each open set $U \subseteq X$ a subobject $\mathcal{G}(U) \subseteq \mathcal{F}(U)$ in \mathfrak{C} , such that for every inclusion of open sets $V \subseteq U$, the restriction map $\text{Res}_{UV}^{\mathcal{F}} : \mathcal{F}(U) \rightarrow \mathcal{F}(V)$ satisfies:

$$\text{Res}_{U,V}^{\mathcal{F}}(\mathcal{G}(U)) \subseteq \mathcal{G}(V) \quad (5.2)$$

Condition 5.2 ensures that we can define the restriction maps of \mathcal{G} by restricting those of \mathcal{F} , thereby making \mathcal{G} a well-defined presheaf. Let \mathfrak{C} be a good category and $\varphi \in \text{Hom}_{\mathbf{Psh}_{\mathfrak{C}}(X)}(\mathcal{F}, \mathcal{G})$. The **presheaf image** of φ assigns $U \mapsto \text{Im}(\varphi(U)) \subseteq \mathcal{G}(U)$ and has the restriction map of \mathcal{G} . The **presheaf kernel** of φ assigns $U \mapsto \text{Ker}(\varphi(U)) \subseteq \mathcal{F}(U)$ and has the restriction map of \mathcal{F} . The **presheaf cokernel** of φ assigns $U \mapsto \text{Coker}(\varphi(U))$ and has the restriction map $\text{Coker}(\varphi(U)) \rightarrow \text{Coker}(\varphi(V)); [t] \mapsto [\text{Res}_{UV}^{\mathcal{G}}(t)]$. Note that the image, kernel, and cokernel of φ are well-defined because we require **diagram 5.1** to commute, and the image presheaf of φ is indeed a subpresheaf of \mathcal{G} , while the kernel presheaf of φ is a subpresheaf of \mathcal{F} .

Just like other categories, a presheaf isomorphism is again a morphism that admits a two-sided inverse.

Let $P \in X$, \mathfrak{C} a good category, and \mathcal{F} a \mathfrak{C} -valued presheaf on X . Its **stalk** \mathcal{F}_P at P is the direct limit of the directed system $(\mathcal{F}(U), \text{Res})$ over all open neighborhoods $U \ni P$. Therefore, an element of \mathcal{F}_P is an equivalence class represented by a pair (U, s) with $s \in \mathcal{F}(U)$, and two such pairs $(U, s), (V, t)$ represent the same element if there exists a neighborhood $W \subseteq U \cap V$ of P such that $s|_W = t|_W$. Let $\varphi \in \text{Hom}_{\mathbf{Psh}_{\mathfrak{C}}(X)}(\mathcal{F}, \mathcal{G})$. It induces a \mathfrak{C} -homomorphism $\varphi_u \in \text{Hom}(\mathcal{F}_P, \mathcal{G}_P)$ via universal property of direct limit:

$$\begin{array}{ccccc}
 & \mathcal{F}(U) & & \mathcal{F}(V) & \\
 \varphi(U) \swarrow & & \searrow & & \swarrow \varphi(V) \\
 \mathcal{G}(U) & & \mathcal{F}_P & & \mathcal{G}(V) \\
 & \searrow & \vdots \varphi_P & \swarrow & \\
 & & \mathcal{G}_P & &
 \end{array}$$

In particular, recall that when X is a quasi-variety, we denote by $\mathcal{O}(U)$ the ring of regular functions on an open set $U \subseteq X$, and by \mathcal{O}_p the local ring of X at a point $p \in X$. One can verify that \mathcal{O} defines a presheaf on X , and that its stalk at p coincides with the local ring \mathcal{O}_p —which is precisely why we adopt this notation in the first place.

We call a presheaf \mathcal{F} on X a **sheaf** if for every union of open sets $U = \bigcup_{i \in I} V_i$, we have

- (i) **(Identity Law)** If $s, t \in \mathcal{F}(U)$ satisfies $s|_{V_i} = t|_{V_i}$ for all i , then $s = t$.
- (ii) **(Gluing Law)** If $\{s_i \in \mathcal{F}(V_i) : i \in I\}$ satisfies $s_i|_{V_i \cap V_j} = s_j|_{V_i \cap V_j}$, then there exists **gluing section** $s \in \mathcal{F}(U)$ such that $s|_{V_i} = s_i$ for all i .

Definition 5.2.1. (Constant sheaves of abelian groups) Let X be a topological space and A an abelian group. Give A the discrete topology. One may check that assigning $\mathcal{A}(U)$ to be the abelian group of all continuous functions form a sheaf with the obvious restriction map forms a sheaf on X .¹ \mathcal{A} is called the **constant sheaf of A on X** . The naming comes from the fact that for every connected $U \subseteq X$, the abelian group $\mathcal{A}(U)$ is isomorphic to A .

For each \mathfrak{C} -valued presheaf \mathcal{F} on X , its **sheafification** is the unique (up to a unique isomorphism) \mathfrak{C} -valued sheaf \mathcal{F}^+ on X together with a \mathfrak{C} -valued sheaf morphism $\theta : \mathcal{F} \rightarrow \mathcal{F}^+$ that satisfies the **universal property**: For each \mathfrak{C} -valued sheaf homomorphism $\varphi : \mathcal{F} \rightarrow \mathcal{G}$, there exists a unique \mathfrak{C} -valued sheaf homomorphism $\tilde{\varphi} : \mathcal{F}^+ \rightarrow \mathcal{G}$ that makes the diagram:

$$\begin{array}{ccc} \mathcal{F} & \xrightarrow{\theta} & \mathcal{F}^+ \\ & \searrow \varphi & \downarrow \tilde{\varphi} \\ & & \mathcal{G} \end{array}$$

commute.

Theorem 5.2.2. (Existence of sheafification of sheaves of good category) Let X be a topological space, and \mathcal{F} a presheaf of abelian groups on X . The sheafification can be defined by setting $\mathcal{F}^+(U)$ to be the set of functions s from U to $\bigcup_{P \in U} \mathcal{F}_P$ such that:

- (i) $s(P) \in \mathcal{F}_P$.
- (ii) For each $P \in U$, there exists neighborhood V of P contained by U , and an element $t \in \mathcal{F}(V)$ such that we have $(V, t) = s(Q) \in \mathcal{F}_Q$ for all $Q \in V$.

with the usual restriction map forms a sheaf that satisfies the universal property.

Proof. It is not difficult to check that \mathcal{F}^+ forms a sheaf. The morphism $\theta : \mathcal{F} \rightarrow \mathcal{F}^+$ is given by:

$$g \in \mathcal{F}(U) \mapsto s \in \mathcal{F}^+(U), \quad \text{where } s(P) = (U, g) \in \mathcal{F}_P$$

We now show (\mathcal{F}^+, θ) satisfies the universal property. Fix $\varphi : \mathcal{F} \rightarrow \mathcal{G}$, we may define $\tilde{\varphi} : \mathcal{F}^+ \rightarrow \mathcal{G}$ by mapping $s \in \mathcal{F}^+(U) \mapsto f \in \mathcal{G}(U)$ where $f \in \mathcal{G}(U)$ is the gluing section of $\{\varphi(t) \in \mathcal{G}(V) : P \in V \subseteq U, t \in \mathcal{F}(V) : (V, t) = s(Q) \in \mathcal{F}_Q \text{ for all } Q \in V\}_{P \in U}$. ■

Theorem 5.2.3. (Sheafification of a sheaf is itself) Let X be a topological space, and \mathcal{F} a sheaf of abelian groups on X . Then, the sheafification $\theta : \mathcal{F} \rightarrow \mathcal{F}^+$ is a abelian group-valued sheaf isomorphism.

¹Use paste lemma to prove the gluing law.

Proof. ■

Let \mathfrak{C} be the category of abelian group. Even though the kernel of a sheaf homomorphism must be also be a sheaf, the image we define earlier may only be a presheaf. Because of such, in the category $\mathbf{Sh}_{\mathfrak{C}}(X)$ of sheaf of abelian groups on X , we define **image of a sheaf homomorphism** $\varphi : \mathcal{F} \rightarrow \mathcal{G}$ to be the sheafification of the induced sheaf $U \mapsto \varphi(\mathcal{F}(U))$.

Equivalent Definition 5.2.4. (Short exact sequences of sheaves of abelian groups)
Let X be a topological space and let

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{G} \longrightarrow \mathcal{H} \longrightarrow 0$$

be a short sequence of sheaves of abelian groups on X . The followings are equivalent:

- (i) $0 \rightarrow \mathcal{F} \rightarrow \mathcal{G} \rightarrow \mathcal{H} \rightarrow 0$ is exact.
- (ii) For all open $U \subseteq X$, the sequence $0 \rightarrow \mathcal{F}(U) \rightarrow \mathcal{G}(U) \rightarrow \mathcal{H}(U) \rightarrow 0$ is exact.
- (iii) For all $P \in X$, the sequence $0 \rightarrow \mathcal{F}_P \rightarrow \mathcal{G}_P \rightarrow \mathcal{H}_P \rightarrow 0$ is exact.

Proof. ■

Given a sheaf \mathcal{F} on X , a subspace $Z \subseteq X$, and a continuous map $f : X \rightarrow Y$, and a sheaf \mathcal{G} on Y , the **direct image sheaf** $f_*\mathcal{F}$ is a sheaf on Y defined by $U \mapsto \mathcal{F}(f^{-1}(U))$ with the restriction map being that of \mathcal{F} , the **inverse image sheaf** $f^{-1}\mathcal{G}$ is the sheafification of the presheaf $U \mapsto \lim_{V \supseteq f(U)} \mathcal{G}(V)$, and the **restriction sheaf** of \mathcal{F} onto Z denoted by $\mathcal{F}|_Z$ is simply the inverse image sheaf of \mathcal{F} under the inclusion map $Z \hookrightarrow X$.

5.3 Scheme

Let A be a ring and \mathfrak{a} an ideal in A . We denote $V(\mathfrak{a}) \subseteq \text{Spec } A$ the set of prime ideals that contains \mathfrak{a} .

Theorem 5.3.1. (Zariski topology on $\text{Spec } A$) Let A be a ring and $\{\mathfrak{a}_\alpha\}$ a collection of ideals in A . Then:

- (i) $V(A) = \emptyset$ and $V(0) = \text{Spec } A$.
- (ii) $V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2) = V(\mathfrak{a}_1 \cap \mathfrak{a}_2)$.
- (iii) $\bigcap V(\mathfrak{a}_\alpha) = V(\sum \mathfrak{a}_\alpha)$.
- (iv) $V(\mathfrak{a}_1) \subseteq V(\mathfrak{a}_2) \iff \sqrt{\mathfrak{a}_1} \supseteq \sqrt{\mathfrak{a}_2}$

Proof. (i) is clear. (ii) follows from the basic property that if a prime ideal contains the intersection of a finite collection of ordinary ideals, then the prime contains at least one of the ordinary ideal. (iii) follows from the fact that sum of any collection of ideal is the smallest ideal that contains the union the collection. (iv) follows from the equivalent definitions of radical ideals. ■

Because of **theorem 5.3.1**, we may define **Zariski topology** on $\text{Spec } A$ by defining the closed subset to be $\{V(\mathfrak{a}) \subseteq \text{Spec } A : \mathfrak{a} \subseteq A \text{ is an ordinary ideal}\}$. Note that for each $f \in A$, we may associate it with an open subset of $\text{Spec } A$ by defining

$$D(f) \triangleq \text{Spec } A - V(\langle f \rangle)$$

Theorem 5.3.2. (Property of open sets associated with element of the underlying ring) Let A be a ring and $f, g \in A$. Then:²

- (i) $D(f) = \{\mathfrak{p} \in \text{Spec } A : f \notin \mathfrak{p}\}$.
- (ii) $D(f) \subseteq D(g) \iff V(\langle f \rangle) \supseteq V(\langle g \rangle)$.
- (iii) $D(f) \cap D(g) = D(fg)$.

Proof. Unroll the definitions. ■

The **structure sheaf** \mathcal{O} on $\text{Spec } A$ is a sheaf of ring defined by assigning each U the ring of functions $s : U \rightarrow \bigsqcup_{\mathfrak{p} \in U} A_{\mathfrak{p}}$ that satisfies:³

- (i) $s(\mathfrak{p}) \in A_{\mathfrak{p}}$ for all $\mathfrak{p} \in U$.

²If you wish, you make think of our notation D stands for "the set of local rings whose denominator Doesn't contain".

³Checking that this indeed forms a sheaf isn't difficult.

- (ii) For each $\mathfrak{p} \in U$, there exists neighborhood V of \mathfrak{p} contained by U and exist $a, f \in A$ such that $f \notin \mathfrak{q}$ and $s(\mathfrak{q}) = a/f$ for all $\mathfrak{q} \in V$.

Theorem 5.3.3. (Basic property of affine scheme $\text{Spec } A$) Let A be a ring, and \mathcal{O} the structure sheaf on $\text{Spec } A$. Then:

- (i) For all $\mathfrak{p} \in \text{Spec } A$, the stalk $\mathcal{O}_{\mathfrak{p}}$ is isomorphic to the local ring $A_{\mathfrak{p}}$.
- (ii) For all $f \in A$, the ring $\mathcal{O}(D(f))$ is isomorphic to A_f .
- (iii) $\mathcal{O}(\text{Spec } A) \cong A$ as rings.

Proof. (i): Let $\varphi : \mathcal{O}_{\mathfrak{p}} \rightarrow A_{\mathfrak{p}}$ be the ring homomorphism induced by universal property of direct limit with $\mathcal{O}(U) \rightarrow A_{\mathfrak{p}}; s \mapsto s(\mathfrak{p})$. In other words, $\varphi : \mathcal{O}_{\mathfrak{p}} \rightarrow A_{\mathfrak{p}}$ has the action $[(U, s)] \mapsto s(\mathfrak{p})$. We are required to prove φ is bijective. Fix $a/f \in A_{\mathfrak{p}}$. Because $\mathfrak{p} \in D(f)$ and because $s \in \mathcal{O}(D(f))$, $s(\mathfrak{q}) \triangleq a/f$ is well defined, we see φ maps $[(D(f), s)]$ to a/f . We have shown φ is surjective.

Let $s, t \in \mathcal{O}(U)$ and $s(\mathfrak{p}) = t(\mathfrak{p})$. To prove φ is injective, we only have to prove $s|_V = t|_V$ for some neighborhood $V \subseteq U$ of \mathfrak{p} . By shrinking U if necessary, we may find $a, f, b, g \in A$ such that:

$$s(\mathfrak{q}) \triangleq a/f, t(\mathfrak{q}) \triangleq b/g, \quad \text{for all } \mathfrak{q} \in U.$$

Because $s(\mathfrak{p}) = t(\mathfrak{p})$, we know $a/f = b/g \in A_{\mathfrak{p}}$, which implies $h(ag - bf) = 0 \in A$ for some $h \in A - \mathfrak{p}$. We now see that $V \triangleq U \cap D(h)$ suffices.

(ii): Let $\psi_f : A_f \rightarrow \mathcal{O}(D(f))$ be the ring homomorphism that sends a/f^n to $s \in \mathcal{O}(D(f))$ where $s(\mathfrak{p}) = a/f^n$ for all $\mathfrak{p} \in D(f)$. Let $\psi(a/f^n) = \psi(b/f^m)$. To prove ψ is injective, we only have to prove $a/f^n = b/f^m \in A_f$.

Because for each $\mathfrak{p} \in D(f)$, we have $a/f^n = b/f^m \in A_{\mathfrak{p}}$ by construction, we know for each $\mathfrak{p} \in D(f)$, there exists $h \in \text{Ann}(af^m - bf^n) - \mathfrak{p}$ is nonempty, i.e., $\text{Ann}(af^m - bf^n) \not\subseteq \mathfrak{p}$. We have shown that for all $\mathfrak{p} \in D(f)$, we have $\mathfrak{p} \notin V(\text{Ann}(af^m - bf^n))$. That is, $D(f) \cap V(\text{Ann}(af^m - bf^n)) = \emptyset$, which implies $V(\text{Ann}(af^m - bf^n)) \subseteq V(\langle f \rangle)$, which by [theorem 5.3.1](#) further implies $f \subseteq \sqrt{\text{Ann}(af^m - bf^n)}$. It now follows that $f^r(af^m - bf^n) = 0 \in A$ for some $r \geq 0$, which implies $a/f^n = b/f^m \in A_f$, as desired.

We now prove ψ_f is surjective. Let $s \in \mathcal{O}(D(f))$. By definition of structure sheaf, we know there exists $\{h_i \in A : i \in I\}$ such that:

- (I) $D(f) \subseteq \bigcup_{i \in I} D(h_i)$.
- (II) $s(\mathfrak{p}) = a_i/h_i \in A_{\mathfrak{p}}$ for all $i \in I$ and $\mathfrak{p} \in D(h_i) \cap D(f)$.

where I may be infinite. We claim that there exists finite subset $J \subseteq I$ such that $D(f) \subseteq \bigcup_{i \in J} D(h_i)$. By (I), the relationship between $D(f)$ and $V(\langle f \rangle)$, and the property of topology of $\text{Spec } A$, we have:

$$V(\langle f \rangle) \supseteq \bigcap_{i \in I} V(\langle h_i \rangle) = V\left(\sum_{i \in I} \langle h_i \rangle\right)$$

Again, this by the property of topology of $\text{Spec } A$ implies $f \in \sqrt{\sum_{i \in I} \langle h_i \rangle}$, which implies that for some $n \geq 1$, we may write f^n as a finite sum:

$$f^n = \sum_{i=1}^r b_i h_i, \quad \text{where } b_i \in A$$

In other words, $f \in \sqrt{\sum_{i=1}^r \langle h_i \rangle}$, which by equivalent definitions of radical ideals implies $\sqrt{\langle f \rangle} \subseteq \sqrt{\sum_{i=1}^r \langle h_i \rangle}$. The claim now follows from the property of topology of $\text{Spec } A$ and the relationship between $D(f)$ and $V(\langle f \rangle)$.⁴

We from now on write $D(f) \subseteq D(h_1) \cup \dots \cup D(h_r)$. Fix i and j . Noting that $\psi_{h_i h_j} : A_{h_i h_j} \rightarrow \mathcal{O}(D(h_i h_j))$ maps both $a_i h_j / h_i h_j$ and $a_j h_i / h_i h_j$ to $\tilde{s}|_{D(h_i h_j)}$, where $\tilde{s} \in \mathcal{O}(D(h_1) \cup \dots \cup D(h_r))$ comes from the gluing axioms of sheaf and:

$$\{s_l \in \mathcal{O}(D(h_l)) : 1 \leq l \leq r \text{ and } s_l(\mathfrak{p}) \triangleq a_l / h_l \text{ for all } \mathfrak{p} \in D(h_l)\}$$

we see from injectivity of $\psi_{h_i h_j} : A_{h_i h_j} \rightarrow \mathcal{O}(D(h_i h_j))$ that:

$$\frac{a_i h_i}{h_i h_j} = \frac{a_j h_i}{h_i h_j} \in A_{h_i h_j}.$$

■

A **ringed space** is a pair (X, \mathcal{O}) consisting of a topological space X and a sheaf of rings \mathcal{O} on X called the **structure sheaf**. A **ringed space morphism** from X to Y is a pair $(f, f^\#)$ of a continuous map $f : X \rightarrow Y$ and a sheaf morphism $f^\#$ from the structure sheaf of Y to the direct image of structure sheaf of X under f .

A ringed space is called a **locally ringed space** if the stalk of its structure sheaf at each point is a local ring. A **locally ringed space morphism** from X to Y is a ringed space morphism $(f, f^\#)$ such that the ring homomorphism from the stalk of the structure sheaf of Y to the stalk of the direct image sheaf induced by $f^\#$ are moreover local ring homomorphisms.

⁴Note that our argument for finding this finite subcover is morally the same as equivalent definition of ideals sum

An **affine scheme** is a locally ringed space isomorphic as a locally ringed space to the spectrum of some ring. A **scheme** is a locally ringed space that has an open cover consisting of open sets when equipped with the restricted sheaf is an affine scheme. A **scheme morphism** is then just a locally ringed space morphism.

5.4 \mathcal{O} -modules

Given a ringed space (X, \mathcal{O}) , if we say a sheaf \mathcal{F} of abelian groups on X is a **\mathcal{O} -module**, we are assigning each abelian group $\mathcal{F}(U)$ a $\mathcal{O}(U)$ -module structure compatible not only with the addition of $\mathcal{F}(U)$ but also the restriction maps in the sense that:

$$(fs)|_V = (f|_V)(s|_V), \quad \text{for each } f \in \mathcal{O}(U), s \in \mathcal{F}(U) \text{ and } V \subseteq U$$

A **\mathcal{O} -module morphism** $\varphi : \mathcal{F} \rightarrow \mathcal{G}$ is then just a sheaf morphism such that all $\varphi(U)$ are also $\mathcal{O}(U)$ -module homomorphisms.

Let $X \subseteq \mathbb{C}^n$ be an affine variety, and let M be an $A(X)$ -module. We may define a presheaf \widetilde{M} of abelian groups on X by setting $\widetilde{M}(U)$ to be the set of functions s from U to $\bigcup_{P \in U} M_P$ such that:

- (i) $s(P) \in M_P$.
- (ii) For all $P \in U$, there exists $F \in \mathbb{C}[x_1, \dots, x_n]$ such that $P \in X - V(F) \subseteq U$ and exists $t \in M_F$ such that $t_P = s(P)$.

We say a sheaf \mathcal{F} of abelian groups on X is **quasi-coherent** if X has an open cover $\{U_\alpha\}$ such that U_α is quasi-variety isomorphic to some affine variety and there exists $(A(U_\alpha))$ -module M_α such that:

$$\mathcal{F}|_{U_\alpha} = \widetilde{M_\alpha}$$

We say X is **coherent** if M_α are moreover all finitely generated.

Chapter 6

Not used yet

6.1 Maybe later

Theorem 6.1.1. (Algebraic structure of global ring, local ring, and function field of projective quasi variety) Let $X \subseteq \mathbb{P}^n$ be a projective quasi variety. We have

- (i) $\mathcal{O}(X) = k$.
- (ii) $\mathcal{O}_{p,X} \cong \Gamma(X)_{(\mathfrak{m}_p)}$ for all $p \in X$.
- (iii) $K(X) \cong \Gamma(X)_{(\langle x \rangle)}$.

6.2 Some Fulton

Given two affine varieties $V \subseteq \mathbb{A}^n, W \subseteq \mathbb{A}^m$, we say mapping $\varphi : V \rightarrow W$ is a **polynomial map**¹ if there are polynomials $T_1, \dots, T_m \in k[x_1, \dots, x_n]$ such that $\varphi(a) = (T_1(a), \dots, T_m(a))$ for all $a \in V$. Every mapping $\varphi : V \rightarrow W$, polynomial or not, induce a ring homomorphism

$$\tilde{\varphi} : \mathcal{F}(W, k) \rightarrow \mathcal{F}(V, k) \quad f \mapsto f \circ \varphi$$

Clearly, if φ is a polynomial map, then $\tilde{\varphi}$ maps $\Gamma(W)$ into $\Gamma(V)$ and is in fact an \mathbb{A} -algebra homomorphism. By **proposition 6.6.8**, there exists an obvious one-to-one correspondence between $(k[x_1, \dots, x_n])^m$ and some subcollection of the space of polynomials map from \mathbb{A}^n to \mathbb{A}^m , so if polynomial map $T : \mathbb{A}^n \rightarrow \mathbb{A}^m$ satisfies

$$\forall a \in \mathbb{A}^n, T(a) = (T_1(a), \dots, T_m(a)) \quad , \text{ for some } T_1, \dots, T_m \in k[x_1, \dots, x_n]$$

it make sense for us to denote $T = (T_1, \dots, T_m)$.

Theorem 6.2.1. (Natural one-to-one correspondence between $\text{Hom}(\Gamma(W), \Gamma(V))$ and $\text{Hom}(V, W)$) Given two affine variety $V \subseteq \mathbb{A}^n, W \subseteq \mathbb{A}^m$, if we denote

$$\begin{aligned} \text{Hom}(V, W) &\triangleq \{\text{polynomial } \varphi : V \rightarrow W\} \\ \text{Hom}(\Gamma W, \Gamma V) &\triangleq \{\mathbb{A}\text{-algebra homomorphism } \phi : \Gamma(W) \rightarrow \Gamma(V)\} \end{aligned}$$

then the mapping $\varphi \mapsto \tilde{\varphi}$ forms a bijection between them.

Proof. It is easy to check the mapping $\varphi \mapsto \tilde{\varphi}$ is injective. We now prove that it is surjective. Fix $\alpha \in \text{Hom}(\Gamma W, \Gamma V)$. Let $T_i \in k[x_1, \dots, x_n]$ satisfies $\alpha([x_i]) = [T_i]$ for each i , and define polynomial map $T \triangleq (T_1, \dots, T_m) : \mathbb{A}^n \rightarrow \mathbb{A}^m$. Note that $\Gamma(\mathbb{A}^n) \cong k[x_1, \dots, x_n]$. It is then easy to check $\tilde{T} : \Gamma(\mathbb{A}^m) \rightarrow \Gamma(\mathbb{A}^n)$ maps $I(W)$ into $I(V)$, which allow us to check $T(V) \subseteq W$. To finish the proof, just check $\tilde{T}|_V : \Gamma W \rightarrow \Gamma V$ is identical with α . ■

A polynomial map $\varphi : V \rightarrow W$ is an **k -affine variety isomorphism** if it's bijective with inverse being also a polynomial map. **Theorem 6.2.1** shows that two affine varieties are isomorphic if and only if their coordinate rings are.

By an **affine change of coordinate** on \mathbb{A}^n , we mean a bijective polynomial map $T : \mathbb{A}^n \rightarrow \mathbb{A}^n$ such that each of its component $T_i \in k[x_1, \dots, x_n]$ is of degree 1.

¹One may check that polynomial maps and affine varieties together form a category

6.3 Dimension Theory

Theorem 6.3.1. (Equivalent definition of variety dimension: Krull dimension of coordinate ring) Given variety $V \subseteq \mathbb{A}^n$, its dimension equals to the Krull dimension of its coordinate ring $\Gamma(V) \cong k[x_1, \dots, x_n]/I(V)$.

Proof. Let $Z_0 \subset \dots \subset Z_m$ be a chain of distinct irreducible closed subset of V . As one may check with **ring correspondence theorem**,

$$I(Z_m) + I(V) \subset \dots \subset I(Z_0) + I(V) \subseteq \Gamma(V)$$

forms a chain of distinct prime ideals of $\Gamma(V)$. We have shown $\dim(V) \leq \text{Krudim}(\Gamma V)$.

Let $\mathfrak{p}_0 \subset \dots \subset \mathfrak{p}_m$ be a chain of distinct prime ideals of $\Gamma(V)$, so again by **ring correspondence theorem**, there exists a chain $I(V) \subseteq I_0 \subset \dots \subset I_m$ of distinct prime ideals of $k[x_1, \dots, x_n]$. It is easy to check that $V(I_m) \subset \dots \subset V(I_0)$ indeed forms a distinct irreducible closed subset of V by corollary of Nullstellensatz. ■

Let $V \subseteq \mathbb{A}^n$ be a nonempty affine variety. We use the notation $k(V) \triangleq \text{Frac}(\Gamma V)$ to denote the **field of rational function on V** . Given rational function f on V , we say $f \in k(V)$ is **defined** at $a \in V$ if there exists $g, h \in \Gamma V$ such that $f = gh^{-1}$ and $h(a) \neq 0$. Given $a \in V$, we use the notation $\mathcal{O}_a(V)$ to denote the ring of rational functions on V that are defined at a . We have

$$k \subseteq \Gamma(V) \subseteq \mathcal{O}_a(V) \subseteq k(V)$$

Clearly, for each $f \in \mathcal{O}_a(V)$, we may well-define a **value of f at a** by saying $f(a) \triangleq g(a)h(a)^{-1}$, and we see that indeed, $\mathcal{O}_a(V)$ is a local ring whose maximal ideal is

$$\mathfrak{m}_a(V) \triangleq \{f \in \mathcal{O}_a(V) : f(a) = 0\}$$

Lemma 6.3.2. Suppose $B \subseteq A$, A integral domain, and B integrally closed. We have

$$\text{Krudim}(A_{\mathfrak{m}}) = \text{Krudim}(B_{B \cap \mathfrak{m}})$$

Theorem 6.3.3. (Equivalent Definition of variety dimension: Transcendence degree of field of rational function) Given nonempty variety $V \subseteq \mathbb{A}^n$, its dimension equals $\text{trdeg}_k k(V)$.

Proof. According to **Noether normalization lemma**, there exists $x_1, \dots, x_r \in \Gamma(V)$, algebraically independent over k with $r = \text{Krudim}(\Gamma V)$ such that $\Gamma(V)$ integral over $k[x_1, \dots, x_r]$. This implies $k(V)$ algebraic over $k(x_1, \dots, x_r)$ and thus $\text{trdeg}_k k(V) = r^2$. ■

²Clearly, $\text{trdeg}_k k(x_1, \dots, x_r) = r$

6.4 Some Fulton 2

For intuitively geometrical reason, we usually call locus of a single non-constant polynomial $F \in k[x_1, \dots, x_n]$ a **hypersurface**, and a hypersurface in \mathbb{A}^2 an **affine plane curve**.

Lemma 6.4.1. (Intuitive Lemma) If $F, G \in k[x, y]$ have no common factor, then $V(F, G) = V(F) \cap V(G)$ is a finite set of points.

Proof. ■

Because algebraically closed field is always infinite, the following classification theorem particularly applies to affine varieties.

Theorem 6.4.2. (Classification of irreducible affine variety in \mathbb{A}^2) If k is infinite, every irreducible affine algebraic set $V \subseteq \mathbb{A}^2$ falls into one of the following class:

- (a) \mathbb{A}^2 .
- (b) Empty set.
- (c) A finite set.
- (d) $V(F)$ where $F \in k[x_1, x_2]$ is irreducible.

Proof. Clearly, if $I(V) = 0$ ³ then $V = \mathbb{A}^2$, class (a). Also, if $I(V)$ contains a nonzero constant, then V is empty, class (b). We have shown that if V is not in class (a) nor class (b), then $I(V)$ contains some non-constant polynomial F .

Because $k[x_1, x_2]$ is a UFD, we may write $F = F_1 \cdots F_n$ where F_1, \dots, F_n are all irreducible. It then follows from $I(V)$ being prime that $F_1 \in I(V)$, WLOG. If $I(V) = \langle F_1 \rangle$, then V is in class (d), so suppose there exists some $G \in I(V) - \langle F_1 \rangle$. This immediately implies $V \subseteq V(F_1, G)$, and since F_1 is irreducible and $G \notin \langle F_1 \rangle$, we may apply [Lemma 6.4.1](#) to see that V is finite, class (c). ■

³Zero ideal is prime in the integral domain $k[x_1, x_2]$.

6.5 More Equivalent Definitions of DVR

Let $u \in K^\times$. We sometimes denote the **fractional principal ideal** Au by $\langle u \rangle$. It is clear that $\langle u \rangle$ is invertible with inverse $\langle u^{-1} \rangle$.

Theorem 6.5.1. (Equivalent Definitions of DVR) Given an integral domain D , the following are equivalent:

- (i) D is a DVR with discrete valuation ν .
- (ii) D is a local Euclidean domain and not a field.
- (iii) D is a local PID and not a field.
- (iv) D is local and every nonzero fractional ideal of D is invertible.
- (v) D is local and
- (vi) D is local, Noetherian and of Krull dimension 1.

Proof. For (i) \implies (ii), note that D is local because **ideals of D are totally ordered by inclusion**, that ν is the desired Euclidean function⁴, and D is not a field because ν is nontrivial.

For (ii) \implies (iii), just recall Euclidean domains are PID.

For (i) \implies (iv), let $\mathfrak{a}_1 = \langle x \rangle$ in Equation ??, and let M be a nonzero fractional ideal. Let $y \in D$ satisfies $yM \subseteq D$, so $yM = \langle x^k \rangle$ for some $k \in \mathbb{N}$. This implies M is a fractional principal ideal $M = \langle x^{k - \frac{\nu(y)}{p}} \rangle$, thus invertible.

For (iv) \implies (i), first note that because every integral ideal of D is invertible, thus finitely generated, **D is Noetherian**. ■

Theorem 6.5.2. (Sufficient conditions for valuation rings to be discrete) If D is a valuation ring of $\nu : \text{Frac}(D) \rightarrow \Gamma \cup \{\infty\}$, then the following are equivalent:

- (a) ν is discrete.
- (b) D is Noetherian.
- (c) D is a principal ideal domain.

⁴Suppose $x, y \in D, y \neq 0$. If $\frac{x}{y} \in D$, then $x = y \cdot \frac{x}{y} + 0$ suffices. If $\frac{x}{y} \notin D$, then $x = y + (x - y)$ suffices.

6.6 PID, UFD and Gauss Lemma

Let A be a ring and $a \in A$ be a non-unit nonzero element. We say a is **irreducible** if $a = xy \implies x$ is a unit or y is a unit. We say a is **prime** if $\langle a \rangle$ is prime. We say an integral domain D is a **UFD (Unique Factorization Domain)** if every nonzero non-unit element of D can be written as some finite product of irreducible elements, up to units and change of order. We say an integral domain is a **PID (Principal Ideal Domain)** if every ideal is principal. We say an integral domain is a **GCD domain** if there always exists a unique minimal principal ideal containing the ideal generated by two given elements. If D is a GCD domain, and $x, y \in D$, we use $\gcd(x, y)$ to denote the unique principal ideal containing $\langle x, y \rangle$. Clearly, every PID is Noetherian, and moreover:

Theorem 6.6.1. (Irreducibles are prime in PID) If D is a PID and $a \in D$ is irreducible, then a is prime.

Proof. Let $bc \in \langle a \rangle$. From the premise, if we write

$$\langle a, b \rangle = \langle d \rangle \text{ and } a = de$$

We see that either d or e is a unit. If e is a unit, then when we write $b = yd$ we see $b = yae^{-1} \in \langle a \rangle$. If d is a unit, then $\langle a, b \rangle = \langle d \rangle = D$ implies existence of some $x, y \in D$ such that $xa + yb = 1$ which implies $c = cxa + ybc \in \langle a \rangle$.⁵ ■

Corollary 6.6.2. (PID are UFD) If D is a PID, then D is an UFD.

Proof. Let

$$\mathcal{U} \triangleq \{ \langle x \rangle \subseteq D : x \in D \text{ can't be written as some finite product of irreducible elements.} \}$$

Assume for a contradiction that \mathcal{U} is nonempty. Because D is Noetherian, there exists maximal $\langle x \rangle \in \mathcal{U}$. By construction, x is reducible and thus not prime, which implies the existence of some maximal ideal $\langle y \rangle$ that strictly include $\langle x \rangle$. Because $\langle y \rangle \notin \mathcal{U}$, we have irreducible factorization $y = a_1 \cdots a_n$. Let $x = sy$ and $u \triangleq sa_2 \cdots a_n$. We shall cause a contradiction from $x = a_1 u$. If $\langle u \rangle \notin \mathcal{U}$, then because a_1 is irreducible, we see x can be written as a finite product of irreducible elements⁶, a contradiction. If $\langle u \rangle \in \mathcal{U}$, then by maximality of $\langle x \rangle$, we have $\langle u \rangle = \langle x \rangle$, which implies a_1 is a unit, a contradiction.

We now prove the uniqueness of factorization. Suppose

$$a = p_1 \cdots p_n = q_1 \cdots q_m$$

⁵Because $bc \in \langle a \rangle$

⁶You may check that in general, if and $\langle t \rangle = \langle t' \rangle$, then $t = u't'$ for some unit u'

are two factorization. Because p_1 is prime, for some i we have $q_i \in \langle p_1 \rangle$. WLOG suppose $i = 1$. Because q_1 is irreducible, we see that $q_1 = u_1 p_1$ for some unit u_1 , which implies⁷

$$p_2 \cdots p_n = u_1 q_2 \cdots q_m$$

Continuing this process, we have

$$p_n = u_{n-1} q_n \cdots q_m$$

The proof then follows from p_n being irreducible. ■

Theorem 6.6.3. (UFD are GCD domain) If D is an UFD, then D is a GCD domain.

Proof. Let $x, y \in D$. If any of x, y is a unit, then $\langle 1 \rangle$ is the unique minimal principal ideal containing $\langle x, y \rangle$, and if y is zero, then $\langle x \rangle$ is the unique minimal principal ideal containing $\langle x, y \rangle$. Now suppose they have the irreducible decomposition:

$$x = (x_1 \cdots x_t) x_{t+1} \cdots x_r \text{ and } y = (x_1 \cdots x_t) y_{t+1} \cdots y_s \quad (6.1)$$

where $ux_i \neq y_j$ for all unit u and $i, j > t$. Define $d \triangleq x_1 \cdots x_t$. Clearly, if $\langle d \rangle$ is the smallest principal ideal containing $\langle x, y \rangle$, then it is the unique minimal principal ideal containing $\langle x, y \rangle$. Therefore, it suffices to prove for any $\langle f \rangle$ containing $\langle x, y \rangle$, we have $\langle d \rangle \subseteq \langle f \rangle$.

If f is a unit, then what we want to prove trivially holds true. Assume for a contradiction that $\langle d \rangle \not\subseteq \langle f \rangle$. Clearly, the irreducible decomposition of f must always contain some g that doesn't divide d in the sense that $d \notin gD$. This implies for some $i, j > t$, g divides both x_i and y_j . This cause a contradiction to how we construct [Equation 6.1](#): $y_j \notin D^\times x_i$ for all $i, j > t$. ■

Let A be a ring, and $f \in A[x_1, \dots, x_n]$ a formal polynomial. Its **content** $\text{cont}(f)$ is the ideal in A generated by its coefficients, and we say f is **primitive** if $\text{cont}(f) = A$. Gauss show that a non-constant polynomial in $\mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ if it is irreducible in $\mathbb{Q}[x]$ and primitive in $\mathbb{Z}[x]$. Here, we generalize his result to the case of commutative ring.

Theorem 6.6.4. (Gauss lemma over commutative ring) For each pair of polynomials $f, g \in A[x_1, \dots, x_n]$, we have

$$\text{cont}(fg) \subseteq \text{cont}(f) \text{cont}(g) \subseteq \sqrt{\text{cont}(fg)}$$

Proof. $\text{cont}(fg) \subseteq \text{cont}(f) \text{cont}(g)$ is clear. By definition of radical, to prove $\text{cont}(f) \text{cont}(g) \subseteq \sqrt{\text{cont}(fg)}$, we only have to prove every prime ideal containing $\text{cont}(fg)$ also contains $\text{cont}(f) \text{cont}(g)$. Let $\mathfrak{p} \subseteq A$ be a prime ideal containing $\text{cont}(fg)$. Because

$$\mathfrak{p}[x_1, \dots, x_n] \triangleq \{h \in A[x_1, \dots, x_n] : \text{All coefficients of } h \text{ lie in } \mathfrak{p}\}$$

⁷Because A is an integral domain.

forms a prime ideal of $A[x_1, \dots, x_n]$ as one can check and because $fg \in \mathfrak{p}[x_1, \dots, x_n]$, we see that one of f, g is an element of $\mathfrak{p}[x_1, \dots, x_n]$, i.e., one of $\text{cont}(f), \text{cont}(g)$ is a subset of \mathfrak{p} . This immediately implies $\text{cont}(f)\text{cont}(g) \subseteq \mathfrak{p}$. ■

Noting that in a GCD domain

$$\gcd(x, y, z) \triangleq \gcd(d, z) \text{ where } \langle d \rangle = \gcd(x, y)$$

and so

$$\gcd(\text{cont}(a_n x^n + \dots + a_1 x + a_0)) \triangleq \gcd(a_0, \dots, a_n) \text{ is well defined.}$$

We may give the Gauss lemma for UFD, whose proof is obvious if one use the notion of "divisors".

Theorem 6.6.5. (Gauss lemma over UFD) If A is an UFD, then for each pair of polynomials $f, g \in A[x_1, \dots, x_n]$, we have

$$\gcd(\text{cont}(fg)) = \gcd(\text{cont}(f)) \gcd(\text{cont}(g))$$

Corollary 6.6.6. (Gauss lemma over UFD) Given UFD A with $K \triangleq \text{Frac}(A)$, if $f \in A[x_1, \dots, x_n]$ is irreducible, then $f \in K[x_1, \dots, x_n]$ is also irreducible.

Proof. If $f = gh \in K[x_1, \dots, x_n]$ is reducible, then $f = g(rh) \in A[x_1, \dots, x_n]$ is reducible, where r is the product of all denominators of coefficients of h . ■

Proposition 6.6.7. () Every algebraically closed set is infinite.

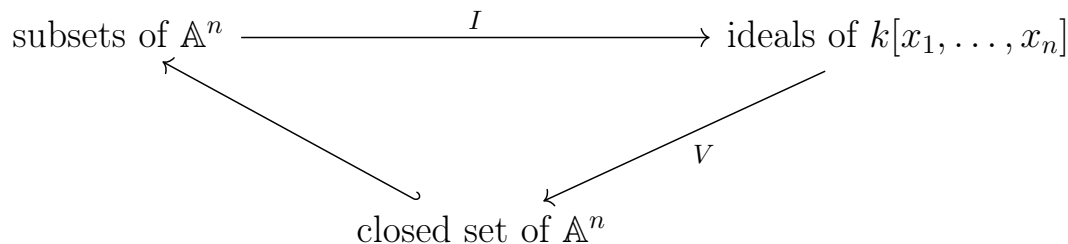
Proposition 6.6.8. () If k is an infinite field, and $F \in k[x_1, \dots, x_n]$ maps all $a \in \mathbb{A}^n$ to 0, then $F = 0$.

6.7 Archived

Moreover, clearly we have

$$I(\overline{X}) = I(X), \quad \text{for all } X \subseteq \mathbb{A}^n$$

and in summary, we have the (not commutative) diagram:



Even though not commutative at the top two nodes, indeed the diagram is commutative at the node below:

$$V = V(I(V)), \quad \text{for all closed } V \subseteq \mathbb{A}^n \quad (6.2)$$

By **Hilbert's basis theorem**, every closed set in \mathbb{A}^1 , even if k is not closed, must be either finite or the whole space.

Because of (B), if k is infinite, then \mathbb{A}^1 is irreducible, which in particular apply to the usual case when k is closed.⁸

$Y \subseteq \mathbb{A}^n$ is irreducible if and only if $I(Y)$ is prime, and in such case if Y moreover is closed, we call Y an **(affine) variety**. This in particular shows that \mathbb{A}^n are irreducible, as $I(\mathbb{A}^n) = 0$, another proof of (D). Because of (C) and (D), clearly \mathbb{A}^1 is 1-dimensional as expected. We will show in the **section on Dimension Theory** that indeed for all n , \mathbb{A}^n is n -dimensional.

⁸To see algebraically closed field is infinite, assume not and consider $1 + \prod (x - y_i)$ where y_i runs through all elements.

Chapter 7

The Great Theorems

7.1 Hilbert's Nullstellensatz and basis theorem

Theorem 7.1.1. (Hilbert's Basis Theorem) If A is Noetherian, then the polynomial ring $A[x]$ is also Noetherian.

Proof. Let X be an ideal in $A[x]$. We are required to show that X is finitely generated. Let I be the ideal in A that contains exactly the leading coefficients of elements of X . Because A is Noetherian, we may let $I = \langle a_1, \dots, a_n \rangle$ and let $f_1, \dots, f_n \in X$ have leading coefficients a_1, \dots, a_n . Let $X' \triangleq \langle f_1, \dots, f_n \rangle \subseteq X$ and let $r \triangleq \max \{\deg(f_1), \dots, \deg(f_n)\}$.

We first show

$$X = \left(X \cap \langle 1, x, \dots, x^{r-1} \rangle \right) + X' \quad (7.1)$$

Let $f \in X$ with $\deg(f) = m$ and leading coefficients a . We wish to show $f \in (X \cap \langle 1, x, \dots, x^{r-1} \rangle) + X'$. Because $a \in I$, we may find some $u_i \in A$ such that $a = \sum u_i a_i$. Clearly, these u_i satisfy

$$f - \sum u_i f_i x^{m-\deg(f_i)} \in X, \quad \text{and} \quad \sum u_i f_i x^{m-\deg(f_i)} \in X'$$

and satisfy

$$\deg \left(f - \sum u_i f_i x^{m-\deg(f_i)} \right) < m$$

Proceeding this way, we end up with $f - g = h$ where $g \in X'$ and $h \in X \cap \langle 1, x, \dots, x^{r-1} \rangle$. We have proved [Equation 7.1](#). Now, because X' is finitely generated, to show X is finitely generated, it only remains to show the ideal $X \cap \langle 1, x, \dots, x^{r-1} \rangle$ is finitely generated, which follows immediately from noting $\langle 1, x, \dots, x^{r-1} \rangle$ as a module is Noetherian. ■

Theorem 7.1.2. (Weak form of Nullstellensatz) Given field k and finitely generated k -algebra B , if B is a field then it is a finite algebraic extension of k .

Proof. A proof can be found in the end of Chapter 5 of Atiyah-MacDonald. Another proof can be found in Chapter 7 of Atiyah-MacDonald, at page 82. ■

Theorem 7.1.3. (Hilbert's Nullstellensatz) Given algebraically closed field k and ideal $I \subseteq k[x_1, \dots, x_n]$. If we let V be the locus of I :

$$V \triangleq \{x \in k^n : F(x) = 0 \text{ for all } F \in I\}$$

and let J be the defining ideal of V :

$$J \triangleq \{F \in k[x_1, \dots, x_n] : F(x) = 0 \text{ for all } x \in V\}$$

then $J = \sqrt{I}$.

Proof. $\sqrt{I} \subseteq J$ is clear. Assume for a contradiction that $F \in J - \sqrt{I}$. Because $F \notin \sqrt{I}$, there exists some prime $\mathfrak{p} \subseteq k[x_1, \dots, x_n]$ that contains \sqrt{I} but does not contain F . Denote

$$B \triangleq k[x_1, \dots, x_n]_{/\mathfrak{p}} \text{ and } g \triangleq [F] \in B \text{ and } C \triangleq B_g$$

Let \mathfrak{m} be some maximal ideal of C . Because of the k -algebra homomorphism diagram:

$$k[x_1, \dots, x_n] \xrightarrow{\text{ring quotient}} B \xrightarrow{\text{localization}} C \xrightarrow{\text{ring quotient}} C_{/\mathfrak{m}} \quad (7.2)$$

We see that by **Hilbert Basis Theorem**, **theorem 1.8.5**, and **equivalent definition of Noetherian**, $C_{/\mathfrak{m}}$ is finitely generated over k , thus a finite algebraic extension of k by **weak form of Nullstellensatz**. Because k is algebraically closed, this implies $C_{/\mathfrak{m}} \cong k$.

Now, for each $1 \leq i \leq n$, let $t_i \in k \cong C_{/\mathfrak{m}}$ be the image of $x_i \in k[x_1, \dots, x_n]$ under the k -module homomorphism in **diagram 7.2**. Letting $t \triangleq (t_1, \dots, t_n) \in k^n$, it is easy to check¹ by direct computation that **diagram 7.2** have action $G \in k[x_1, \dots, x_n] \mapsto G(t) \in k$. Because $I \subseteq \mathfrak{p}$, by construction of B we see **diagram 7.2** maps every element of I to $0 \in k$. Yet, at the same time the image of F in C is a unit by construction of C , which implies the image of F in the quotient ring $C_{/\mathfrak{m}}$ is nonzero. We have shown $t \in V$ and $F(t) \neq 0$, a contradiction. ■

¹Recall $k[x_1, \dots, x_n] = \langle x_1, \dots, x_n \rangle$.

7.2 Noether Normalization Lemma (Half way there)

Let k be a field and A a k -algebra. If we say $E \subseteq A$ is **algebraically independent over k** , we mean that there exists no $\{y_1, \dots, y_n\} \subseteq E$ and polynomial $F \neq 0 \in k[x_1, \dots, x_n]$ such that $F(y_1, \dots, y_n) = 0$. Before stating our version of **Noether Normalization Lemma**, we should prove what we should have proved in **the previous section on Integral Dependence**, so one can see the equivalency between our version and others.

Theorem 7.2.1. (Integral and Finite Type) Given rings $B \subseteq A$, if $x_1, \dots, x_n \in A$ are integral over B , then $B[x_1, \dots, x_n]$ as a B -module finitely generated.

Proof. We shall prove by induction on n . Base case $n = 1$ follows from **the second definition of integral dependence**. Let $n > 1$. Trivially, x_n is integral over $B[x_1, \dots, x_{n-1}]$, so it follows from **the second definition of integral dependence** that $B[x_1, \dots, x_n] = (B[x_1, \dots, x_{n-1}])[x_n]$ is finitely generated as a $B[x_1, \dots, x_{n-1}]$ -module. Now, because inductive hypothesis said that $B[x_1, \dots, x_{n-1}]$ is finitely generated as a B -module, we see from **theorem 1.2.6²** that indeed $B[x_1, \dots, x_n]$ is finitely generated as a B -module. ■

Corollary 7.2.2. (Integral and Finite Type) Let k be a field, and A a finitely generated k -algebra. Given any $y_1, \dots, y_r \in A$, we have

$$A \text{ as a } k[y_1, \dots, y_r]\text{-module is finitely generated} \iff A \text{ is integral over } k[y_1, \dots, y_r]$$

Proof. (\implies) : This follows from **the third definition of integral dependence**.

(\impliedby) : Because A is finitely generated as a k -algebra, there exists some m and $y'_1, \dots, y'_m \in A$ such that $A = k[y'_1, \dots, y'_m]$. The proof then follows from $A = (k[y_1, \dots, y_r])[y'_1, \dots, y'_m]$ and **Theorem 7.2.1**. ■

Theorem 7.2.3. (Noether Normalization Lemma) Let k be a field. If A is a finitely generated k -algebra, says,

$$A = k[y'_1, \dots, y'_m] \text{ for smallest } m,$$

then there exists $y_1, \dots, y_r \in A$ algebraically independent over k such that A as a $k[y_1, \dots, y_r]$ -module is finitely generated.

Proof. We shall prove by induction on m . Consider the base case $m = 1$. If y'_1 is algebraic independent over k , then $y_1 \triangleq y'_1$ suffices trivially. If not, then clearly A as a k -algebra is isomorphic to the quotient $k[y]/I$, where $k[y]$ is the formal polynomial ring and I is the (clearly nonzero) ideal of polynomials vanishing at y'_1 . Let f be the generator of I .³ The

²You may check that the module structures here all agree with scalar extension.

³ $k[y]$ is a PID (To see this, just consider smallest degree element and division algorithm.). Its nonzero prime ideals are exactly those whose generator is irreducible (To see irreducible polynomials generate prime ideals, prove that they generate maximal ideal.).

proof then follows from noting A as a k -module is generated by $1, y, \dots, y^{\deg f - 1}$.

Let $m \geq 2$. If y'_i are algebraically independent, then $y_i \triangleq y'_i$ suffices trivially. Suppose not. (Remains to show Krudim)

■

(So $\text{Krudim}(A) = 0$. HOW? Because $A = k[y]/I$ and I nonzero $\text{Krudim}(k[y]) = 1$) If A is itself a field and the algebra-defining ring homomorphism $k \longrightarrow A$ forms an injective field homomorphism, then we can talk about the **transcendence degree** $\text{trdeg}_k A$ **of** A **over** k . By Zorn's Lemma, there exists some maximal algebraically independent subset $E \subseteq A$, and by an argument similar to that for vector space, two maximal algebraically independent subsets $E_1, E_2 \subseteq A$ must have the same cardinality. It thus make sense for us to talk about the transcendence degree $\text{trdeg}_k A$.

7.3 Hilbert-Serre Theorem

Theorem 7.3.1. (Hilbert-Serre Theorem)