

Notes on Algebraic Geometry and Commutative Algebra

Eric Liu

CONTENTS

CHAPTER 1 LOCAL RING, INTEGRAL CLOSURE, AND NOETHER PAGE 3

1.1	Rings	3
1.2	Modules and Algebra	6
1.3	Localization and local ring	9
1.4	Integral dependence	13
1.5	Homological lemmas	16
1.6	Noetherian	18
1.7	Length	21
1.8	Tensor product for modules	24

CHAPTER 2 VALUATION RING AND DVR PAGE 26

2.1	Localization of ideals	26
2.2	Uniqueness of Primary Decomposition	28
2.3	Existence of Primary Decomposition in Noetherian ring	31
2.4	Artin Rings	32
2.5	Valuation Rings	35
2.6	Equivalent Characterizations of DVR	37
2.7	UFT for ideals in 1-Krull-dimensional Noetherian domain	39
2.8	Fractional Ideal	41
2.9	Dedekind domain	43

CHAPTER 3 GREAT THEOREMS LIKE A BRIDGE PAGE 45

3.1	Hilbert's Nullstellensatz and basis theorem	45
3.2	Noether Normalization Lemma (Half way there)	47

CHAPTER 4	VARIETY	PAGE 49
------------------	----------------	----------------

4.1	Topology of Zariski	49
4.2	Affine variety	52
4.3	Projective variety	54
4.4	Morphism	58
4.5	Category of Quasi Varieties	64
4.6	Rational Map (Just started)	66
4.7	Dimension Theory (Planned)	68

CHAPTER 5	SCHEME	PAGE 69
------------------	---------------	----------------

CHAPTER 6	NOT USED YET	PAGE 70
------------------	---------------------	----------------

6.1	Maybe later	70
6.2	Some Fulton	71
6.3	Dimension Theory	72
6.4	Some Fulton 2	73
6.5	More Equivalent Definitions of DVR	74
6.6	PID, UFD and Gauss Lemma	75
6.7	Archived	78

Chapter 1

Local Ring, Integral Closure, and Noether

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 R is an additive subgroup I such that $ar \in I$ for all $a \in I, r \in R$, or equivalently, the kernel of some ring homomorphism. To see the equivalency, one simply construct the **quotient ring**² R/I , under which the quotient map $\pi : R \rightarrow R/I$ is a surjective ring homomorphism whose kernel is the ideal I . Remarkably, the mapping defined by

$$\text{Ideal } J \text{ of } R \text{ that contains } I \mapsto \{[x] \in R/I : x \in J\}$$

forms a bijection between the collection of the ideals of R containing I and the collection of the ideals of R/I . This fact is commonly referred to as the **correspondence theorem** for rings.

¹Respecting addition immediately implies respecting 0 and negation.

²Consider the equivalence relation on R defined by $x \sim y \iff x - y \in I$

A **unit** is an element that has a multiplicative inverse. Under our initial requirement that rings are commutative, for a non-zero ring R to be a **field**, we only need all non-zero elements of R to be units, or equivalently, the only ideals of R to be $\{0\}$ or R itself.

We use the term **proper** to describe strict set inclusion. By a **maximal ideal**, we mean a proper ideal I contained by no other proper ideals, or equivalently³, a proper ideal I such that R/I is a field.

A **zero-divisor** is an element x that has some non-zero element y such that $xy = 0$. Again, under our initial requirement that rings are commutative, for a non-zero ring R to be an **integral domain**, we only need all non-zero elements to be zero-divisors. By a **prime ideal**, we mean a proper ideal I such that the product of two elements belongs to I only if one of them belong to I , or equivalently, a proper ideal I such that R/I is an integral domain.

There are many binary operations defined for ideals. Given two ideals I and S , we define their **sum** and **product** by

$$I + S \triangleq \left\{ \sum_{\text{finite}} x + y \in R : x \in I \text{ and } y \in S \right\} \quad IS \triangleq \left\{ \sum_{\text{finite}} xy \in R : x \in I \text{ and } y \in S \right\} \quad (1.1)$$

Note that the ideal multiplications are indeed distributive over addition, and they are both associative, so it make sense to write something like $I_1 + I_2 + I_3$ or $I_1 I_2 I_3$. Clearly, the intersection of ideals is still ideal, while the union of ideals generally are not⁴. Moreover, we define their **quotient** by

$$(I : S) \triangleq \{x \in R : xS \subseteq I\} \quad (1.2)$$

To simplify matters, we write $(I : x)$ instead of $(I : \langle x \rangle)$.

For all subsets S of some ring R , we may **generate** an ideal by setting it to be the set of all finite sum $\sum rs$ such that $r \in R$ and $s \in S$, or equivalently, the smallest ideal of R containing S . An ideal is called **principal** and denoted by $\langle x \rangle$ if it can be generated by a single element x .

An element x is called **nilpotent** if $x^n = 0$ for some $n \in \mathbb{N}$. The set of all nilpotent elements obviously form an ideal, which we call **nilradical** and denote by $\text{Nil}(R)$. Here, we give a nice description of the nilradical.

³By the Correspondence Theorem for Rings.

⁴However, $I \cup J$ generates $I + J$.

Theorem 1.1.1. (Equivalent Definition for Nilradical) We use the term **spectrum** of R and the notation $\text{spec}(R)$ to denote the set of prime ideals of R . We have

$$\text{Nil}(R) = \bigcap \text{spec}(R)$$

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

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

Let I be an ideal of the ring R . By the term **radical** of I , we mean

$$\sqrt{I} \triangleq \{x \in R : x^n \in I \text{ for some } n > 0\}$$

which is equivalent to the preimage of $\text{Nil}(R/I)$ under the quotient map and equivalent⁵ to the intersection of all prime ideals of R that contain I .

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 I, Q , we have

$$IQ \subseteq I \subseteq \sqrt{I} \text{ and } I \subseteq (I : Q)$$

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 $E^c = f^{-1}(E)$.

⁵This follows from the fact that the correspondence between the ideals of R and the ideals of R/I can be restricted to a bijection between $\text{Spec}(R)$ and $\text{Spec}(R/I)$.

1.2 Modules and Algebra

Let A be some ring. By an **A -module**, we mean an abelian group M together with a A -scalar multiplication. Given another A -module N , we use the notation $\text{Hom}(M, N)$ to denote the space of **A -module homomorphism** from M to N . It is clear that the obvious assignment of A -scalar multiplication and addition makes $\text{Hom}(M, N)$ a A -module.

Let M be an A -module, and let N be a subset of M . We say N is a **A -submodule** if N forms an additive subgroup and is closed under A -scalar multiplication. Just like how ideals is proved to always be the kernel of some ring homomorphism, to see submodules is always the kernel of some A -module homomorphism, we simply construct the **quotient module** M/N , and get the quotient map $\pi : M \rightarrow M/N$ that is a A -module homomorphism with kernel N , and get also the bijection

$$A\text{-submodule } S \text{ of } M \text{ that contains } N \mapsto \{[x] \in M/N : x \in S\}$$

between the collection of the A -submodules of M that contains N and the collection of the A -submodule of M/N . This is called the **correspondence theorem** for modules.

Again similar to the other algebraic structure, we have the **third isomorphism theorem** for modules. Let $N \subseteq M \subseteq L$ be three modules. It is obvious that M/N is a subset of L/N , and moreover, M/N forms a submodule of L/N . We have an isomorphism $\phi : (L/N)/(M/N) \rightarrow L/M$ defined by $(l+N)/(M/N) \mapsto l+M$. To simplify matters, from now on we use the term "module" in place of " A -module" until the end of this section.

Let $\{M_i : i \in I\}$ be a collection of 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 E of M , clearly its **span**, the set of finite sum $\sum rx$ where $x \in E$, forms a submodule. Interestingly, depending on the view one wish to take, there are multiple common notation for spans of E . To view modules as generalization of vector spaces, one may write $\text{span}(E)$, to view module as generalizations of rings, one may write $\langle E \rangle$, and to adapt the algebraic convention, one may also write $\sum_{x \in E} Ax$.

We say M is **finitely generated** if M can be spanned by some finite set $\{x_1, \dots, x_n\} \subseteq M$. Clearly, $(a_1, \dots, a_n) \mapsto \sum a_i x_i$ forms a surjective homomorphism from A^n to M , which implies M is isomorphic to some quotient of A^n . This behavior, albeit seems unimportant for now, will later prove to be useful for it guarantees that finitely generated module over rings of some certain properties carry the same property ⁶. 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 $an \triangleq f(a)n$.

Theorem 1.2.1. (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.

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 . ■

By the **Jacobson radical** $\text{Jacob}(A)$ of A , we mean the intersection of all maximal ideals of A . Given an ideal \mathfrak{a} of A , some module M and some submodule N of M , the **product $\mathfrak{a}N$ of the submodule N by the ideal \mathfrak{a}** is the submodule of M consisting of finite sum $\sum a_i x_i$ where $a_i \in \mathfrak{a}$ and $x_i \in N$. We may now state **Nakayama's Lemma**.

Lemma 1.2.2. (Nakayama) Let M be a finitely generated A -module, and \mathfrak{a} an ideal of A contained by the Jacobson radical of A . If $\mathfrak{a}M = M$, 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

$$(1 - a_n)u_n = a_1 u_1 + \dots + a_{n-1} u_{n-1} \quad (1.3)$$

We know that $1 - a_n$ must be a unit, otherwise by Zorn's Lemma⁷ 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 1.3**, u_n can be generated by $\{u_1, \dots, u_{n-1}\}$, a contradiction to the minimality of $\{u_1, \dots, u_n\}$. ■

There are multiple ways to give definition to the term **algebra B over ring A** , and the easiest way is to say we have a ring homomorphism $A \xrightarrow{f} B$, which induce the scalar product:

$$a(b) \triangleq f(a)b$$

⁶For example, this shows that finitely generated module over Noetherian ring is Noetherian. See **Theorem 1.6.5**

⁷Note that union of proper ideals is always proper because otherwise one of them would have contain 1.

Let B be an A -algebra. Because there are three structures on B , one shall be careful when one says " B is finitely generated," since B can be finitely generated as a ring, as an A -module, or even as an A -algebra. If we say B is **finitely generated as an A -algebra**, we mean that there exists some $b_1, \dots, b_n \in B$ such that $B = (f(A))[b_1, \dots, b_n]$.

1.3 Localization and local ring

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 $A \xrightarrow{f} B$ satisfies the universal property of localization of A by S . A routine check shows that for 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.⁸ 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 , and, 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 $A \rightarrow S^{-1}A$ maps T into $(S^{-1}A)^\times$. This by universal property implies the existence and uniqueness of a ring homomorphism from

⁸Just like the universal properties for other mathematical objects, one may 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.

$T^{-1}A$ to $S^{-1}A$ that forms a commutative triangle with the two canonical ring homomorphisms. This ring homomorphism has the obvious action, and will be how we are going to identify $T^{-1}A$ as a subring of $S^{-1}A$ ⁹. 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 composed $A \hookrightarrow B \longrightarrow S^{-1}B$, 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.

⁹One 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 structure¹⁰, 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 given

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

Clearly, we have

$$S^{-1}(g \circ f) = S^{-1}g \circ S^{-1}f$$

In other words, localization forms a functor.

Theorem 1.3.1. (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.

¹⁰It is the obvious one.

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 $\frac{m}{s} = S^{-1}f(\frac{m'}{st})$. ■

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 ¹¹.

A nonzero ring is said to be a **local ring** if it has only one maximal ideal, if and only if its set of non-units form an ideal, or that if and only if it is the localization of some ring B at some prime ideal \mathfrak{p} of B ¹², thus the name "local 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 $k \triangleq A/\mathfrak{m}$.

¹¹Because if $s \in A$ is not in any maximal ideal of A , then s must be a unit.

¹²If A is local, then it is the localization of itself at its unique maximal ideal. If $A = B_{\mathfrak{p}}$, then the set of non-units $\{\frac{p}{s} \in B_{\mathfrak{p}} : p \in \mathfrak{p}\}$ is clearly the only maximal ideal of A .

1.4 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 1.4.1. (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 following equivalent definitions of integral dependence, which are the keys for defining integral closure.

Theorem 1.4.2. (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.

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

Corollary 1.4.3. (Definition of Integral Closure) If A is a subring of B , then the set of elements of B which are integral over A forms a subring of B containing A .

Proof. Let $x, y \in B$ be integral over A . We are required to prove $x \pm y, xy$ are also integral over A . The first step of the proof is to observe that $A[x + y], A[x - y], A[xy]$ are both contained by the ring $A[x, y]$, which is a subring of C . Therefore, we only have to show $A[x, y]$ as an A -module is finitely generated.

Now, note that $A[x, y] = (A[x])[y]$. Clearly y is integral over $A[x]$, so we know $A[x, y] = (A[x])[y]$ is a finitely generated $A[x]$ -module. Moreover, because x is integral over A , we also know $A[x]$ is a finitely generated A -module. Let $A[x, y]$ as an $A[x]$ -module be generated by $\{z_1, \dots, z_n\}$, and let $A[x]$ as an A -module be generated by $\{v_1, \dots, v_k\}$. It is easy to check that, indeed, $A[x, y]$ as an A -module is generated by $\{z_i v_j \in A[x, y] : 1 \leq i \leq n, 1 \leq j \leq k\}$. ■

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

Let A be a subring of B . Because of **Corollary 1.4.3**, when we talk about the **integral closure of A in B** , the set of elements of B integral over A , we know we are indeed talking about a ring. If A itself is the integral closure of itself in B , we say A is **integrally closed in B** .

For the proof of **Corollary 1.4.4**, note that induction and argument similar to the second paragraph of the proof of **Corollary 1.4.3** shows that if x_1, \dots, x_n are all integral over A , then $A[x_1, \dots, x_n]$ as an A -module is finitely generated.

Corollary 1.4.4. (Transitivity of Integral Closure) Let B be a subring of C , and A a subring of B . If A is integrally closed in B and B is integrally closed in C , then A is integrally closed in C .

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

$$x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0, \quad \text{for some } b_0, \dots, b_{n-1} \in B$$

By **Theorem 1.4.2**, we are only required to show $A[b_0, \dots, b_{n-1}, x]$ as an A -module is finitely generated. Clearly, x is integral over the subring $A[b_0, \dots, b_{n-1}]$, so by **Theorem 1.4.2**, we

know $A[b_0, \dots, b_{n-1}, x]$ as an $A[b_0, \dots, b_{n-1}]$ -module is finitely generated. The proof then follows from noting $A[b_0, \dots, b_{n-1}]$ is finitely generated as an A -module since all b_0, \dots, b_{n-1} are all integral over A . ■

An integral domain is said to be an **integrally closed domain** if it is integrally closed in its field of fraction.

1.5 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 1.5.1. (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 1.5.2. (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 1.5.3. (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 1.5.4. (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.

1.6 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 1.6.1. (Equivalent Definition of Noetherian) 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 1.6.2](#) in [theorem 2.6.1](#).

Corollary 1.6.2. (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 1.6.3. (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 1.6.2](#). (\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. \blacksquare

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. \blacksquare

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

Proposition 1.6.4. (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. \blacksquare

Theorem 1.6.5. (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 1.1.1](#). The proof is nontrivial.

Proof. For (i), just apply **Proposition 1.6.4** inductively to

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

And for (ii), just apply **Proposition 1.6.4** 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 1.6.6. (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 1.6.5**. ■

1.7 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 1.7.1. (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

$$N \subset M \implies l(N) < l(M) \quad (1.4)$$

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 1.4**.

Now, let $M'_0 \subset \cdots \subset M'_r$ be some composition series of M . The proof then follows from using **statement 1.4** to deduce

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

■

Because of **Theorem 1.7.1**, 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 1.7.2. (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 1.7.3. (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 1.6.4](#), 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 1.6.5](#) 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 1.7.2](#) 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}

1.8 Tensor product for modules

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**¹⁶, 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 $\bar{f}(\sum r(x_1, \dots, x_n)) \triangleq \sum rf(x_1, \dots, x_n)$, 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.

¹⁶Elements 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

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

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 $\frac{a}{s} = \frac{as' s''}{ss' s''}$ and $as' s'' \in \sqrt{I}$ 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 Q is **primary** if for each $xy \in Q$, either $x \in Q$ or $y^n \in Q$ for some $n > 0$. Equivalently, a proper ideal I is primary if and only if every zero-divisors in A/Q is nilpotent. Clearly, the radical $P = \sqrt{Q}$ of a primary ideal Q is prime. In such case, we say Q is **P -primary**. A **primary decomposition** of an ideal I is an expression of I as a finite intersection of primary ideals

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

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

$$\bigcap_{j \neq i} Q_j \not\subseteq Q_i \text{ for all } i.$$

An ideal I is said to be **decomposable** if there exists some primary decomposition of I . Because finite intersection of P -primary ideals is again P -primary, every decomposable ideal has an irredundant primary decomposition.

Theorem 2.2.1. (First uniqueness theorem for irredundant primary decomposition) Given some irredundant primary decomposition $I = \bigcap_{i=1}^n Q_i$, we have

$$\left\{ \sqrt{Q_i} : 1 \leq i \leq n \right\} = \text{Spec}(R) \cap \left\{ \sqrt{(I : x)} \subseteq R : x \in R \right\} \quad (2.1)$$

Proof. Before showing that both sides of [equation 2.1](#) are subsets of each other, we first make the following observation. For all $x \in R$, clearly

$$(I : x) = \left(\bigcap Q_i : x \right) = \bigcap (Q_i : x)$$

Therefore,

$$\sqrt{(I : x)} = \bigcap \sqrt{(Q_i : x)} = \bigcap_{k: x \notin Q_k} \sqrt{Q_k} \quad (2.2)$$

where the last equality is justified by

$$x \in Q_i \implies (Q_i : x) = R, \quad \text{and } x \notin Q_i \implies \sqrt{(Q_i : x)} = \sqrt{Q_i}$$

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 $x \in R$ such that x belongs to all Q_j except Q_i . This x by [equation 2.2](#) must satisfies

$$\sqrt{Q_i} = \sqrt{(I : x)}$$

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

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

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 2.2.2. (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 2.2.3. (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 2.2.2](#) 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 2.2.2](#) 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 1.7.3](#) 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^1 , 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 1.6.2](#), 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 1.7.3](#) 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. ■

¹Otherwise 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 Lemma²](#), $\mathfrak{m} = 0$, 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 Lemma³](#) 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.⁴ [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. ■

²Because A is [Noetherian](#), we know \mathfrak{m} is finitely generated.

³ $\mathfrak{m}/\langle x \rangle$ is finitely generated because A is [Noetherian](#).

⁴If $\mathfrak{a} = A$, then $\mathfrak{a} = \langle 1 \rangle$.

2.5 Valuation Rings

Let K be a field and D a subring of K . If for all $x \in K$ either $x \in D$ or $x^{-1} \in D$, then the mapping $F \longrightarrow \text{Frac}(D)$ 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 field isomorphism. Because of this identification, for each integral domain D , it make sense to say D is a **valuation ring of field K** if

$$x \in \text{Frac}(D) \implies x \in D \text{ or } x^{-1} \in D \quad (2.4)$$

since if we replace $\text{Frac}(D)$ with K in [Equation 2.4](#), 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 $\nu(x) \neq \nu(y)$.

Theorem 2.5.1. (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 $D = \{x \in \text{Frac}(D) : \nu(x) \geq 0 \in \Gamma\}$. ■

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 2.5.2. (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 $\nu^{-1}(0)$.⁵ 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:

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

⁵Because $0 = \nu(1) = \nu(x) + \nu(x^{-1})$ 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 $\nu(x) = 0 \implies \nu(x^{-1}) = 0 \implies x^{-1} \in D$.

2.6 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

$$\mathfrak{a}_k = \{x \in D : \nu(x) \geq pk\} = \langle x^k \rangle \text{ for any } \nu(x) = p \triangleq \min \{\nu(d) \in \mathbb{N} : d^{-1} \notin D\} \quad (2.5)$$

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

Theorem 2.6.1. (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 1.6.2**, 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 1.6.5](#), 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 $\text{Krudim}(D) = 1$.

2.7 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 2.7.1. (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 2.7.2. (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 2.7.1**, 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 2.7.1**, 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. ■

2.8 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 2.8.1. (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 1.1](#) and [Equation 1.2](#)

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 2.8.2. (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.

2.9 Dedekind domain

Theorem 2.9.1. (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 2.5, 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 2.6.1 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 2.8.1 $1 \in \mathfrak{m}^{-1}$.

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 Lemma¹⁶ 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 2.9.2. (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 1.6.1. 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 2.9.1**, 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

Great Theorems like a bridge

3.1 Hilbert's Nullstellensatz and basis theorem

Theorem 3.1.1. (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

$$X = \left(X \cap \langle 1, x, \dots, x^{r-1} \rangle \right) + X' \quad (3.1)$$

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 3.1](#). 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 3.1.2. (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 3.1.3. (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:

$$k[x_1, \dots, x_n] \xrightarrow{\text{ring quotient}} B \xrightarrow{\text{localization}} C \xrightarrow{\text{ring quotient}} C_{/\mathfrak{m}} \quad (3.2)$$

We see that by Hilbert Basis Theorem, theorem 1.6.5, 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 3.2. Letting $t \triangleq (t_1, \dots, t_n) \in k^n$, it is easy to check¹ by direct computation that diagram 3.2 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 3.2 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 $k[x_1, \dots, x_n] = \langle x_1, \dots, x_n \rangle$.

3.2 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 3.2.1. (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 1.2.1²** that indeed $B[x_1, \dots, x_n]$ is finitely generated as a B -module. ■

Corollary 3.2.2. (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 3.2.1**. ■

Theorem 3.2.3. (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 $\text{trdeg}_k A$.

Chapter 4

Variety

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 .

Equivalent Definition 4.1.1. (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.

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. ■

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 . From this point of view, clearly, if $Y \subseteq X$ is irreducible, then so is \overline{Y} . By Zorn's Lemma¹, every $x \in X$ has

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 .

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.

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 4.1.2. (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: $E_1 \subset E_1 \cup E_2 \subset E_1 \cup E_2 \cup E_3 \subset \cdots$, 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 stop permanently at some point. ■

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

Theorem 4.1.3. (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

$$V = V_1 \cup \cdots \cup V_m \tag{4.1}$$

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

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

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 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 $\emptyset = Z_0 \subset Z_1 \subset \dots \subset Z_n$ 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

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.

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 the notation \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 notation $V(S) = \{a \in \mathbb{A}^n : F(a) = 0 \text{ for all } F \in S\}$ to denote its **zero set (locus)**, 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 locus 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. Clearly, we have

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

Already, at this early stage, we have the prime-irreducibility correspondence:

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

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

Proof. (\implies): Assume $fg \in I(X)$ and $f, g \notin I(X)$ for a contradiction. Because fg vanishes on X , we have $X = (X \cap V(f)) \cup (X \cap V(g))$. Because neither f nor g vanish on X , we see that $X \cap V(f) \neq X \neq X \cap V(g)$, a contradiction.

(\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 $f \in I(V_1) - I(X)$ that doesn't vanish on the whole 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. ■

Corollary 4.2.2. (Irreducible criteria in affine spaces) For all $X \subseteq \mathbb{A}^n$,

$$X \text{ is irreducible} \iff \overline{X} \text{ is irreducible}$$

Proof. If X is irreducible, then $I(\overline{X}) = I(X)$ is prime. If \overline{X} is irreducible, then $I(X) = I(\overline{X})$ is 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 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:

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 $\bigcap V(S_\alpha) = V(\bigcup S_\alpha)$

⁷Given descending chain of closed subset $X_0 \supset X_1 \supset \dots \supset X_m$ of \mathbb{A}^n , we must have $I(X_0) \subset I(X_1) \subset \dots \subset I(X_m)$ 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**.

Theorem 4.2.3. (Polynomial Identity Principal) Let k be an infinite field and $F \in k[x_1, \dots, x_n]$. If $F(\mathbf{a}) = 0$ for all $\mathbf{a} \in \mathbb{A}^n$, then $F = 0$.

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

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

Premise $F(\mathbf{a}) = 0, \forall \mathbf{a} \in \mathbb{A}^n$ and base case together implies that $G_i(\mathbf{x}) = 0$ for all i and $\mathbf{x} \in \mathbb{A}^{n-1}$, which by inductive hypothesis implies $G_i = 0 \in k[x_1, \dots, x_{n-1}]$ for all i . ■

Corollary 4.2.4. (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. Assume for a contradiction that $\mathbb{A}^n = V(f_1, \dots, f_r) \cup V(g_1, \dots, g_m)$ where the two closed set are both proper subset of \mathbb{A}^n . Clearly $f_1 \cdots f_r g_1 \cdots g_m$ vanish identically 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, a contradiction. ■

Most of the time we require k to be closed. In such case, we call irreducible closed sets of \mathbb{A}^n **affine varieties**, and we have the powerful **Nullstellensatz**:

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

As **Theorem 4.2.1** 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 $\text{Max}(k[x_1, \dots, x_n])$ ⁹.

⁹Using **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

Given some ring A and monoid M , by a **M -grading on A** , we mean a collection $(A_m)_{m \in M}$ of subgroup of the additive group of A such that $A = \bigoplus A_m$ ¹⁰ and $A_m A_n \subseteq A_{m+n}$ ¹¹ for all $m, n \in M$. Fix $a \in A$. If $a = a_{m_1} + \cdots + a_{m_r}$ for $a_{m_i} \in A_{m_i}$, we say a_{m_i} are the **homogeneous components of a** , and if $r = 1$ 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.

We say an ideal $I \subseteq A$ is **homogeneous** if I have a set of generators that are all homogeneous, or equivalently, if $I = \bigoplus I \cap A_n$. Note that the sum, product, and intersection of homogeneous ideals are homogeneous. Clearly, if $M = \mathbb{Z}$ or \mathbb{Z}_0^+ , then A_0 forms a subring of A ¹²; A_i all form obvious A_0 -modules; and radical of homogeneous ideal remain homogeneous¹³.

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 4.3.1. (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 $a_1 s_2 u = a_2 s_1 u$ for some $u \in S$. By definition and premise, a_1, s_1, s_2 , and u are all homogeneous, which with $a_1 s_2 u = a_2 s_1 u$ 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

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

¹⁰The direct sum is a direct sum of groups.

¹¹You may interpret $A_m A_n$ as $\{a_m a_n \in A : a_m \in A_m, a_n \in A_n\}$ here.

¹²To see $1 \in A_0$, consider the highest graded component of 1 and $1 = 1 \cdot 1$.

¹³If $(x_1 + \cdots + x_r)^l \in I$ 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 $x_1 + \cdots + x_{r-1} \in \sqrt{I}$.

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

$$\frac{a}{s} = \frac{a_0 s_1 \cdots s_n + \cdots + a_n s_0 \cdots s_{n-1}}{s_0 \cdots s_n}$$

We know that either

$$\frac{a_0 s_1 \cdots s_n + \cdots + a_n s_0 \cdots s_{n-1}}{s_0 \cdots s_n} = 0$$

or $(a_0 s_1 \cdots s_n + \cdots + a_n s_0 \cdots s_{n-1})$ homogeneous with

$$\deg(a) + \deg(s_0 \cdots s_n) = \deg(a_0 s_1 \cdots s_n + \cdots + a_n s_0 \cdots s_{n-1}) + \deg(s).$$

Assume for a contradiction that $a_0 s_1 \cdots s_n + \cdots + a_n s_0 \cdots s_{n-1}$ is homogeneous. WLOG, we have

$$\deg(a) + \deg(s_0 \cdots s_n) = \deg(a_0 s_1 \cdots s_n) + \deg(s).$$

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 4.3.1](#). Clearly $A_{(\mathfrak{p})}$ is also a local ring with maximal ideal $\{a/s \in A_{(\mathfrak{p})} : a \in \mathfrak{p}\}$ ¹⁴. 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 4.3.2. (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

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

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 4.3.1](#). 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

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

¹⁴This set is clearly the set of non units of $A_{(\mathfrak{p})}$, and it clearly forms an ideal of $A_{(\mathfrak{p})}$

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 4.3.2](#).

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}_k^n , or \mathbb{P}^n when k is understood, to represent the set of equivalence class of k^{n+1} .

Clearly, when we give the polynomial ring $k[x_0, \dots, x_n]$ the obvious grading, a polynomial $f \in k[x_0, \dots, x_n]$ is homogeneous in the graded sense if and only if it is homogeneous in the usual sense¹⁵. Suppose $f \in k[x_0, \dots, x_n]$. 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. Trivially, for each algebraic $V \subseteq \mathbb{P}^n$, the **defining ideal of V** , the ideal generated by homogeneous $f \in k[x_0, \dots, x_n]$ that vanishes on V , is homogeneous, and

¹⁵i.e., every term has the same degree.

moreover, contains only polynomials that "vanishes on V in the obvious sense".

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. Note that we define the notions **projective variety** and **dimension** similar to before.

Theorem 4.3.3. (Standard topological embedding of \mathbb{A}^n into \mathbb{P}^n) Let k be a field¹⁶, and $U \triangleq \mathbb{P}^n - V(x_0)$ ¹⁷. The map $\varphi : U \rightarrow \mathbb{A}^n$

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

is a well-defined homeomorphism.

Proof. It is routine to check φ is well-defined and bijective. We now prove it is indeed bicontinuous. Let S be the set of homogeneous elements of $k[x_0, \dots, x_n]$. Clearly, we may well-define mapping $\alpha : S \rightarrow k[x_1, \dots, x_n], \beta : k[x_1, \dots, x_n] \rightarrow S$ ¹⁸ by

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

Now, 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 \overline{Y} . To see $\varphi(Y)$ is closed, just check $\varphi(Y) = V(\alpha(T))$. Conversely, given closed $W \subseteq \mathbb{A}^n$, one have $\varphi^{-1}(W) = V(\beta(I(W))) \cap U$ ¹⁹. ■

¹⁶It needs not to be algebraically closed.

¹⁷Clearly $x_0 \in k[x_0, \dots, x_n]$ is homogeneous.

¹⁸The setting of α and β are standard. Respectively, they are called **dehomogenization** and **homogenization**. Their actions are actually easy to memorize. Homogenization send $y - x^2$ to $wy - x^2$ and send $z - x^3$ to $zw^2 - x^3$.

¹⁹You will need the fact $V(I(W)) = W$ in the proof of this equality, which holds true because W is closed.

4.4 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 , equivalently, we can define X to be a quasi variety if and only if X is open in \overline{X} ²⁰. One key property for quasi variety X is that, their closed sets are always intersection of algebraic set and X , since

$$E \stackrel{\text{closed}}{\subseteq} X \subseteq V \stackrel{\text{closed}}{\subseteq} (\mathbb{A}^n \text{ or } \mathbb{P}^n) \implies E = \text{cl}_V(E) \cap X$$

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 . Given some quasi projective variety $X \subseteq \mathbb{P}^n$ and $f : X \rightarrow k$, in the projective setting we say f is **regular at** $p \in X$ if there exists $U \subseteq X$ containing p and exist 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 , and we denote the **ring of regular function on** X by $\mathcal{O}(X)$.²¹

Theorem 4.4.1. (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.

Proof. Because every closed set in \mathbb{A}^1 is either finite or the whole space, 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 coherent²² 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 $U_i \cap f^{-1}(a) = V(g - ah) \cap U_i$. ■

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

$$(U, f) \sim (O, g) \iff f = g \text{ on } U \cap O \quad (4.3)$$

²⁰Because we will always have $\overline{X} \subseteq V$

²¹It is IMPORTANT to deduce that regular functions indeed forms a ring here, since it is impossible to later check transitivity of **equivalence 4.3** 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.

²²You 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 $X - Z = \bigcup (U_i - Z)$.

²³to form the ring $\mathcal{O}_{p,X}$ of **germs**²⁴ of regular functions on X near p and the **function field** $K(X)$ of X .

Let $(U, f) \in K(X)$. If $p \in U$ and f doesn't vanish at p , then f^{-1} is well-defined and regular on some smaller neighborhood of p . This implies that indeed $K(X)$ is a field, and that 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 colloquial convention of calling $\mathcal{O}_{p,X}$ the **local ring of p on X** ²⁵. Clearly, the obvious mappings of $\mathcal{O}(X) \longrightarrow \mathcal{O}_{p,X} \longrightarrow K(X)$ are well-defined injective ring homomorphism, and they will be how we treat one as subset of another.

Let X, Y be two quasi varieties. We say $\varphi : X \rightarrow Y$ is a **quasi variety morphism** if φ is continuous and for every open $U \subseteq Y$ and regular $f : U \rightarrow k$, the function $f \circ \varphi : \varphi^{-1}(U) \rightarrow k$ is regular. 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.²⁶ Clearly, if $\varphi : X \rightarrow Y$ is a quasi variety isomorphism, then $\mathcal{O}(X)$ and $\mathcal{O}(Y)$ as ring are isomorphic; for each $p \in X$, $\mathcal{O}_{p,X}$ and $\mathcal{O}_{\varphi(p),Y}$ as ring are isomorphic; and $K(X)$ and $K(Y)$ as ring are isomorphic. Because of such, we often say $\mathcal{O}(X)$, $\mathcal{O}_{p,X}$, and $K(X)$ are **invariant up to isomorphisms**.

In fact, given quasi variety mapping φ whose target is affine, there is an if and only if test for whether φ is a quasi variety morphism.

Theorem 4.4.2. (If and only if test for quasi variety mapping whose target is affine) Given quasi variety mapping $\varphi : X \rightarrow Y \subseteq \mathbb{A}^n$,

φ is a quasi variety morphism. $\iff x_i \circ \varphi : X \rightarrow k$ 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 regular $(U \subseteq Y, g : U \rightarrow k)$ 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 $O \subseteq U$

²³As noted before, to check transitivity, you must consider the regular function $f - h$.

²⁴You may Google what does **germ** means. It is generic.

²⁵Recall that if the set of non-units forms an ideal, then the ring is local.

²⁶One may check that the standard topological embedding of $\varphi : \mathbb{A}^n \rightarrow \mathbb{P}^n$ in **Theorem 4.3.3** is a quasi variety isomorphism.

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 where 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 $\deg(f_1 f_4) = \deg(f_2 f_3)$ if X projective. We have shown that indeed $g \circ \varphi$ is regular at p . ■

Given an affine quasi variety $X \subseteq \mathbb{A}^n$, we use notation $\Gamma(X)$ to denote its **coordinate ring** $k[x_1, \dots, x_n]/I(X)$, which is clearly isomorphic to the ring of function $f : X \rightarrow k$ such that $f = F|_X$ for some $F \in k[x_1, \dots, x_n]$ ²⁷. From the second point of view, immediately we see that coordinate ring of affine quasi variety is in fact an integral domain²⁸. Later we will see more usage of the realization of $\Gamma(Y)$ as ring of polynomials function in the proof of [Theorem 4.4.3](#).

Theorem 4.4.3. (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

²⁷We call these functions **polynomial functions**.

²⁸If $FG = 0$ on $X \subseteq Y \subseteq \mathbb{A}^n$ where Y is a variety, then because Y is irreducible, one of $F^{-1}(0) \cap Y, G^{-1}(0) \cap Y$ must be whole Y .

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 mapping²⁹: $f/g \mapsto [(U, f/g)]$ where $f, g : X \rightarrow k$ are polynomial function and $U = \{x \in X : g(x) \neq 0\}$. Clearly β is an injective ring homomorphism³⁰. 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 homomorphism. It remains to prove α is surjective, which follows from checking the diagram:

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

³¹is 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 4.4.3**, one quickly encounters difficulties and will be forced

²⁹From β you can see that the done localization $\Gamma(X)_{\mathfrak{m}_p}$ is of geometrical nature, not algebraic.

³⁰Note 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 . ($\because Z \subseteq Y \subseteq X \implies \text{cl}_Z(Y) = \text{cl}_X(X) \cap Y$)

³¹The left isomorphism is explain in [this paragraph](#) of [Section 1.3](#), the bottom isomorphism is from (ii), and the right injective homomorphism is from [this paragraph](#) of this section.

to use isomorphism $\mathcal{O}(X) \cong \Gamma(X)$ ³².

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 4.4.3**, the ring isomorphism $\mathcal{O}(Y) \cong \Gamma(Y)$ is also a k -algebra isomorphism.

Theorem 4.4.4. (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 quasi variety morphism $X \rightarrow Y$ 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.

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 injective³³, 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 $h(F) = F(h(x_1), \dots, h(x_n))$ ³⁴. This by definition of ξ and ψ give us

$$h(F) = F(\xi_1, \dots, \xi_n) = F \circ \psi \quad (4.4)$$

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

Noticing that **Equation 4.4** also holds true for any $F \in \Gamma(Y)$ ³⁵ 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 4.4.2**. ■

Corollary 4.4.5. (Quasi 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

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

³²As the action of isomorphism α in **Theorem 4.4.3** suggest, one can really just write $\mathcal{O}(X) = \Gamma(X)$

³³A 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 $F(p_1) \neq F(p_2)$.

³⁴For 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.

³⁵Perhaps here it will be better to write $k[x_1, \dots, x_n]$ in place of $\Gamma(Y)$.

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 4.4.6. (Obvious grading of the quotient of graded ring) Given \mathbb{Z}_0^+ -graded ring A , homogeneous ideal $I \subseteq A$, and quotient ring $\pi : A \twoheadrightarrow A/I$, we have a well defined \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 4.4.6](#).

4.5 Category of Quasi Varieties

Fix n and m . In this section, we express elements of $\mathbb{P}^{(n+1)(m+1)-1}$ (non uniquely, of course) as matrices:

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

Similarly, we write the coordinate of $\mathbb{P}^{(n+1)(m+1)-1}$, the polynomial ring, as $k[z_{i,j}]$. 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 a projective variety to justify calling it an embedding. Consider

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

Theorem 4.5.1. (Image of Segre embedding is a projective variety) 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 $\alpha \in V(S)$. ■

From now on, if we treat $\mathbb{P}^n \times \mathbb{P}^m$ as a variety, we mean that we are identifying $\mathbb{P}^n \times \mathbb{P}^m$ as a subvariety of $\mathbb{P}^{(n+1)(m+1)-1}$ using the Segre embedding.

Theorem 4.5.2. (Projections are quasi varieties morphisms) Identifying $\mathbb{P}^n \times \mathbb{P}^m$ as a sub projective varieties of $\mathbb{P}^{(n+1)(m+1)-1}$ using Segre embedding, the projection $\pi : \mathbb{P}^n \times \mathbb{P}^m \rightarrow \mathbb{P}^n$ is a quasi variety morphism.

Proof. ■

Theorem 4.5.3. (Well-defined of product of projective quasi varieties: Irreducibility) Let $X \subseteq \mathbb{P}^n$ and $Y \subseteq \mathbb{P}^m$ be two quasi-projective varieties. Identifying $X \times Y$ as a subset of $\mathbb{P}^{(n+1)(m+1)-1}$ using Segre embedding, $X \times Y$ is irreducible.

Theorem 4.5.4. (Well-defined of product of affine quasi varieties: Irreducibility) Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be two quasi varieties. The Zariski topology on $X \times Y$ is irreducible.

4.6 Rational Map (Just started)

Theorem 4.6.1. (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. WLOG³⁶, let $Y \subseteq \mathbb{P}^n$. Consider $\varphi \times \psi : X \rightarrow \mathbb{P}^n \times \mathbb{P}^n$, where $\mathbb{P}^n \times \mathbb{P}^n$ is identified as a subvariety of \mathbb{P}^{2n} using **Segre Embedding**. ■

Let X and Y be two quasi varieties. Because of **Theorem 4.6.1**, we may well-define **rational map** $\varphi : X \dashrightarrow Y$ to be equivalence 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. Given a rational map $\varphi : X \dashrightarrow Y$, we say φ is **dominant** if for some and hence every³⁷ pair (U, φ_U) , the image of φ_U is dense in Y . Consider two dominant rational maps $X \xrightarrow{\varphi} Y \xrightarrow{\psi} Z$, and consider $(U, \varphi_U) \in \varphi$ and $(V, \psi_V) \in \psi$. Because $\varphi(U)$ is dense in Y , we know $\varphi_U^{-1}(V)$ is nonempty. Therefore, it make sense to talk about the composition $\psi \circ \varphi : X \dashrightarrow Z$ of the dominant rational maps, the equivalence class containing $(\varphi_U^{-1}(V), \psi \circ \varphi)$. It is trivial to check the composition is indeed well-defined. It is clear that composition of dominant rational maps is again dominant³⁸.

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 must be unique. Two quasi varieties are said to be **birational equivalent** if there exists a birational map between them.

Theorem 4.6.2. (Birational equivalence implies isomorphism of function field as k -algebra) Let X and Y be two quasi varieties.

$$X \text{ and } Y \text{ are birational equivalent} \implies K(X) \cong K(Y) \text{ as } k\text{-algebra.}$$

Proof. Let dominant rational $\varphi : X \dashrightarrow Y$ and $\psi : Y \dashrightarrow X$ be inverse to each other, consider $(U, \varphi_U) \in \varphi$ and $(V, \psi_V) \in \psi$, and consider $E \triangleq \varphi_U^{-1}(\psi_V^{-1}(U))$ and $F \triangleq \psi_V^{-1}(\varphi_U^{-1}(V))$.

³⁶As we have mentioned, one may check that the map $\mathbb{A}^n \rightarrow \mathbb{P}^n - \{x_0 = 0\}$ in **Theorem 4.3.3** is a quasi variety isomorphism. One can also check that given any quasi variety isomorphism $\varphi : Y \rightarrow Z$ and open $E \subseteq Y$, $\varphi(E)$ is open in Z and $\varphi|_E : E \rightarrow \varphi(E)$ forms a quasi variety isomorphism.

³⁷Let $U, V \subseteq X$ 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 $Y = \overline{\varphi(U)} = \overline{\varphi(\text{cl}_U(U \cap V))} \subseteq \overline{\varphi(U \cap V)} \subseteq \overline{\varphi(V)}$.

³⁸Let $W \subseteq Z$ be open. We are required to show W intersect with $\psi(V \cap \varphi(U))$. Because $\psi_V(V) \subseteq Z$ is 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.

Clearly, $E \subseteq U$ and $F \subseteq V$ are open, and a routine check shows that φ_E maps E isomorphically to F with inverse being ψ_F . A routine check now shows that $K(X) \rightarrow K(Y)$ defined by

$$[(T, f)] \longmapsto [(\psi_F^{-1}(T), f \circ \psi)]$$

and $K(Y) \rightarrow K(X)$ defined by

$$[(H, g)] \longmapsto [(\varphi_E^{-1}(H), g \circ \varphi)]$$

are two well-defined k -algebra homomorphism being inverse to each others³⁹. ■

Let $\varphi : X \dashrightarrow Y$ be a dominant rational map and $(U, \varphi_U) \in \varphi$. Let $(V, f) \in K(Y)$. Clearly, $\varphi_U^{-1}(V)$ is nonempty and open, and $f \circ \varphi_U$ is a regular function on $\varphi_U^{-1}(V)$. In other words, $(\varphi_U^{-1}(V), f \circ \varphi_U) \in K(X)$.

Verify this is

- (i) well-defined as a set map.
- (ii) a k -algebra homomorphism.

³⁹Therefore they are isomorphisms inverse to each other.

4.7 Dimension Theory (Planned)

X is a quasi variety iff X is irreducible and X is open in \overline{X} .
 X is irreducible iff \overline{X} is irreducible.

Chapter 5

Scheme

Given some ring R , we may give $\text{Spec}(R)$ its **Zariski topology** by defining $E \subseteq \text{Spec}(R)$ to be closed if and only if $E = \{J \in \text{Spec}(R) : I \subseteq J\}$ for some ordinary ideal $I \subseteq R$.

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.

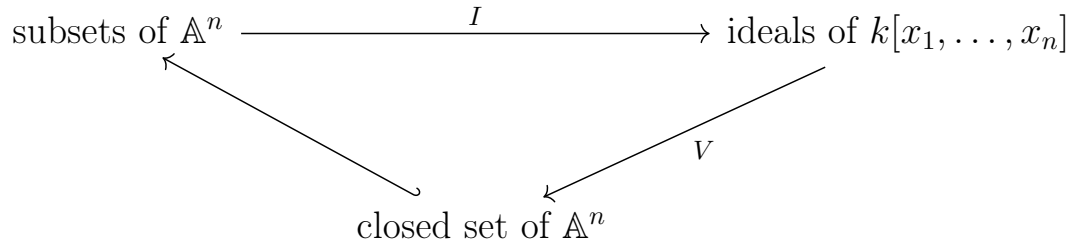
Proposition 6.6.8. () If k is an infinite field, and $F \in k[x_1, \dots, x_n]$ maps all $a \in \mathbb{A}^n$ to 0, then $F = 0$.

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.