Algebra toward Algebraic Geometry

No Cover Image

Use \coverimage{filename} to add an image

“”

Algebra toward Algebraic Geometry

Author: Tianle Yang

Email: loveandjustice@88.com

Homepage: https://www.tianleyang.com

Source code: github.com/MonkeyUnderMountain/TexTemplates

Version: 0.1.0

Last updated: August 27, 2025

Contents

1 Commutative Algebra **5**

1.1 Some fundamental Results . . . 5

1.1.1 Rings and modules . . . 5

1.1.2 Localization . . . 6

1.1.3 Chain conditions . . . 7

1.1.4 Nakayama's Lemma . . . 7

1.1.5 Nullstellensatz . . . 8

1.2 Associated prime ideals . . . 8

1.2.1 Associated prime ideals . . . 8

1.2.2 Primary decomposition . . . 10

1.3 Dimension and Depth . . . 11

1.3.1 Artinian Rings and Length of Modules . . . 12

1.3.2 DVR and Dedekind Domain . . . 14

1.3.3 Krull's Principal Ideal Theorem . . . 14

1.3.4 Cohen-Macaulay rings . . . 16

1.3.5 Regular rings . . . 17

1.4 Finite Algebra and Normality . . . 18

1.4.1 Finite algebra . . . 18

1.5 Smoothness . . . 21

1.5.1 Modules of differentials and derivations . . . 21

1.5.2 Applications to affine varieties . . . 25

1.6 Formal Completion . . . 28

1.6.1 Formal completion of rings and modules . . . 28

1.6.2 Complete local rings . . . 31

2 Homological Algebra **39**

2.1 Complexes and Homology . . . 39

2.2 Derived Functors . . . 39

2.2.1 Resolution . . . 39

2.3 Applications to Commutative Algebra . . . 40

2.3.1 Homological dimension 40
2.3.2 Depth and regularity by homological algebra 43

Chapter 1

Commutative Algebra

1.1 Some fundamental Results

Yang: To be completed

1.1.1 Rings and modules

In the appendix and all the note, the "ring" is always commutative and with identity. We denote by $\operatorname{Spec} A$ the set of prime ideals of a ring A. We denote by $\operatorname{mSpec} A$ the set of maximal ideals of A. Let $I \subset A$ be an ideal of A. We define

$$V(I) \coloneqq \{\mathfrak{p} \in \operatorname{Spec} A : I \subset \mathfrak{p}\}.$$

Let $\mathfrak{a}, \mathfrak{b}$ be ideals of A. We define

$$(\mathfrak{a} : \mathfrak{b}) \coloneqq \{a \in A : a\mathfrak{b} \subset \mathfrak{a}\}.$$

This is an ideal of A.

Let $\operatorname{rad}(A)$ be the Jacobian radical of A, i.e., the intersection of all maximal ideals of A. Let $\operatorname{nil}(A)$ be the nilradical of A, i.e., the ideal of A consisting of all nilpotent elements.

Proposition 1.1.1. Let A be a ring. Then we have

$$\operatorname{nil}(A) = \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}.$$

Proof. Yang: To be completed. □

Proposition 1.1.2. Let A be a ring, $\mathfrak{p}, \mathfrak{p}_i$ prime ideals of A and $\mathfrak{a}, \mathfrak{a}_i$ ideals of A.

(a) Suppose $\mathfrak{a} \subset \bigcup_{i=1}^n \mathfrak{p}_i$. Then there exists i such that $\mathfrak{a} \subset \mathfrak{p}_i$.

(b) Suppose $\bigcap_{i=1}^n \mathfrak{a}_i \subset \mathfrak{p}$. Then there exists i such that $\mathfrak{a}_i \subset \mathfrak{p}$.

Proof. Yang: To be completed. □

Let M be an A-module. We say that M is *finite* if there exists an exact sequence

$$A^n \to M \to 0.$$

We say that M is *finite presented* if there exists an exact sequence

$$A^m \to A^n \to M \to 0.$$

If A is a noetherian ring, then every finite A-module is finite presented.

Definition 1.1.3. Let A be a ring and M an A-module. The *support* of M is defined as

$$\operatorname{Supp} M \coloneqq \{\mathfrak{p} \in \operatorname{Spec} A : M_{\mathfrak{p}} \neq 0\}.$$

The *annihilator* of M is defined as

$$\operatorname{Ann} M \coloneqq \{a \in A : aM = 0\}.$$

This is an ideal of A.

Proposition 1.1.4. Let A be a ring and M a finite A-module. Then $\operatorname{Supp} M = V(\operatorname{Ann} M)$. In particular, $\operatorname{Supp} M$ is a closed subset of $\operatorname{Spec} A$.

Proof. Yang: To be completed. □

1.1.2 Localization

Definition 1.1.5. Let A be a ring and $S \subset A$ a multiplicative subset, i.e., $1 \in S$ and $s_1, s_2 \in S$ implies $s_1 s_2 \in S$. Let M be an A-module. The *localization* of M at S is defined as

$$S^{-1}M \coloneqq M \times S / \sim,$$

where $(m, s) \sim (n, t)$ if there exists $u \in S$ such that $u(tm - sn) = 0$. We denote the equivalence class of (m, s) by $\frac{m}{s}$ or m/s.
The localization $S^{-1}A$ is still a ring and hence an A-algebra. The localization $S^{-1}M$ is an $S^{-1}A$-module. If $M = B$ is an A-algebra, then $S^{-1}B$ is an $S^{-1}A$-algebra.

Example 1.1.6. Let A be a ring, $\mathfrak{p}$ a prime ideal of A and M an A-module. Then $S = A \setminus \mathfrak{p}$ is a multiplicative subset. The localization $S^{-1}M$ is denoted by $M_{\mathfrak{p}}$ and called the localization of M at $\mathfrak{p}$.

Let $f \in A$ be an element. Then $S = \{f^n : n \geq 0\}$ is a multiplicative subset. The localization $S^{-1}M$ is denoted by $M[1/f]$.

Proposition 1.1.7. The natural map $A \to S^{-1}A$ is injective if and only if S contains no zero divisors.

Proposition 1.1.8. Let A be a ring, $S \subset A$ a multiplicative subset and M an A-module. Then we have a natural isomorphism of $S^{-1}A$-modules

$$S^{-1}M \cong M \otimes_A S^{-1}A.$$

Proposition 1.1.9. The localization $S^{-1}A$ is a flat A-algebra.

1.1.3 Chain conditions

Definition 1.1.10. Let A be a ring. We say that A is *noetherian* (resp. *artinian*) if every ascending (resp. descending) chain of ideals of A stabilizes.

Proposition 1.1.11. Let A be a ring. The following are equivalent:

(a) A is noetherian.

(b) Every ideal of A is finitely generated.

(c) Every non-empty set of ideals of A has a maximal element (with respect to inclusion).

Proof. Yang: To be completed. □

Theorem 1.1.12 (Hilbert's Basis Theorem)**.** If A is a noetherian ring, then $A[x]$ is noetherian.

Proof. Yang: To be completed. □

Remark 1.1.13. By a similar argument replacing $\deg f$ by $\operatorname{ord} f$, we can show that if A is noetherian, then the formal power series ring $A[[x]]$ is also noetherian.

1.1.4 Nakayama's Lemma

Theorem 1.1.14 (Nakayama's Lemma)**.** Let A be a ring and $\mathfrak{M}$ be its Jacobi radical. Suppose M is a finitely generated A-module. If $\mathfrak{a}M = M$ for $\mathfrak{a} \subset \mathfrak{M}$, then $M = 0$.

Proof. Suppose M is generated by $x_1, \cdots, x_n$. Since $M = \mathfrak{a}M$, formally we have $(x_1, \cdots, x_n)^T = \Phi(x_1, \cdots, x_n)^T$ for $\Phi \in M_n(\mathfrak{a})$. Then $(\Phi - \mathrm{id})(x_1, \cdots, x_n)^T = 0$. Note that $\det(\Phi - \mathrm{id}) = 1 + a$ for $a \in \mathfrak{a} \subset \mathfrak{M}$. Then $\Phi - \mathrm{id}$ is invertible and then $M = 0$. □

The finiteness of M is crucial in Nakayama's Lemma. The followings are counterexamples when M is not finite.

Example 1.1.15. Let $\overline{\mathbb{Z}}$ be the ring of algebraic integers in $\overline{\mathbb{Q}}$. Choose a non-zero prime ideal $\mathfrak{p}$ of $\overline{\mathbb{Z}}$. Then we have that $\mathfrak{p}\overline{\mathbb{Z}}_{\mathfrak{p}} = \mathfrak{p}^2\overline{\mathbb{Z}}_{\mathfrak{p}}$. Indeed, if $a \in \mathfrak{p}\overline{\mathbb{Z}}_{\mathfrak{p}}$, let $b = \sqrt{a} \in \overline{\mathbb{Z}}_{\mathfrak{p}}$. Then $b^2 = a \in \mathfrak{p}\overline{\mathbb{Z}}_{\mathfrak{p}}$ and whence $b \in \mathfrak{p}\overline{\mathbb{Z}}_{\mathfrak{p}}$ since $\mathfrak{p}$ is prime. It follows that $a = b^2 \in \mathfrak{p}^2\overline{\mathbb{Z}}_{\mathfrak{p}}$.

Example 1.1.16. Let $A = \mathbf{k}[x]$ and $B = \mathbf{k}[t]$ with $t^2 = x$. Then B is a A-module. Let $\mathfrak{m} = (x-1) \subset A$ and $\mathfrak{n} = (t-1) \subset B$. Then $B_{\mathfrak{n}}$ is a $A_{\mathfrak{m}}$-module which is not finite. Note that $\mathfrak{m}B_{\mathfrak{n}} = (t^2-1)B_{\mathfrak{n}} = (t-1)(t+1)B_{\mathfrak{n}} = \mathfrak{n}B_{\mathfrak{n}}$. Then $B_{\mathfrak{n}} \otimes_A \kappa(\mathfrak{m}) = \mathbf{k}$ is generated by 1. However, $B_{\mathfrak{n}}$ is not generated by 1 as a $A_{\mathfrak{m}}$-module.

Proposition 1.1.17 (Geometric form of Nakayama's Lemma)**.** Let $X = \operatorname{Spec} A$ be an affine scheme, $x \in X$ a closed point and $\mathcal{F}$ a coherent sheaf on X. If $a_1, \cdots, a_k \in \mathcal{F}(X)$ generate $\mathcal{F}|_x = \mathcal{F} \otimes \kappa(x)$, then there is an open subset $U \subset X$ such that $a_i|_U$ generate $\mathcal{F}(U)$.

Proof. Yang: To be completed. ☐

Corollary 1.1.18. Let X be a scheme and $\mathcal{F}$ a coherent sheaf on X. Then the function $x \mapsto \dim_{\kappa(x)} \mathcal{F}|_x$ is upper semicontinuous.

Proof. Yang: To be completed. ☐

1.1.5 Nullstellensatz

Let $\mathbf{k}$ be a field and $\Bbbk$ be its algebraic closure.

Theorem 1.1.19 (Noether's Normalization Lemma)**.** Let A be a $\mathbf{k}$-algebra of finite type. Then there is an injection $\mathbf{k}[T_1, \cdots, T_d] \hookrightarrow A$ such that A is finite over $\mathbf{k}[T_1, \cdots, T_d]$.

Remark 1.1.20. Here A does not need to be integral. For example,

Theorem 1.1.21 (Hilbert's Nullstellensatz)**.** Let A be a $\mathbf{k}$-algebra of finite type.

(a) If $\mathfrak{m}$ is a maximal ideal of A, then $A/\mathfrak{m}$ is a finite extension of $\mathbf{k}$.

(b) Suppose that $\mathbf{k}$ is algebraically closed and $A = \mathbf{k}[x_1, \cdots, x_n]/\mathfrak{a}$. Then there is a bijection between the set of maximal ideals of A and the set $\{(a_1, \cdots, a_n) \in \mathbf{k}^n : f(a_1, \cdots, a_n) = 0, \forall f \in \mathfrak{a}\}$.

1.2 Associated prime ideals

1.2.1 Associated prime ideals

Definition 1.2.1 (Associated prime ideals)**.** Let A be a noetherian ring and M an A-module. The *associated prime ideals* of M are the prime ideals $\mathfrak{p}$ of form $\mathrm{Ann}(x)$ for some $x \in M$. The set of associated prime ideals of M is denoted by $\mathrm{Ass}(M)$.

Example 1.2.2. Let $A = \Bbbk[x, y]/(xy)$ and $M = A$. First we see that $(x) = \mathrm{Ann}\, y, (y) = \mathrm{Ann}\, x \in \mathrm{Ass}\, M$. Then we check other prime ideals. For (x, y), if $xf = yf = 0$, then $f \in (x) \cap (y) = (0)$. If $(x - a) = \mathrm{Ann}\, f$ for some f, note that $y \in (x - a)$ for $a \in \Bbbk^*$, then $f \in (x)$. Hence $f = 0$. Therefore $\mathrm{Ass}\, M = \{(x), (y)\}$.

Example 1.2.3. Let $A = \Bbbk[x, y]/(x^2, xy)$ and $M = A$. The underlying space of $\mathrm{Spec}\, A$ is the y-axis since $\sqrt{(x^2, xy)} = (x)$. First note that $(x) = \mathrm{Ann}\, y, (x, y) = \mathrm{Ann}\, x \in \mathrm{Ass}\, M$. For $(x, y - a)$ with $a \in \Bbbk^*$, easily see that $xf = (y - a)f = 0$ implies $f = 0$ since $A = \Bbbk \cdot x \bigoplus \Bbbk[y]$ as $\Bbbk$-vector space. Hence $\mathrm{Ass}\, M = \{(x), (x, y)\}$.

Lemma 1.2.4. Let A be a noetherian ring and M an A-module. Then the maximal element of the set

$$\{\operatorname{Ann} x : x \in M_{\mathfrak{p}}, x \neq 0\}$$

belongs to $\operatorname{Ass} M$.

Proof. We just need to show that such $\operatorname{Ann} x$ is prime. Otherwise, there exist $a, b \in A$ such that $ab \in \operatorname{Ann} x$ but $a, b \notin \operatorname{Ann} x$. It follows that $\operatorname{Ann} x \subsetneq \operatorname{Ann} ax$ since $b \in \operatorname{Ann} ax \setminus \operatorname{Ann} x$. This contradicts the maximality of $\operatorname{Ann} x$. $\square$

An element $a \in A$ is called a zero divisor for M if $M \to aM, m \mapsto am$ is not injective.

Corollary 1.2.5. Let A be a noetherian ring and M an A-module. Then

$$\{\text{zero divisors for } M\} = \bigcup_{\mathfrak{p} \in \operatorname{Ass} M} \mathfrak{p}.$$

Lemma 1.2.6. Let A be a noetherian ring and M an A-module. Then $\mathfrak{p} \in \operatorname{Ass}_A M$ iff $\mathfrak{p}A_{\mathfrak{p}} \in \operatorname{Ass}_{A_{\mathfrak{p}}} M_{\mathfrak{p}}$.

Proof. Suppose $\mathfrak{p}A_{\mathfrak{p}} \in \operatorname{Ass}_{A_{\mathfrak{p}}} M_{\mathfrak{p}}$. Let $\mathfrak{p}A_{\mathfrak{p}} = \operatorname{Ann} y_0/c$ with $y_0 \in M$ and $c \in A \setminus \mathfrak{p}$. For $a \in \operatorname{Ann} y_0$, $ay_0 = 0$. Then $a/1 \in \mathfrak{p}A_{\mathfrak{p}}$. It follows that $a \in \mathfrak{p}$. Hence $\operatorname{Ann} y_0 \subset \mathfrak{p}$.

Inductively, if $\operatorname{Ann} y_n \subsetneq \mathfrak{p}$, then there exists $b_n \in A \setminus \mathfrak{p}$ such that $y_{n+1} := b_n y_n$, $\operatorname{Ann} y_{n+1} \subset \mathfrak{p}$ and $\operatorname{Ann} y_n \subsetneq \operatorname{Ann} y_{n+1}$. To see this, choose $a_n \in \mathfrak{p} \setminus \operatorname{Ann} y_n$. Then $(a_n/1)y_n = 0$ since $a_n/1 \in \mathfrak{p}A_{\mathfrak{p}}$. By definition, there exist $b_n \in A \setminus \mathfrak{p}$ such that $a_n b_n y_n = 0$. This process must terminate since A is noetherian. Thus $\operatorname{Ann} y_n = \mathfrak{p}$ for some n. Hence $\mathfrak{p} \in \operatorname{Ass}_A M$.

Conversely, suppose $\mathfrak{p} = \operatorname{Ann} x \in \operatorname{Ass} M$. If $(a/s)(x/1) = 0 \in M_{\mathfrak{p}}$, there exist $t \in A \setminus \mathfrak{p}$ such that $tax = 0$. It follows that $ta \in \mathfrak{p}$ and then $(a/s) \in \mathfrak{p}A_{\mathfrak{p}}$. Hence $\mathfrak{p}A_{\mathfrak{p}} \in \operatorname{Ass}_{A_{\mathfrak{p}}} M_{\mathfrak{p}}$. $\square$

Proposition 1.2.7. We have $\operatorname{Ass} M \subset \operatorname{Supp} M$. Moreover, if $\mathfrak{p} \in \operatorname{Supp} M$ satisfies $V(\mathfrak{p})$ is an irreducible component of $\operatorname{Supp} M$, then $\mathfrak{p} \in \operatorname{Ass} M$.

Proof. For any $\mathfrak{p} = \operatorname{Ann} x \in \operatorname{Ass} M$, we have $A/\mathfrak{p} \cong A \cdot x \subset M$. Tensoring with $A_{\mathfrak{p}}$ gives $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \hookrightarrow M_{\mathfrak{p}}$ since $A_{\mathfrak{p}}$ is flat. Hence $M_{\mathfrak{p}} \neq 0$ and $\mathfrak{p} \in \operatorname{Supp} M$.

Now suppose $\mathfrak{p} \in \operatorname{Supp} M$ and $V(\mathfrak{p})$ is an irreducible component of $\operatorname{Supp} M$. First we show that $\mathfrak{p} \in \operatorname{Ass}_{A_{\mathfrak{p}}} M_{\mathfrak{p}}$. Let $x \in M_{\mathfrak{p}}$ such that $\operatorname{Ann} x$ is maximal in the set

$$\{\operatorname{Ann} x : x \in M_{\mathfrak{p}}, x \neq 0\}.$$

Then we claim that $\operatorname{Ann} x = \mathfrak{p}A_{\mathfrak{p}}$. First, $\operatorname{Ann} x$ is prime by Lemma 1.2.4. If $\operatorname{Ann} x \neq \mathfrak{p}$, then $V(\operatorname{Ann} x) \supset V(\mathfrak{p})$. This implies that $\operatorname{Ann} x \notin \operatorname{Supp} M_{\mathfrak{p}}$ since $\operatorname{Supp} M_{\mathfrak{p}} = \operatorname{Supp} M \cap \operatorname{Spec} A_{\mathfrak{p}}$. This is a contradiction. Thus $\mathfrak{p}A_{\mathfrak{p}} \in \operatorname{Ass}_{A_{\mathfrak{p}}} M_{\mathfrak{p}}$. By Lemma 1.2.6, we have $\mathfrak{p} \in \operatorname{Ass} M$. $\square$

Remark 1.2.8. The existence of irreducible component is guaranteed by Zorn's Lemma.

Definition 1.2.9. A prime ideal $\mathfrak{p} \in \operatorname{Ass} M$ is called *embedded* if $V(\mathfrak{p})$ is not an irreducible component of $\operatorname{Supp} M$.

Example 1.2.10. For $M = A = \Bbbk[x, y]/(x^2, xy)$, the origin (x, y) is an embedded point.

Proposition 1.2.11. If we have exact sequence $0 \to M_1 \to M_2 \to M_3$, then $\operatorname{Ass} M_2 \subset \operatorname{Ass} M_1 \cup \operatorname{Ass} M_3$.

Proof. Let $\mathfrak{p} = \operatorname{Ann} x \in \operatorname{Ass} M_2 \setminus \operatorname{Ass} M_1$. Then the image $[x]$ of x in M_3 is not equal to 0. We have that $\operatorname{Ann} x \subset \operatorname{Ann}[x]$. If $a \in \operatorname{Ann}[x] \setminus \operatorname{Ann} x$, then $ax \in M_1$. Since $\operatorname{Ann} x \subsetneq \operatorname{Ann} ax$, there is $b \in \operatorname{Ann} ax \setminus \operatorname{Ann} x$. However, it implies $ba \in \operatorname{Ann} x$, and then $a \in \operatorname{Ann} x$ since $\operatorname{Ann} x$ is prime, which is a contradiction. □

Corollary 1.2.12. If M is finitely generated, then the set $\operatorname{Ass} M$ is finite.

Proof. For $\mathfrak{p} = \operatorname{Ann} x \in \operatorname{Ass} M$, we know that the submodule M_1 generated by x is isomorphic to $A/\mathfrak{p}$. Inductively, we can choose M_n be the preimage of a submodule of M/M_{n-1} which is isomorphic to $A/\mathfrak{q}$ for some $\mathfrak{q} \in \operatorname{Ass} M/M_{n-1}$. We can take an ascending sequence $0 = M_0 \subset M_1 \subset \cdots \subset M_n \subset \cdots$ such that $M_i/M_{i-1} \cong A/\mathfrak{p}_i$ for some prime $\mathfrak{p}_i$. Since M is finitely generated, this is a finite sequence. Then the conclusion follows by Proposition 1.2.11. □

1.2.2 Primary decomposition

Definition 1.2.13. An A-module is called *co-primary* if $\operatorname{Ass} M$ has a single element. Let M be an A-module and $N \subset M$ a submodule. Then N is called *primary* if M/N is co-primary. If $\operatorname{Ass} M/N = \{\mathfrak{p}\}$, then N is called $\mathfrak{p}$-primary.

Remark 1.2.14. This definition coincide with primary ideals in the case $M = A$. Recall an ideal $\mathfrak{q} \subset A$ is called *primary* if $\forall ab \in \mathfrak{p}$, $a \notin \mathfrak{q}$ implies $b^n \in \mathfrak{q}$ for some n.

Let $\mathfrak{q}$ be a $\mathfrak{q}$-primary ideal. Since $\operatorname{Supp} A/\mathfrak{q} = \{\mathfrak{p}\}$, $\mathfrak{p} \in \operatorname{Ass} A/\mathfrak{q}$. Suppose $\operatorname{Ann}[a] \in \operatorname{Ass} A/\mathfrak{q}$. Then $\mathfrak{p} \subset \operatorname{Ann}[a]$ since $V(\mathfrak{p}) = \operatorname{Supp} A/\mathfrak{q}$. If $b \in \operatorname{Ann}[a]$, then $ab \in \mathfrak{q}$ and $a \notin \mathfrak{q}$. Hence $b^n \in \mathfrak{q}$, and then $b \in \mathfrak{p}$. This shows that $\operatorname{Ass} A/\mathfrak{q} = \{\mathfrak{p}\}$ and $\mathfrak{q}$ is $\mathfrak{p}$-primary as an A-submodule.

Let $\mathfrak{q} \subset A$ be a $\mathfrak{p}$-primary A-submodule. First we have $\mathfrak{p} = \sqrt{\mathfrak{q}}$ since $V(\mathfrak{p})$ is the unique irreducible component of $\operatorname{Supp} A/\mathfrak{q}$. Suppose $ab \in \mathfrak{q}$ and $a \notin \mathfrak{q}$. Then $b \in \operatorname{Ann}[a] \subset \mathfrak{p}$ since $\mathfrak{p}$ is the unique maximal element in $\{\operatorname{Ann}[c] : c \in A \setminus \mathfrak{q}\}$. This implies that $b^n \in \mathfrak{q}$.

Definition 1.2.15. Let A be a noetherian ring, M an A-module and $N \subset M$ a submodule. A *minimal primary decomposition* of N in M is a finite set of primary submodules $\{Q_i\}_{i=1}^n$ such that

$$N = \bigcap_{i=1}^{n} Q_i,$$

no Q_i can be omitted and $\operatorname{Ass} M/Q_i$ are pairwise distinct. For $\operatorname{Ass} M/Q_i = \{\mathfrak{p}\}$, Q_i is called belonging to $\mathfrak{p}$.

Indeed, if $N \subset M$ admits a minimal primary decomposition $N = \bigcap Q_i$ with Q_i belonging to $\mathfrak{p}$, then $\operatorname{Ass}(M/N) = \{\mathfrak{p}_i\}$. For given i, consider $N_i := \bigcap_{j \neq i} Q_j$, then $N_i/N \cong (N_i + Q_i)/Q_i$. Since $N_i \neq N$, $\operatorname{Ass} N_i/N \neq \emptyset$. On the other hand, $\operatorname{Ass} N_i/N \subset \operatorname{Ass} M/Q_i = \{\mathfrak{p}\}$. It follows that $\operatorname{Ass} N_i/N = \{\mathfrak{p}_i\}$, whence $\mathfrak{p}_i \in \operatorname{Ass} M/N$. Conversely, we have an injection $M/N \hookrightarrow \bigoplus M/Q_i$, so $\operatorname{Ass} M/N \subset \bigcup \operatorname{Ass} M/Q_i$. Due to this, if Q_i belongs to $\mathfrak{p}$, we also say that Q_i is the $\mathfrak{p}$-component of N.

Proposition 1.2.16. Suppose $N \subset M$ has a minimal primary decomposition. If $\mathfrak{p} \in \operatorname{Ass} M/N$ is not embedded, then the $\mathfrak{p}$ component of N is unique. Explicitly, we have $Q = \nu^{-1}(N_{\mathfrak{p}})$, where $\nu : M \to M_{\mathfrak{p}}$.

Proof. First we show that $Q = \nu^{-1}(Q_{\mathfrak{p}})$. Clearly $Q \subset \nu^{-1}(Q_{\mathfrak{p}})$. Suppose $x \in \nu^{-1}(Q_{\mathfrak{p}})$. Then there exists $s \in A \setminus \mathfrak{p}$ such that $sx \in Q$. That is, $[sx] = 0 \in M/Q$. If $[x] \neq 0$, we have $s \in \operatorname{Ann}[x] \subset \mathfrak{p}$. This contradiction enforces $Q = \nu^{-1}(Q_{\mathfrak{p}})$.

Then we show that $N_{\mathfrak{p}} = Q_{\mathfrak{p}}$. Just need to show that for $\mathfrak{p}' \neq \mathfrak{p}$ and the $\mathfrak{p}'$ component Q' of N, $Q'_{\mathfrak{p}} = M_{\mathfrak{p}}$. Since $\mathfrak{p}$ is not embedded, $\mathfrak{p}' \not\subset \mathfrak{p}$. Then $\mathfrak{p} \notin V(\mathfrak{p}) = \operatorname{Supp} M/Q'$. So $M_{\mathfrak{p}}/Q'_{\mathfrak{p}} = 0$. □

Example 1.2.17. If $\mathfrak{p}$ is embedded, then its components may not be unique. For example, let $M = A = \Bbbk[x,y]/(x^2,xy)$. Then for every $n \in \mathbb{Z}_{\geq 1}$, $(x) \cap (x^2, xy, y^n)$ is a minimal primary decomposition of $(0) \subset M$.

Let A be a noetherian ring and $\mathfrak{p} \subset A$ a prime ideal. We consider the $\mathfrak{p}$ component of $\mathfrak{p}^n$, which is called n-th symbolic power of $\mathfrak{p}$, denoted by $\mathfrak{p}^{(n)}$. We have $\mathfrak{p}^{(n)} = \mathfrak{p}^n A_{\mathfrak{p}} \cap A$. In general, $\mathfrak{p}^{(n)}$ is not equal to $\mathfrak{p}^n$; see below example.

Example 1.2.18. Let $A = \mathbf{k}[x,y,z,w]/(y^2 - zx^2, yz - xw)$ and $\mathfrak{p} = (y,z,w)$. We have $z = y^2/x^2, w = yz/x \in \mathfrak{p}^2 A_{\mathfrak{p}}$, whence $\mathfrak{p}^2 A_{\mathfrak{p}} = (z,w) \neq \mathfrak{p}^2$.

Theorem 1.2.19. Let A be a noetherian ring and M an A-module. Then for every $\mathfrak{p} \in \operatorname{Ass} M$, there is a $\mathfrak{p}$-primary submodule $Q(\mathfrak{p})$ such that

$$(0) = \bigcap_{\mathfrak{p} \in \operatorname{Ass} M} Q(\mathfrak{p}).$$

Proof. Consider the set

$$\mathcal{N} := \{N \subset M : \mathfrak{p} \notin \operatorname{Ass} N\}.$$

Note that $\operatorname{Ass} \bigcup N_i = \bigcup \operatorname{Ass} N_i$ by definition of associated prime ideals. Then it is easy to check that $\mathcal{N}$ satisfies the conditions of Zorn's Lemma. Hence $\mathcal{N}$ has a maximal element $Q(\mathfrak{p})$. We claim that $Q(\mathfrak{p})$ is $\mathfrak{p}$-primary. If there is $\mathfrak{p}' \neq \mathfrak{p} \in \operatorname{Ass} M/Q(\mathfrak{p})$, then there is a submodule $N' \cong A/\mathfrak{p}$. Let N'' be the preimage of N' in M. We have $Q(\mathfrak{p}) \subsetneq N''$ and $N'' \in \mathcal{N}$. This is a contradiction. By the fact $\operatorname{Ass} \bigcap N_i = \bigcap \operatorname{Ass} N_i$, we get the conclusion. □

Corollary 1.2.20. Let A be a noetherian ring and M a finite A-module. Then every submodule of M has a minimal primary decomposition.

1.3 Dimension and Depth

There are three numbers measuring the "size" of a local ring $(A, \mathfrak{m})$:

- $\dim A$: the Krull dimension of A.

- $\operatorname{depth} A$: the depth of A.
- $\dim_{\kappa(\mathfrak{m})} T_{A,\mathfrak{m}}$: the dimension of Zariski tangent space $T_{A,\mathfrak{m}} := (\mathfrak{m}/\mathfrak{m}^2)^\vee$ as a $\kappa(\mathfrak{m})$-vector space.

Somehow the Krull dimension is "homological" and the depth is "cohomological".

Definition 1.3.1. Let A be a noetherian ring. The *height of a prime ideal* $\mathfrak{p}$ in A is defined as the maximum length of chains of prime ideals contained in $\mathfrak{p}$, that is,

$$\operatorname{ht}(\mathfrak{p}) := \sup\{n \mid \exists \text{ a chain of prime ideals } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}\}.$$

The *Krull dimension* of A is defined as

$$\dim A := \max_{\mathfrak{p}\in \operatorname{Spec} A} \operatorname{ht}(\mathfrak{p}).$$

Example 1.3.2. Let A be a PID. For every two non-zero prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$, if $\mathfrak{p}_1 = t_1 A \subset \mathfrak{p}_2 = t_2 A$, then $t_2 \mid t_1$ and hence $\mathfrak{p}_1 = \mathfrak{p}_2$. It follows that $\dim A = 1$. Consequently, the ring of integers $\mathbb{Z}$ and the polynomial ring $\mathbf{k}[T]$ in one variable over a field have Krull dimension 1.

Definition 1.3.3. Let A be a noetherian ring, $I \subset A$ an ideal and M a finitely generated A-module. A sequence $t_1, \cdots, t_n \in I$ is called an *M-regular sequence in I* if t_i is not a zero divisor on $M/(t_1, \cdots, t_{i-1})M$ for all i.

Example 1.3.4. Let $A = \mathbf{k}[x, y]/(x^2, xy)$ and $I = (x, y)$. Then $\operatorname{depth}_I A = 0$.

Definition 1.3.5. Let A be a noetherian ring. For every $\mathfrak{p} \in \operatorname{Spec} A$, $\mathfrak{p}/\mathfrak{p}^2$ is a vector space over $\kappa(\mathfrak{p})$. The *Zariski's tangent space* $T_{A,\mathfrak{p}}$ of A at $\mathfrak{p}$ is defined as $(\mathfrak{p}/\mathfrak{p}^2)^\vee$, the dual $\kappa(\mathfrak{p})$-vector space of $\mathfrak{p}/\mathfrak{p}^2$.

1.3.1 Artinian Rings and Length of Modules

Definition 1.3.6. Let A be a ring and M an A module. *A simple module filtration of* M is a filtration

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0$$

such that M_i/M_{i-1} is a simple module, i.e. it has no submodule except 0 and itself. If M has a simple module filtration as above, we define the *length of* M as n and say that M has *finite length*.

The following proposition guarantees the length is well-defined.

Proposition 1.3.7. Suppose M has a simple module filtration $M = M_{0,0} \supsetneq M_{1,0} \supsetneq \cdots \supsetneq M_{n,0} = 0$. Then for any other filtration $M = M_{0,0} \supset M_{0,1} \supset \cdots \supset M_{0,m} = 0$ with $m > n$, there exist $k < m$ such that $M_{0,k} = M_{0,k+1}$.

Proof. We claim that there are at least $0 \le k_1 < \cdots < k_{m-n} < m$ satisfies that $M_{0,k_i} = M_{0,k_i+1}$. Let $M_{i,j} := M_{i,0} \cap M_{0,j}$. Inductively on n, we can assume that there exist $k_1, \cdots, k_{n-m+1}$ such that

$M_{1,k} = M_{1,k+1}$. Consider the sequence

$$M_{0,0}/M_{1,0} \supset (M_{0,1} + M_{1,0})/M_{1,0} \supset \cdots \supset (M_{0,m} + M_{1,0})/M_{1,0} = 0$$

in $M_{0,0}/M_{1,0}$. Since $M_{0,0}/M_{1,0}$ is simple, there is at most one k_i with $M_{0,k_i} + M_{1,0} \neq M_{0,k_i+1} + M_{1,0}$. And note that if $M_{0,k_i} + M_{1,0} = M_{0,k_i+1} + M_{1,0}$ and $M_{0,k_i} \cap M_{1,0} = M_{0,k_i} \cap M_{1,0}$, then $M_{0,k_i} = M_{0,k_i+1}$ by the Five Lemma. □

Example 1.3.8. Let A be a ring and $\mathfrak{m} \in \operatorname{mSpec} A$. Then $A/\mathfrak{m}$ is a simple module. Yang: To be completed.

Proposition 1.3.9. Let A be a ring and M an A-module. Then M is of finite length iff it satisfies both a.c.c and d.c.c.

Proof. Note that if M has either a strictly ascending chain or a strictly descending chain, M is of infinite length. Conversely, d.c.c guarantee M has a simple submodule and a.c.c guarantee the sequence terminates. □

Proposition 1.3.10. The length $l(-)$ is an additive function for modules of finite length. That is, if we have an exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$ with M_i of finite length, then $l(M_2) = l(M_1) + l(M_3)$.

Proof. The simple module filtrations of M_1 and M_3 will give a simple module filtration of M_2. □

Proposition 1.3.11. Let $(A, \mathfrak{m})$ be a local ring. Then A is artinian iff $\mathfrak{m}^n = 0$ for some $n \geq 0$.

Proof. Suppose A is artinian. Then the sequence $\mathfrak{m} \supset \mathfrak{m}^2 \supset \mathfrak{m}^3 \supset \cdots$ is stable. It follows that $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ for some n. By the Nakayama's Lemma 1.1.14, $\mathfrak{m}^n = 0$.

Conversely, we have

$$\mathfrak{m} \subset \mathfrak{N} \subset \bigcap_{\text{minimal prime ideal}} \mathfrak{p},$$

whence $\mathfrak{m}$ is minimal. □

Proposition 1.3.12. Let A be a ring. Then A is artinian iff A is of finite length.

Proof. First we show that A has only finite maximal ideal. Otherwise, consider the set $\{\mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_k\}$. It has a minimal element $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$ and for any maximal ideal $\mathfrak{m}$, $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \subset \mathfrak{m}$. It follows that $\mathfrak{m} = \mathfrak{m}_i$ for some i. Let $\mathfrak{M} = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$ be the Jacobi radical of A. Consider the sequence $\mathfrak{M} \supset \mathfrak{M}^2 \supset \cdots$ and by Nakayama's Lemma, we have $\mathfrak{M}^k = 0$ for some k. Consider the filtration

$$A \supset \mathfrak{m}_1 \supset \cdots \supset \mathfrak{m}_1^k \supset \mathfrak{m}_1^k \mathfrak{m}_2 \supset \cdots \supset \mathfrak{m}_1^k \cdots \mathfrak{m}_n^k = (0).$$

We have $\mathfrak{m}_1^k \cdots \mathfrak{m}_i^j / \mathfrak{m}_1^k \cdots \mathfrak{m}_i^{j+1}$ is an $A/\mathfrak{m}_i$-vector space. It is artinian and then of finite length. Hence A is of finite length. □

Theorem 1.3.13. Let A be a ring. Then A is artinian iff A is noetherian and of dimension 0.

Proof. Suppose A is artinian. Then A is noetherian by Proposition 1.3.12. Let $\mathfrak{p} \in \operatorname{Spec} A$. Then $A/\mathfrak{p}$ is an artinian integral domain. If there is $a \in A/\mathfrak{p}$ is not invertible, consider $(a) \supset (a^2) \supset \cdots$, we see $a = 0$. Hence $\mathfrak{p}$ is maximal and $\dim A = 0$.

Suppose that A is noetherian and of dimension 0. Then every maximal ideal is minimal. In particular, A has only finite maximal ideal $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$. Let $\mathfrak{q}_i$ be the $\mathfrak{p}_i$-component of (0). Then we have $A \hookrightarrow \bigoplus_i A/\mathfrak{q}_i$. We just need to show that $A/\mathfrak{q}_i$ is of finite length as A-module. If $\mathfrak{q}_i \subset \mathfrak{p}_j$, take radical we get $\mathfrak{p}_i \subset \mathfrak{q}_j$ and hence $i = j$. So $A/\mathfrak{q}_i$ is a local ring with maximal ideal $\mathfrak{p}_i A/\mathfrak{q}_i$. Then every element in $\mathfrak{p}_i A/\mathfrak{q}_i$ is nilpotent. Since $\mathfrak{p}_i$ is finitely generated, $(\mathfrak{p}_i A/\mathfrak{q}_i)^k = 0$ for some k. Then $A/\mathfrak{q}_i$ is artinian and then of finite length as $A/\mathfrak{q}_i$-module. Then the conclusion follows. □

1.3.2 DVR and Dedekind Domain

Definition 1.3.14. A *valuation* on a field K is a function $v : K^\times \to \Gamma$, where Γ is a totally ordered abelian group, such that for all $x, y \in K^\times$:

(i) $v(xy) = v(x) + v(y)$.

(ii) $v(x + y) \geq \min(v(x), v(y))$ if $x + y \neq 0$.

We extend v to K by setting $v(0) = +\infty$, where $+\infty$ is an element greater than all elements of Γ. If Γ is discrete with respect to the order topology, we say that v is a *discrete valuation*.

Example 1.3.15. (a) Let $\mathbf{K} = \mathbb{Q}$ and p be a prime number. Let $v : \mathbb{Q}^\times \to \mathbb{Z}$ be defined by $v(a/b) = n$ if $a/b = p^n(c/d)$ with c, d coprime to p. Then v is a discrete valuation on $\mathbb{Q}$.

(b) Let $\mathbf{K} = \mathbf{k}(T)$ be the field of rational functions over a field $\mathbf{k}$. For $f = x^n g \in \mathbf{k}(t)$ with $g(0) \in \mathbf{k}^\times$, let $v(f) = n$.

(c) Let $\mathbf{K} = \mathbb{C}_p$ the p-adic complex numbers. For $x \in \mathbb{C}_p^\times$, let $v(x) = -\log_p |x|_p$. Then v is a valuation on $\mathbb{C}_p$ which is not discrete.

Definition 1.3.16 (Discrete Valuation Ring)**.** Let V be a domain with field of fractions $\mathbf{K}$. We say that V is a *discrete valuation ring (DVR)* if there exists a discrete valuation v on $\mathbf{K}$ such that $V = \{x \in \mathbf{K} \mid v(x) \geq 0\}$.

Yang: To be completed

1.3.3 Krull's Principal Ideal Theorem

Theorem 1.3.17 (Krull's Principal Ideal Theorem)**.** Let A be a noetherian ring. Suppose $f \in A$ is not a unit. Let $\mathfrak{p}$ be a minimal prime ideal among those containing f. Then $\operatorname{ht}(\mathfrak{p}) \leq 1$.

Proof. By replacing A by $A_{\mathfrak{p}}$, we may assume A is local with maximal ideal $\mathfrak{p}$. Note that $A/(f)$ is artinian since it has only one prime ideal $\mathfrak{p}/(f)$.

Let $\mathfrak{q} \subsetneq \mathfrak{p}$. Consider the sequence $\mathfrak{q}^{(1)} \supset \mathfrak{q}^{(2)} \supset \cdots$, its image in $A/(f)$ is stationary. Then there exists $n \in \mathbb{Z}_{\geq 0}$ such that $\mathfrak{q}^{(n)} + (f) = \mathfrak{q}^{(n+1)} + (f)$. For $x \in \mathfrak{q}^{(n)}$, we may write $x = y + af$ for $y \in \mathfrak{q}^{(n+1)}$. Then $af \in \mathfrak{q}^{(n)}$. Since $\mathfrak{q}^{(n)}$ is $\mathfrak{q}$-primary and $f \notin \mathfrak{q}$, $a \in \mathfrak{q}^{(n)}$. Then we get $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)} + f\mathfrak{q}^{(n)}$. That is, $\mathfrak{q}^{(n)}/\mathfrak{q}^{(n+1)} = f\mathfrak{q}^{(n)}/\mathfrak{q}^{(n+1)}$. Note that $f \in \mathfrak{p}$, by Nakayama's Lemma, $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$. That is, $\mathfrak{q}^n A_\mathfrak{q} = \mathfrak{q}^{n+1} A_\mathfrak{q}$. By Nakayama's Lemma again, $\mathfrak{q}^n A_\mathfrak{q} = 0$. It follows that $\mathfrak{q}A_\mathfrak{q}$ is minimal, whence $A_\mathfrak{q}$ is artinian. Therefore, $\mathfrak{q}$ is minimal in A. □

Corollary 1.3.18. Let A be a noetherian local ring. Suppose $f \in A$ is not a unit. Then $\dim A/(f) \geq \dim A - 1$. If f is not contained in a minimal prime ideal, the equality holds.

Proof. Let $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ be a sequence of prime ideals. By assumption, $f \in \mathfrak{p}_n$. If $f \in \mathfrak{p}_0$, we get a sequence of prime ideals in $A/(f)$ of length n. Now we suppose $f \notin \mathfrak{p}_0$. Then there exists $k \geq 0$ such that $f \in \mathfrak{p}_{k+1} \setminus \mathfrak{p}_k$.

Choose $\mathfrak{q}$ be a minimal prime ideal among those containing $(\mathfrak{p}_{k-1}, f)$ and contained in $\mathfrak{p}_{k+1}$. Then by Krull's Principal Ideal Theorem 1.3.17, $\mathfrak{q}_k \subsetneq \mathfrak{p}_{k+1}$. Replace $\mathfrak{p}_k$ by $\mathfrak{q}_k$, we have $f \in \mathfrak{q}_k \setminus \mathfrak{p}_{k-1}$

Repeat this process, we get a sequence $\mathfrak{p}'_0 \subsetneq \cdots \subsetneq \mathfrak{p}'_n$ such that $f \in \mathfrak{p}'_1$. This gives a sequence $\mathfrak{p}'_1 \subsetneq \cdots \subsetneq \mathfrak{p}'_n$ in $A/(f)$. Hence we get $\dim A/(f) \geq \dim A - 1$.

Since f is not contained in minimal prime ideal, preimage of a minimal prime ideal in $A/(f)$ has height 1. Hence a sequence of prime ideals in A/fA can be extended by a minimal prime ideal in A. It follows that $\dim A/(f) + 1 \leq \dim A$. □

Proposition 1.3.19. Let $(A, \mathfrak{m})$ be a local noetherian ring with residue field $\mathbf{k}$. Then the following inequalities hold:

$$\operatorname{depth} A \leq \dim A \leq \dim_{\mathbf{k}} T_{A,\mathfrak{m}}.$$

Proof. The first inequality is a direct corollary of Corollary 1.3.18.

Let $t_1, \cdots, t_n$ be a $\kappa(\mathfrak{m})$-basis of $\mathfrak{m}/\mathfrak{m}^2$. Then we have $\mathfrak{m}/(t_1, \cdots, t_n) + \mathfrak{m}^2 = 0$, whence $\mathfrak{m}/(t_1, \cdots, t_n) = \mathfrak{m}(\mathfrak{m}/(t_1, \cdots, t_n))$. It follows that $\mathfrak{m} = (t_1, \cdots, t_n)$ by Nakayama's Lemma. By Corollary 1.3.18,

$$n + \dim A/(t_1, \cdots, t_n) \geq n - 1 + \dim A/(t_1, \cdots, t_{n-1}) \geq \cdots \geq 1 + \dim A/(t_1) \geq \dim A.$$

We conclude the result. □

Definition 1.3.20. Let X be a locally noetherian scheme and $k \in \mathbb{Z}_{\geq 0}$. We say that X *verifies property* (R_k) or *is regular in codimension* k if $\forall \xi \in X$ with $\operatorname{codim} Z_\xi \leq k$,

$$\dim_{\kappa(\xi)} T_{X,\xi} = \dim \mathcal{O}_{X,\xi}.$$

We say that X *verifies property* (S_k) if $\forall \xi \in X$ with $\operatorname{depth} \mathcal{O}_{X,\xi} < k$,

$$\operatorname{depth} \mathcal{O}_{X,\xi} = \dim \mathcal{O}_{X,\xi}.$$

Example 1.3.21. Let A be a noetherian ring. Then A verifies (S_1) iff A has no embedded point.

Suppose A verifies (S_1). If $\mathfrak{p} \in \operatorname{Ass} A$, every element in $\mathfrak{p}$ is a zero divisor. Then $\operatorname{depth} A_\mathfrak{p} = 0$. It follows that $\dim A_\mathfrak{p} = 0$ and then $\mathfrak{p}$ is minimal.

Suppose A has no embedded point. Let $\mathfrak{p} \in \operatorname{Spec} A$ with $\operatorname{depth} A_{\mathfrak{p}} = 0$. This means every element in $\mathfrak{p}A_{\mathfrak{p}}$ is a zero divisor. Then

$$\mathfrak{p} \subset \{\text{zero divisors in } A\} = \bigcup_{\text{minimal prime ideals}} \mathfrak{q}.$$

By Proposition 1.1.2, $\mathfrak{p} = \mathfrak{q}$ for some minimal $\mathfrak{q}$, whence $\dim A_{\mathfrak{p}} = 0$.

Example 1.3.22. Let A be a noetherian ring. Then A is reduced iff it verifies (R_0) and (S_1).

Suppose A is reduced. Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ be all minimal prime ideals of A. We have $\bigcap \mathfrak{p}_i = \mathfrak{N} = (0)$, where $\mathfrak{N}$ is the nilradical of A. Hence A has no embedded point. Since $A_{\mathfrak{p}}$ is artinian, local and reduced, $A_{\mathfrak{p}}$ is a field and hence regular.

Conversely, let $\operatorname{Ass} A$ be equal to $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_n\}$. Then every $\mathfrak{p}_i$ is minimal by (S_1). Let f be in $\mathfrak{N}$. Then the image of f in $A_{\mathfrak{p}_i}$ is 0 since by (R_0), $A_{\mathfrak{p}_i}$ is a field. It follows that $f \in \mathfrak{q}_i$, where $\mathfrak{q}_i$ is the $\mathfrak{p}_i$ component of (0) in A. Hence $f \in \bigcap \mathfrak{q}_i = (0)$. That is, A is reduced.

1.3.4 Cohen-Macaulay rings

Definition 1.3.23 (Cohen-Macaulay)**.** A noetherian local ring $(A, \mathfrak{m})$ is called *Cohen-Macaulay* if $\dim A = \operatorname{depth} A$. A noetherian ring A is called *Cohen-Macaulay* if for every prime ideal $\mathfrak{p} \in \operatorname{Spec} A$, the localization $A_{\mathfrak{p}}$ is Cohen-Macaulay. This is equivalent to that A verifies (S_k) for all $k \geq 0$.

Definition 1.3.24. Let $(A, \mathfrak{m})$ be a noetherian local ring of dimension d. A sequence $t_1, \cdots, t_d \in \mathfrak{m}$ is called a *system of parameters* if Yang: To be completed.

Example 1.3.25 (Non Cohen-Macaulay rings)**.** Yang: To be completed.

Corollary 1.3.26. Let A be a noetherian ring, M a finite A-module and $a \in A$ an M-regular element. Then $\operatorname{depth} M = \operatorname{depth} M/aM + 1$.

Corollary 1.3.27. Let A be a noetherian ring $a \in A$ a nonzero divisor. Then A verifies (S_d) iff A/aA verifies (S_{d-1}).

Definition 1.3.28. An ideal I of a noetherian ring A is called *unmixed* if

$$\operatorname{ht}(I) = \operatorname{ht}(\mathfrak{p}), \quad \forall \mathfrak{p} \in \operatorname{Ass}(A/I).$$

Here $\operatorname{ht}(I)$ is defined as

$$\operatorname{ht}(I) := \inf\{\operatorname{ht}(\mathfrak{p}) : I \subset \mathfrak{p}\}.$$

We say that *the unmixedness theorem holds for a noetherian ring* A if any ideal $I \subset A$ generated by $\operatorname{ht}(I)$ elements is unmixed. We say that *the unmixedness theorem holds for a locally noetherian scheme* X if $\mathcal{O}_{X,\xi}$ is unmixed for any point $\xi \in X$.

Proposition 1.3.29. Let X be a locally noetherian scheme. Then the unmixedness theorem holds for X if and only if X is Cohen-Macaulay.

Proof. We can assume that $X = \operatorname{Spec} A$ is affine.

Suppose X is Cohen-Macaulay. Let $I \subset A$ be an ideal generated by $a_1, \cdots, a_r$ with $r = \operatorname{ht}(I)$. We claim that $a_1, \cdots, a_r$ is an A-regular sequence. If so, we get that the unmixedness theorem holds for A by applying Example 1.3.21 on A/I. Since $\operatorname{ht}(a_1, \cdots, a_{r-1}) \leq r-1$ by Krull's Principal Ideal Theorem 1.3.17 and $\operatorname{ht}(a_1, \cdots, a_r) = r \leq \operatorname{ht}(a_1, \cdots, a_{r-1}) + 1$, we have $\operatorname{ht}(a_1, \cdots, a_{r-1}) = r-1$. By induction on r, we can assume that $a_1, \cdots, a_{r-1}$ is an A-regular sequence. Hence any prime ideal $\mathfrak{p} \in \operatorname{Ass} A/(a_1, \cdots, a_{r-1})$ has height $r-1$. Now suppose a_r is a zero divisor in $A/(a_1, \cdots, a_{r-1})$. Then there exists a prime ideal $\mathfrak{p} \in \operatorname{Ass} A/(a_1, \cdots, a_{r-1})$ such that $a_r \in \mathfrak{p}$. Then $I \subset \mathfrak{p}$ and $\operatorname{ht}(I) \leq r-1$. This contradicts that $\operatorname{ht}(I) = r$.

Suppose the unmixedness theorem holds for A. Let $\mathfrak{p} \in \operatorname{Spec} A$ be a prime ideal with $\operatorname{ht}(\mathfrak{p}) = r$. Then $\mathfrak{p} \in \operatorname{Ass} A$ if and only if $\operatorname{ht}(\mathfrak{p}) = 0$. If $r > 0$, there is a nonzero divisor $a \in \mathfrak{p}$. By Krull's Principal Ideal Theorem 1.3.17, $\operatorname{ht}(\mathfrak{p}A/aA) = r-1$. Inductively, we can find a regular sequence $a_1, \cdots, a_r$ in $\mathfrak{p}$. Then $\operatorname{depth} A_{\mathfrak{p}} = r$. □

Theorem 1.3.30. Let A be a noetherian ring of dimension d. The following are equivalent: Yang: To be completed.

Proof. Yang: To be completed. □

1.3.5 Regular rings

Definition 1.3.31. A noetherian ring A is said to be *regular at* $\mathfrak{p} \in \operatorname{Spec} A$ if we have

$$\dim_{\kappa(\mathfrak{p})} T_{A,\mathfrak{p}} = \dim A_{\mathfrak{p}},$$

where $\dim A_{\mathfrak{p}}$ is the Krull dimension of the local ring $A_{\mathfrak{p}}$.

A noetherian ring A is said to be *regular* if it is regular at every prime ideal $\mathfrak{p} \in \operatorname{Spec} A$. This is equivalent to the condition that A verifies (R_k) for all $k \geq 0$.

Remark 1.3.32. A noetherian ring A is regular if and only if it is regular at every maximal ideal $\mathfrak{m} \in \operatorname{mSpec} A$. The proof uses homological tools; see Theorem 2.3.17 and Corollary 2.3.18.

Definition 1.3.33. Let A be a noetherian ring that is regular at $\mathfrak{p} \in \operatorname{Spec} A$. A sequence $t_1, \cdots, t_n \in \mathfrak{p}$ is called a *regular system of parameters* at $\mathfrak{p}$ if their images form a basis of the $\kappa(\mathfrak{p})$-vector space $\mathfrak{p}/\mathfrak{p}^2$.

Proposition 1.3.34. Let $(A, \mathfrak{m})$ be a noetherian local ring that is regular at $\mathfrak{m}$. Let $t_1, \cdots, t_n$ be a regular system of parameters at $\mathfrak{m}$, $\mathfrak{p}_i = (t_1, \cdots, t_i)$ and $\mathfrak{p}_0 = (0)$. Then $\mathfrak{p}_i$ is a prime ideal of height i, and $A/\mathfrak{p}_i$ is a regular local ring for all i. In particular, regular local ring is integral, and the regular system of parameters $t_1, \cdots, t_n$ is a regular sequence in A.

Proof. By the Krull's Principal Ideal Theorem 1.3.17, we have

$$n-1=\dim A-1\leq \dim A/(t_1)\leq \dim_{\kappa(\mathfrak{m}/(t_1))} T_{A/(t_1),\mathfrak{m}/(t_1)}\leq n-1.$$

Hence $\dim A/(t_1)=n-1$ and $\mathrm{ht}(t_1)=1$. Since $t_2,\cdots,t_n$ generate $\mathfrak{m}/(t_1)$, we have that $A/(t_1)$ is regular at $\mathfrak{m}/(t_1)$ and the images of $t_2,\cdots,t_n$ form a regular system of parameters.

For integrality, we induct on the dimension of A. If $\dim A=0$, then A is a field and hence integral. Suppose $\dim A>0$, let $\mathfrak{q}$ be a minimal prime ideal of A. Then $t_1\notin \mathfrak{q}$. We have

$$n-1=\dim A-1\leq \dim A/(\mathfrak{q}+t_1A)\leq \dim_{\kappa(\mathfrak{q}/(t_1))} T_{A/(\mathfrak{q}+t_1A),\mathfrak{q}/(t_1)}\leq n-1.$$

By similar arguments, we have $A/(\mathfrak{q}+t_1A)$ is regular at $\mathfrak{m}/(\mathfrak{q}+t_1A)$. By induction hypothesis, both of A/t_1A and $A/(\mathfrak{q}+t_1A)$ are integral and of dimension $n-1$. Hence $t_1A=t_1A+\mathfrak{q}$, i.e. $\mathfrak{q}\subset t_1A$. For every $a=bt_1\in\mathfrak{q}$, we have $b\in\mathfrak{q}$ since $t_1\notin\mathfrak{q}$. Then $\mathfrak{q}\subset t_1\mathfrak{q}\subset\mathfrak{m}\mathfrak{q}$. By Nakayama's Lemma, $\mathfrak{q}=0$, whence A is integral. □

Corollary 1.3.35. A regular noetherian ring is Cohen-Macaulay.

Corollary 1.3.36. A regular noetherian ring is normal.

Remark 1.3.37. Indeed we can show a stronger result: a noetherian regular local ring is a UFD; see Yang: ref.

1.4 Finite Algebra and Normality

Let R be a ring and A be an R-algebra. We say that A is *of finite type* over R if there exists a surjective R-algebra homomorphism $R[T_1,\cdots,T_n]\to A$ for some $n\geq 0$. We say that A is finite over R if it is finite as an R-module.

1.4.1 Finite algebra

Let A be a ring and B a finite A-algebra.

Example 1.4.1. Let K be a number field. Then O_K is a finite $\mathbb{Z}$-algebra. Yang: To be completed.

Lemma 1.4.2. Let $A\subset B$ be noetherian rings such that B is finite over A. Then the induced morphism $\operatorname{Spec} B\to\operatorname{Spec} A$ is surjective.

Proof. For $\mathfrak{p}\in\operatorname{Spec} A$, let $S:=A-\mathfrak{p}$ and denote $S^{-1}B$ by $B_\mathfrak{p}$. Then we have $A_\mathfrak{p}\hookrightarrow B_\mathfrak{p}$ and $B_\mathfrak{p}$ is finite over $A_\mathfrak{p}$. Let $\mathfrak{P}B_\mathfrak{p}$ be a maximal ideal of $B_\mathfrak{p}$. We claim that $\mathfrak{P}B_\mathfrak{p}\cap A_\mathfrak{p}$ is maximal. Indeed, consider $A_\mathfrak{p}/(\mathfrak{P}\cap A_\mathfrak{p})\hookrightarrow B_\mathfrak{p}/\mathfrak{P}B_\mathfrak{p}$, the latter is finite over the former. This enforces $A_\mathfrak{p}/(\mathfrak{P}B_\mathfrak{p}\cap A_\mathfrak{p})$ be a field. Hence $\mathfrak{P}B_\mathfrak{p}\cap A_\mathfrak{p}=\mathfrak{p}A_\mathfrak{p}$, and then $\mathfrak{P}\cap A=\mathfrak{p}$. □

Proposition 1.4.3. Let $A\subset B$ be noetherian rings such that B is finite over A. Then $\dim A=\dim B$.

Proof. If we have a sequence $\mathfrak{P}_1 \subsetneq \mathfrak{P}_2$ of prime ideals in B, then there exists $f \in \mathfrak{P}_2 \setminus \mathfrak{P}_1$. Since B is finite over A, there exist $a_1, \cdots, a_n \in A$ such that

$$f^n + a_1 f^{n-1} + \cdots + a_n = 0.$$

Then $a_n \in \mathfrak{P}_2 \cap A$. If $a_n \in \mathfrak{P}_1$, $f^{n-1} + \cdots + a_{n_1} \in \mathfrak{P}_1$ since $f \notin \mathfrak{P}_1$. Then $a_{n-1} \in \mathfrak{P}_2$. Repeat the process, it will terminate, whence $\mathfrak{P}_1 \cap A \subsetneq \mathfrak{P}_2 \cap A$. Otherwise, we have $f^n \in a_1 B + \cdots + a_n B \subset \mathfrak{P}_1$.

Conversely, suppose we have $\mathfrak{p}_1, \mathfrak{p}_2 \in \operatorname{Spec} A$ with $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2$. Choose $\mathfrak{P}_1 \in \operatorname{Spec} B$ such that $\mathfrak{P}_1 \cap A = \mathfrak{p}_1$, then we have $A/\mathfrak{p}_1 \subset B/\mathfrak{P}_1$. Let $\mathfrak{P}_2$ be the preimage of the prime ideal in $B/\mathfrak{P}_1$ which is over image of $\mathfrak{p}_2$ in $A/\mathfrak{p}_1$. Proposition 1.4.2 guarantees that such $\mathfrak{P}_2$ exists. Then we get $\mathfrak{P}_1 \subsetneq \mathfrak{P}_2$. Repeat this progress, we get $\dim B \geq \dim A$. □

Yang: To be completed

Definition 1.4.4. An integral domain A is called *normal* if it is integrally closed in its field of fractions $\operatorname{Frac}(A)$.

Lemma 1.4.5. Let $A \subset C$ be rings and B the integral closure of A in C, S a multiplicatively closed subset of A. Then the integral closure of $S^{-1}A$ in $S^{-1}C$ is $S^{-1}B$.

Proof. For every $b \in B$ and $\forall s \in S$, there exists $a_i \in A$ s.t.

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0.$$

Then

$$\left(\frac{b}{s}\right)^n + \frac{a_1}{s^1}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_n}{s^n} = 0.$$

Hence b/s is integral over $S^{-1}A$, $S^{-1}B$ is integral over $S^{-1}A$.

If $c/s \in S^{-1}C$ is integral over $S^{-1}A$, then $\exists a_i \in S^{-1}A$ s.t.

$$\left(\frac{c}{s}\right)^n + a_1\left(\frac{c}{s}\right)^{n-1} + \cdots + a_n = 0.$$

Then

$$c^n + a_1 s c^{n-1} + \cdots + a_n s^n = 0 \in S^{-1}C$$

Then $\exists t \in S$ s.t.

$$t(c^n + a_1 s c^{n-1} + \cdots + a_n s^n) = 0 \in C.$$

Then

$$(ct)^n + a_1 st(ct)^{n-1} + \cdots + a_n s^n t^n = t^n(c^n + a_1 s c^{n-1} + \cdots + a_n s^n) = 0.$$

Hence ct is integral over A, then $ct \in B$. Then $c/s = (ct)/(st) \in S^{-1}B$. This completes the proof. □

Proposition 1.4.6. Normality is a local property. That is, for an integral domain A, TFAE:

(i) A is normal.

(ii) For any prime ideal $\mathfrak{p} \in \operatorname{Spec} A$, the localization $A_{\mathfrak{p}}$ is normal.

(iii) For any maximal ideal $\mathfrak{m} \in \operatorname{mSpec} A$, the localization $A_{\mathfrak{m}}$ is normal.

Proof. When A is normal, $A_{\mathfrak{p}}$ is normal by Lemma 1.4.5.

Assume that $A_{\mathfrak{m}}$ is normal for every $\mathfrak{m} \in \operatorname{mSpec} A$. If A is not normal, let $\tilde{A}$ be the integral closure of A in $\operatorname{Frac} A$, $\tilde{A}/A$ is a nonzero A-module. Suppose $\mathfrak{p} \in \operatorname{Supp} \tilde{A}/A$ and $\mathfrak{p} \subset \mathfrak{m}$. We have $\tilde{A}_{\mathfrak{m}}/A_{\mathfrak{m}} = 0$ and $\tilde{A}_{\mathfrak{p}}/A_{\mathfrak{p}} = (\tilde{A}_{\mathfrak{m}}/A_{\mathfrak{m}})_{\mathfrak{p}} \neq 0$. This is a contradiction. □

Proposition 1.4.7. Let A be a normal ring. Then $A[X]$ is also normal.

Definition 1.4.8. A scheme X is called *normal* if the local ring $\mathscr{O}_{X,\xi}$ is normal for any point $\xi \in X$. A ring A is called *normal* if $\operatorname{Spec} A$ is normal.

Remark 1.4.9. For a general ring A, let $S := A \setminus (\bigcup_{\mathfrak{p} \in \operatorname{Ass} A} \mathfrak{p}) = \bigcap_{\mathfrak{p} \in \operatorname{Ass} A} A \setminus \mathfrak{p}$. Then S is a multiplicative set. The localization $S^{-1}A$ is called *the total ring of fractions* of A.

Suppose A is reduced and $\operatorname{Ass} A = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_n\}$. Denote its total ring of fractions by Q. Note that elements in Q are either unit or zero divisor. Hence any maximal ideal $\mathfrak{m}$ is contained in $\bigcup \mathfrak{p}_i Q$, whence contained in some $\mathfrak{p}_i Q$. Thus $\mathfrak{p}_i Q$ are maximal ideals. And we have $\bigcap \mathfrak{p}_i Q = 0$. By the Chinese Remainder Theorem, we have $Q = \prod Q/\mathfrak{p}_i Q = \prod A_{\mathfrak{p}_i}$.

Let A be a reduced ring with total ring of fractions Q. Then A is normal iff A is integral closed in Q. If A is normal, then for every $\mathfrak{p} \in \operatorname{Spec} A$, $A_{\mathfrak{p}}$ is integral. Then there is unique minimal prime ideal $\mathfrak{p}_i \subset \mathfrak{p}$. In particular, any two minimal prime ideal are relatively prime. By the Chinese Remainder Theorem, $A = \prod A/\mathfrak{p}_i$. Just need to check $A/\mathfrak{p}_i$ is integral closed in $A_{\mathfrak{p}_i}$. This is clear by check pointwise.

Conversely, suppose A is integral closed in Q. Let e_i be the unit element of $A_{\mathfrak{p}_i}$. It belongs to A since $e_i^2 - e_i = 0$. Since $1 = e_1 + \cdots + e_n$ and $e_i e_j = \delta_{ij}$, we have $A = \prod A e_i$. Since Ae_i is integral closed in $A_{\mathfrak{p}_i}$, it is normal. Hence A is normal.

Lemma 1.4.10. Let A be a normal ring. Then A verifies (R_1) and (S_2).

Proof. Since all properties are local, we can assume A is integral and local.

For (S_2), by Example **??**, we only need to show that $\operatorname{Ass}_A A/f$ has no embedded point. Let $\mathfrak{p} = (f : g) =\in \operatorname{Ass}_A A/fA$ and $t := f/g \in \operatorname{Frac} A$. After Replacing A by $A_{\mathfrak{p}}$, we can assume that $\mathfrak{p}$ is maximal. By definition, $t^{-1}\mathfrak{p} \subset A$. If $t^{-1}\mathfrak{p} \subset \mathfrak{p}$, suppose $\mathfrak{p}$ is generated by $(x_1, \cdots, x_n)$ and $t^{-1}(x_1, \cdots, x_n)^T = \Phi(x_1, \cdots, x_n)^T$ for $\Phi \in M_n(A)$. There is a monic polynomial $\chi(T) \in A[T]$ vanishing Φ. Then $\chi(t^{-1}) = 0$ and $t^{-1} \in A$. This is impossible by definition of t. Then $t^{-1}\mathfrak{p} = A$, and $\mathfrak{p} = (t)$ is principal. By Krull's Principal Ideal Theorem 1.3.17, $\operatorname{ht}(\mathfrak{p}) = 1$.

Now we show that A verifies (R_1). Suppose $(A, \mathfrak{m})$ is local of dimension 1. Choosing $a \in \mathfrak{m}$, A/a is of dimension 0. Then by 1.3.11, $\mathfrak{m}^n \subset aA$ for some $n \geq 1$. Suppose $\mathfrak{m}^{n-1} \not\subset aA$. Choose $b \in \mathfrak{m}^{n-1} \setminus aA$ and let $t = a/b$. By construction, $t^{-1} \notin A$ and $t^{-1}\mathfrak{m} \subset A$. After similar argument, we see that $\mathfrak{m} = tA$, whence A is regular. □

Lemma 1.4.11. Let $(A, \mathfrak{m})$ be a noetherian local ring of dimension 1. Then A is normal iff A is regular.

Proof. By lemma 1.4.10, we just need to show that regularity implies normality.

Let $t \in \mathfrak{m} \setminus \mathfrak{m}^2$. Since A is regular, $\mathfrak{m} = (t)$. Let $I \subset \mathfrak{m}$ be an ideal. If $I \subset \bigcap_n \mathfrak{m}^n$, then for every $a \in I$, there exists a_n such that $a = a_n t^n$. Then we get an ascending chain of ideals $(a_1) \subset (a_2) \subset \cdots$. Hence $a = 0$ by Nakayama's Lemma. Suppose I is not zero. Then there is some n such that $I \subset \mathfrak{m}^n$ and $I \not\subset \mathfrak{m}^{n+1}$. For every $at^n \in I \setminus \mathfrak{m}^{n+1}$, $a \notin \mathfrak{m}$, whence a is a unit in A. Then $I = (t^n)$. Hence A is PID and hence normal. □

Proposition 1.4.12. Let A be a noetherian integral domain of dimension ≥ 1 verifying (S_2). Then

$$A = \bigcap_{\mathfrak{p} \in \operatorname{Spec} A, \operatorname{ht}(\mathfrak{p}) = 1} A_{\mathfrak{p}}.$$

Proof. Clearly $A \subset \bigcap A_{\mathfrak{p}}$. Let $t = f/g \in \bigcap A_{\mathfrak{p}}$. Since $f \in gA_{\mathfrak{p}}$ and we have $gA = \bigcap (gA_{\mathfrak{p}} \cap A)$, $f \in gA$. It follows that $t \in A$. □

Theorem 1.4.13 (Serre's criterion for normality)**.** Let X be a locally noetherian scheme. Then X is normal if and only if it verifies (R_1) and (S_2).

Proof. One direction has been proved in Lemma 1.4.10. Suppose X verifies (R_1) and (S_2). Again we can assume $X = \operatorname{Spec} A$ is affine and A is local. By Remark 1.4.9, we just need to show that A is integral closed in its total ring of fractions Q. Suppose we have

$$\left(\frac{a}{b}\right)^n + c_1 \left(\frac{a}{b}\right)^{n-1} + \cdots + c_n = 0 \in Q.$$

Since A verifies (S_2), $bA = \bigcap \nu_{\mathfrak{p}}^{-1}(b_{\mathfrak{p}} A_{\mathfrak{p}})$. So it is sufficient to show that $a_{\mathfrak{p}} \in b_{\mathfrak{p}} A_{\mathfrak{p}}$ with $\operatorname{ht}(\mathfrak{p}) = 1$. Note that $A_{\mathfrak{p}}$ is regular and hence normal by Lemma 1.4.11. Then above equation gives us desired result. □

1.5 Smoothness

1.5.1 Modules of differentials and derivations

In this subsection, let R be a ring and A an R-algebra.

Definition 1.5.1 (Derivation)**.** A *derivation* of A over R is an R-linear map $\partial : A \to M$ with an A-module such that for all $a, b \in A$, we have

$$\partial(ab) = a\partial(b) + b\partial(a).$$

Given the module M, the set of all derivations of A over R into M forms an A-module, denoted by $\operatorname{Der}_R(A, M)$.

Given a module homomorphism $f : M \to N$ of A-modules and a derivation $\partial \in \mathrm{Der}_R(A, M)$, the map $f \circ \partial$ is a derivation of A over R into N.

Proposition 1.5.2. The functor $\mathrm{Der}_R(A, -)$ is representable. The representing object is denoted by $\Omega_{A/R}$, which is called the *module of differentials* of A over R.

Proof. First suppose A is a free R-algebra with a set of generators $a_\lambda, \lambda \in \Lambda$. Then an R-derivation $\partial \in \mathrm{Der}_R(A, M)$ is uniquely determined by its values on the generators a_λ. Let

$$\Omega_{A/R} \coloneqq \bigoplus_{\lambda \in \Lambda} A \cdot \mathrm{d}a_\lambda$$

and $\mathrm{d} : A \to \Omega_{A/R}$ be the R-derivation defined by $a_\lambda \mapsto \mathrm{d}a_\lambda$. For any R-derivation $\partial \in \mathrm{Der}_R(A, M)$, we can define a unique A-module homomorphism $\Phi_\partial : \Omega_{A/R} \to M$ by sending $\mathrm{d}a_\lambda$ to $\partial(a_\lambda)$ such that $\partial = \Phi_\partial \circ \mathrm{d}$. This gives a bijection

$$\mathrm{Der}_R(A, M) \cong \mathrm{Hom}_A(\Omega_{A/R}, M), \quad \partial \mapsto \Phi_\partial.$$

Now suppose $A = F/I$ is an arbitrary R-algebra, where F is a free R-algebra and I is an ideal of F. Then we can define the module of differentials

$$\Omega_{A/R} \coloneqq \left(\Omega_{F/R} \otimes_F A\right) / \sum_{f \in I} A \cdot \mathrm{d}f.$$

The R-linear map $\mathrm{d}_A : F \otimes_F A \xrightarrow{\mathrm{d}_F} \Omega_{F/R} \otimes_F A \to \Omega_{A/R}$ is a derivation of A over R.

For any R-derivation $\partial \in \mathrm{Der}_R(A, M)$, note that $F \to A \xrightarrow{\partial} M$ is an R-derivation of F over R into M. Then we get an F-module homomorphism $\Omega_F \to M$. It gives an A-module homomorphism $\Omega_F \otimes_F A \to M, \mathrm{d}f \otimes 1 \mapsto \partial f$. This map factors into $\Omega_F \otimes_F A \to \Omega_{A/R}$ and $\Phi_\partial : \Omega_{A/R} \to M$. Since Φ_∂ is A-linear and $\Omega_{A/R}$ is generated by $\mathrm{d}a_\lambda$ as A-module, such Φ_∂ is unique. □

Corollary 1.5.3. Suppose A is of finite type over R. Then the module of differentials $\Omega_{A/R}$ is a finitely generated A-module.

Remark 1.5.4. Let B be an A-algebra, M an A-module and N a B-module. If there is a homomorphism of A-modules $M \to N$, then we can extend it to a homomorphism of B-modules $M \otimes_A B \to N$ by sending $m \otimes b$ to $m \cdot b$. And such extension is unique in the sense of following commutative diagram:

$$\begin{tikzcd} M \arrow[r] \arrow[d] & N . \\ M \otimes_A B \arrow[ur, "\exists!"'] & \end{tikzcd}$$

Hence we get a natural bijection

$$\mathrm{Hom}_A(M, N) \cong \mathrm{Hom}_B(M \otimes_A B, N).$$

Proposition 1.5.5. Let A, R' be R-algebras and $A' := A \otimes_R R'$. Then the module of differentials $\Omega_{A'/R'}$ is isomorphic to $\Omega_{A/R} \otimes_A A'$.

Proof. We check the universal property of $\Omega_{A/R} \otimes_A A'$. First, the map

$$\mathrm{d}_{A'} : A \otimes_R R' \to \Omega_{A/R} \otimes_R R' \cong \Omega_{A/R} \otimes_A A', \quad a \otimes r \mapsto \mathrm{d}a \otimes r$$

is an R'-derivation of A' into $\Omega_{A/R} \otimes_A A'$. For any R'-derivation $\partial' : A' \to M$ into an A'-module M, we can compose it with the homomorphism $A' \to A$ and get an R-derivation $\partial : A \to M$. By the universal property of $\Omega_{A/R}$, there is a unique A-module homomorphism $\Phi : \Omega_{A/R} \to M$ such that $\partial = \Phi \circ \mathrm{d}_A$. Then we can extend it to an A'-module homomorphism $\Phi' : \Omega_{A/R} \otimes_A A' \to M$ by Remark 1.5.4. By the construction, we have $\Phi' \circ \mathrm{d}_{A'} = \partial'$. □

Proposition 1.5.6. Let A be an R-algebra and S a multiplicative set of A. Then we have an isomorphism

$$\Omega_{S^{-1}A/R} \cong S^{-1}\Omega_{A/R}.$$

Proof. Let

$$\mathrm{d}_{S^{-1}A} : S^{-1}A \to S^{-1}\Omega_{A/R}, \quad \frac{a}{s} \mapsto \frac{s\mathrm{d}a - a\mathrm{d}s}{s^2}.$$

By direct computation, $\mathrm{d}_{S^{-1}A}$ is an R-derivation of $S^{-1}A$ over R into $S^{-1}\Omega_{A/R}$. For any R-derivation $\partial : S^{-1}A \to M$ into an $S^{-1}A$-module M, we can get an $S^{-1}A$-module homomorphism $\Phi' : S^{-1}\Omega_{A/R} \to M$ as proof of Proposition 1.5.5. We have

$$\partial(s \cdot \frac{a}{s}) = s\partial(\frac{a}{s}) + \frac{a}{s}\partial s.$$

It follows that

$$\partial(\frac{a}{s}) = \frac{s\partial a - a\partial s}{s^2} = \frac{s\Phi'(\mathrm{d}a) - a\Phi'(\mathrm{d}s)}{s^2} = \Phi'(\frac{s\mathrm{d}a - a\mathrm{d}s}{s^2}).$$

Thus, $\Phi' \circ \mathrm{d}_{S^{-1}A} = \partial$. □

Theorem 1.5.7. Let A be an R-algebra and B an A-algebra. Then there is a natural short exact sequence

$$\Omega_{A/R} \otimes_A B \to \Omega_{B/R} \to \Omega_{B/A} \to 0$$

of B-modules.

Proof. Let $\mathrm{d}_{A/R} : A \to \Omega_{A/R}$ be the R-derivation of A over R. The map $A \to B \xrightarrow{\mathrm{d}_{B/R}} \Omega_{B/R}$ induces a B-linear map

$$u : \Omega_{A/R} \otimes_A B \to \Omega_{B/R}, \quad \mathrm{d}_{A/R}(a) \otimes b \mapsto b\mathrm{d}_{B/R}(a).$$

The map $\mathrm{d}_{B/A}$ is an A-derivation and hence R-derivation. Then it induces a B-linear map

$$v : \Omega_{B/R} \to \Omega_{B/A}, \quad \mathrm{d}_{B/R}(b) \mapsto \mathrm{d}_{B/A}(b).$$

Since $\Omega_{B/A}$ is generated by elements of the form $\mathrm{d}_{B/A}(b)$ for $b \in B$, the map v is surjective. And clearly $\mathrm{d}_{B/A}(a) = a\mathrm{d}_{B/A}(1) = 0$ for $a \in A$.

Consider the composition $B \xrightarrow{\mathrm{d}_{B/R}} \Omega_{B/R} \to \Omega_{B/R}/\mathfrak{J}u$. For every $a \in A, b \in B$, we have

$$[\mathrm{d}_{B/R}(ab)] = [b\mathrm{d}_{B/R}(a) + a\mathrm{d}_{B/R}(b)] = [b\mathrm{d}_{B/R}(a)] + [a\mathrm{d}_{B/A}(b)] = [a\mathrm{d}_{B/A}(b)].$$

Hence it is indeed an A-derivation of B. Then it induces a B-linear map

$$\varphi : \Omega_{B/A} \to \Omega_{B/R}/\mathfrak{J}u, \quad \mathrm{d}_{B/A}(b) \mapsto [\mathrm{d}_{B/R}(b)].$$

The map φ is surjective since $\Omega_{B/R}$ is generated by elements of the form $\mathrm{d}_{B/R}(b)$ for $b \in B$. Note that the composition

$$\Omega_{B/A} \xrightarrow{\varphi} \Omega_{B/R}/\mathfrak{J}u \to \Omega_{B/A}/\operatorname{Ker} v$$

is the identity map. Thus, φ is injective and hence an isomorphism. In particular, we have $\operatorname{Ker} v = \mathfrak{J}u$. □

Remark 1.5.8. The exact sequence in Theorem 1.5.7 is left exact if and only if every R-derivation of A into B-module extends to an R-derivation of B into B-module.

Yang: To be completed.

Theorem 1.5.9. Let A be an R-algebra and I an ideal of A. Set $B \coloneqq A/I$. Then there is a natural short exact sequence

$$I/I^2 \to \Omega_{A/R} \otimes_A B \to \Omega_{B/R} \to 0$$

of B-modules.

Proof. Suppose $A = F/\mathfrak{b}$ for some free R-algebra F and an ideal $\mathfrak{b}$ of F. Let $\mathfrak{a}$ be the preimage of I in F. Let $\mathrm{d}\mathfrak{b}$ (resp. $\mathrm{d}\mathfrak{a}$) denote the image of $\mathfrak{b}$ (resp. $\mathfrak{a}$) in $\Omega_{F/R}$. Then we have

$$\Omega_{A/R} \otimes_A B = \Omega_{F/R} \otimes_F B/(\mathrm{d}\mathfrak{b} \otimes_F B), \quad \Omega_{B/R} = \Omega_{F/R} \otimes_F B/(\mathrm{d}\mathfrak{a} \otimes_F B).$$

Clearly

$$I/I^2 \cong (\mathfrak{a}/\mathfrak{b}) \otimes_F B \to (\mathrm{d}\mathfrak{a} \otimes_F B)/(\mathrm{d}\mathfrak{b} \otimes_F B)$$

is surjective. Then the exact sequence follows. □

Definition 1.5.10. Let $\mathbf{k}$ be a field and A an integral $\mathbf{k}$-algebra of finite type of dimension n. We say A is *smooth at* $\mathfrak{p} \in \operatorname{Spec} A$ if the module of differentials $\Omega_{A,\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module of rank n.

Example 1.5.11. Let $\mathbf{K}/\mathbf{k}$ be a finite generated field extension and $\mathbf{k}'$ be the algebraic closure of $\mathbf{k}$ in $\mathbf{K}$. Then

$$\dim_{\mathbf{K}} \Omega_{\mathbf{K}/\mathbf{k}} = \operatorname{trdeg}(\mathbf{K}/\mathbf{k}) + \dim_{\mathbf{k}'} \Omega_{\mathbf{k}'/\mathbf{k}},$$

and $\dim_{\mathbf{k}'} \Omega_{\mathbf{k}'/\mathbf{k}} = 0$ if and only if $\mathbf{k}'$ is separable over $\mathbf{k}$.

First suppose $\mathbf{K} = \mathbf{k}'$ is algebraic over $\mathbf{k}$. Suppose $\mathbf{k}'/\mathbf{k}$ is separable. For every $\alpha \in \mathbf{k}'$, suppose $f(\alpha) = 0$ for $f \in \mathbf{k}[T]$. Then $\mathrm{d}f(\alpha) = f'(\alpha)\mathrm{d}\alpha = 0$. By the separability of $\mathbf{k}'/\mathbf{k}$, we have $f'(\alpha) \neq 0$. It follows that $\mathrm{d}\alpha = 0$. Conversely, let $\alpha \in \mathbf{k}'$ be a inseparable element over $\mathbf{k}$. Since $\mathbf{k}[\alpha] \to \mathbf{k}[\alpha], \alpha^n \mapsto n\alpha^{n-1}$ is a non-zero R-derivation, we have $\Omega_{\mathbf{k}[\alpha]/\mathbf{k}} \neq 0$. By induction on number of generated elements, choosing a middle field $\mathbf{k} \subset \mathbf{k}'' \subset \mathbf{k}'$, at least one of $\Omega_{\mathbf{k}''/\mathbf{k}}$ and $\Omega_{\mathbf{k}'/\mathbf{k}''}$ is non-zero. Then $\Omega_{\mathbf{K}/\mathbf{k}} \neq 0$ by Theorem 1.5.7.

Then suppose $\mathbf{k}' = \mathbf{k}$. By the Noether's Normalization Lemma, we can find a finite set of elements $T_1, \cdots, T_n \in \mathbf{K}$ such that $\mathbf{K}$ is algebraic over $\mathbf{k}'(T_1, \ldots, T_n)$. Note that we can choose T_i such that $\mathbf{K}/\mathbf{k}'(T_1, \cdots, T_n)$ is separable. To see this, if $\alpha \in \mathbf{K}$ is an inseparable element over $\mathbf{k}'(T_1, \cdots, T_n)$, then by replacing a suitable T_i with α, we reduce the inseparable degree of $\mathbf{K}/\mathbf{k}'(T_1, \cdots, T_n)$.

Since $\mathbf{K}/\mathbf{k}'(T_1, \cdots, T_n)$ is finite, every $\mathbf{k}$-derivation of $\mathbf{k}'(T_1, \cdots, T_n)$ into $\mathbf{K}$-module extends to a $\mathbf{k}$-derivation of $\mathbf{K}$ into $\mathbf{K}$-module. Then by Remark 1.5.8, we have

$$0 \to \Omega_{\mathbf{k}'(T_1,\cdots,T_n)/\mathbf{k}} \otimes_{\mathbf{k}'(T_1,\cdots,T_n)} \mathbf{K} \to \Omega_{\mathbf{K}/\mathbf{k}} \to \Omega_{\mathbf{K}/\mathbf{k}'(T_1,\cdots,T_n)} \to 0.$$

Finally, note that every $\mathbf{k}$-derivation ∂ of $\mathbf{k}'$ into $\mathbf{K}$-module can be extended to $\mathbf{k}'[T_1, \cdots, T_n]$ by setting $\partial T_i = 0$. Thus, we have

$$0 \to \Omega_{\mathbf{k}'/\mathbf{k}} \otimes_{\mathbf{k}'} \mathbf{k}'[T_1, \cdots, T_n] \to \Omega_{\mathbf{k}'[T_1,\cdots,T_n]/\mathbf{k}} \to \Omega_{\mathbf{k}'[T_1,\cdots,T_n]/\mathbf{k}'} \to 0.$$

This follows that

$$\dim_{\mathbf{K}} \Omega_{\mathbf{K}/\mathbf{k}} = \dim_{\mathbf{K}} \Omega_{\mathbf{K}/\mathbf{k}'} + \dim_{\mathbf{k}'} \Omega_{\mathbf{k}'/\mathbf{k}}.$$

1.5.2 Applications to affine varieties

Let $\mathbf{k}$ be arbitrary field, $A = \mathbf{k}[T_1, \ldots, T_n]$ and $\mathfrak{m}$ a maximal ideal of A such that $\kappa(\mathfrak{m})$ is separable over $\mathbf{k}$. We try to give an explanation of Zariski's tangent space at $\mathfrak{m}$ using the language of derivation. We know that $\Omega_{A/\mathbf{k}} = \bigoplus_{i=1}^n A\mathrm{d}T_i$, thus $\Omega_{A_\mathfrak{m}/\mathbf{k}} \cong \bigoplus_{i=1}^n A_\mathfrak{m}\mathrm{d}T_i$. Then

$$\mathrm{Der}_{\mathbf{k}}(A_\mathfrak{m}, A_\mathfrak{m}) \cong \mathrm{Hom}_{\mathbf{k}}(\Omega_{A_\mathfrak{m}/\mathbf{k}}, A_\mathfrak{m}) \cong \bigoplus_{i=1}^n A_\mathfrak{m}\partial_i,$$

where $\partial_i \in \mathrm{Der}_{\mathbf{k}}(A_\mathfrak{m}, A_\mathfrak{m})$ is the derivation defined by $\mathrm{d}T_i \mapsto 1$ and $\mathrm{d}T_j \mapsto 0$ for $j \neq i$. It coincides with the usual derivation $f \mapsto \partial f/\partial T_i$. Consider the restriction of ∂_i to $\mathfrak{m}$ and take values in the residue field $\kappa(\mathfrak{m})$, we get

$$\Phi : \mathfrak{m} \xrightarrow{(\partial_1,\cdots,\partial_n)^T} A_\mathfrak{m}^n \to \kappa(\mathfrak{m})^n.$$

Since $\kappa(\mathfrak{m})$ is separable over $\mathbf{k}$, we claim that $\mathrm{Ker}\,\Phi = \mathfrak{m}^2$. Indeed, by Remark 1.5.12, we can write every $f \in \mathfrak{m} \setminus \mathfrak{m}^2$ as $\sum_i a_i g_i$. Then

$$\frac{\partial f}{\partial T_i} = a_i \frac{\partial g_i}{\partial T_i} + g_i \frac{\partial a_i}{\partial T_i}.$$

Since g_i is separable, the image of $\partial g_i/\partial T_i$ in $\kappa(\mathfrak{m})$ is not zero. Hence $\Phi(f) \neq 0$. By the claim, Φ induces an isomorphism $\mathfrak{m}/\mathfrak{m}^2 \cong \kappa(\mathfrak{m})^n$ of $\kappa(\mathfrak{m})$-vector spaces. Then we get

$$T_{A,\mathfrak{m}} = (\mathfrak{m}/\mathfrak{m}^2)^\vee \cong \bigoplus_{i=1}^n \kappa(\mathfrak{m}) \cdot \partial_i|_x,$$

where $x \in \mathbb{a}_{\mathbf{k}}^n$ is the point corresponding to $\mathfrak{m}$. This coincides with the usual tangent space at x in language of differential geometry.

Remark 1.5.12. Let $\mathbf{k}$ be arbitrary field, $A = \mathbf{k}[T_1, \cdots, T_n]$ and g_i irreducible polynomials in one variable T_i over $\mathbf{k}$. Then for every $f \in A$, we can write

$$f = \sum_{I=(i_1,\cdots,i_n)\in\mathbb{Z}^n_{\geq 0}} a_I g_1^{i_1} \cdots g_n^{i_n}, \quad a_I \in A, \quad \deg_{T_i} a_I \leq \deg g_i.$$

This is called the *Taylor expansion of f with respect to $g_1, \cdots, g_n$*.

When $n = 1$, it follows from division algorithm. For $n > 1$, we can use induction on n. Let $\mathbf{K} = \mathbf{k}(T_1, \cdots, T_{n-1})$. Then we can write f as

$$f = \sum_{i=0}^{r} a_i g_n^i, \quad a_i \in \mathbf{K}[T_n], \quad \deg a_i < \deg g_n.$$

Comparing the coefficients of two sides from the highest degree of T_n to the lowest degree, we see that

$$a_i \in \mathbf{k}[T_1, \cdots, T_{n-1}].$$

By induction hypothesis, the conclusion follows.

Let $B = A/I$ be a $\mathbf{k}$ of finite type, $I = (F_1, \dots, F_m) \subset \mathfrak{m}$ and $\mathfrak{n}$ the image of $\mathfrak{m}$ in B. We have an exact sequence of $\kappa(\mathfrak{m})$-vector spaces

$$0 \to I/(I \cap \mathfrak{m}^2) \to \mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{n}/\mathfrak{n}^2 \to 0.$$

It induces an isomorphism

$$T_{B,\mathfrak{n}} \cong \{\partial \in T_{A,\mathfrak{m}} : \partial(f) = 0, \forall f \in I\}.$$

The *Jacobian matrix* of $F_1, \dots, F_m$ is the $m \times n$ matrix

$$J(F_1, \dots, F_m) := \left(\frac{\partial F_i}{\partial T_j}\right)_{1\leq i\leq m, 1\leq j\leq n}$$

with entries in B.

Theorem 1.5.13. Setting as above. Then B is regular at $\mathfrak{n}$ if and only if the Jacobian matrix J has maximal rank $n - \dim B_{\mathfrak{n}}$ after taking values in the residue field $\kappa(\mathfrak{m})$.

Proof. We have an exact sequence

$$0 \to T_{B,\mathfrak{n}} \to T_{A,\mathfrak{m}} \xrightarrow{\Psi} \kappa^m \to 0,$$

where Ψ sends $\partial \in T_{A,\mathfrak{m}}$ to $(\partial(F_1), \dots, \partial(F_m))^T$. Note that the matrix of Ψ is just J^T, the transpose of the Jacobian matrix. Hence

$$\operatorname{rank} J = n - \dim_\kappa T_{B,\mathfrak{n}} \leq n - \dim B_{\mathfrak{n}}$$

and the equality holds if and only if B is regular at $\mathfrak{n}$. □

Remark 1.5.14. If $\kappa(\mathfrak{m})$ is not separable over $\mathbf{k}$, then we still have the inequality

$$\operatorname{rank} J \leq n - \dim B_{\mathfrak{n}}.$$

Indeed, in any case, we have an exact sequence

$$0 \to I/(I \cap \mathfrak{m}^2) \to \mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{n}/\mathfrak{n}^2 \to 0.$$

Hence $\dim_\kappa I/(I \cap \mathfrak{m}^2) = n - \dim B_\mathfrak{n}$. There is a $\kappa(\mathfrak{m})$-linear map

$$I/(I \cap \mathfrak{m}^2) \to \kappa(\mathfrak{m})^n, \quad [f] \mapsto (\partial_1(f), \dots, \partial_n(f))^T,$$

and every row of the Jacobian matrix J is in the image of this map. Thus, the rank of J is at most $n - \dim B_\mathfrak{n}$.

Hence if $\operatorname{rank} J = n - \dim B_\mathfrak{n}$, we can still see that B is regular at $\mathfrak{n}$. However, the converse does not hold in general.

Proposition 1.5.15. Let $\mathbf{k}$ be a field, $\Bbbk$ the algebraic closure of $\mathbf{k}$, A a $\mathbf{k}$-algebra of finite type and $A_\Bbbk \coloneqq A \otimes_\mathbf{k} \mathbf{k}$. Yang: Suppose $A_\Bbbk$ is integral. Let $\mathfrak{m} \in \operatorname{mSpec} A$ and $\mathfrak{m}'$ be a maximal ideal of $A_\Bbbk$ lying over $\mathfrak{m}$. Then

(a) If $A_\Bbbk$ is regular at $\mathfrak{m}'$, then A is regular at $\mathfrak{m}$;

(b) suppose $\kappa(\mathfrak{m})$ is separable over $\mathbf{k}$, the converse holds.

Proof. Regarding $J_\mathfrak{m}$ and $J_{\mathfrak{m}'}$ as matrices with entries in $\Bbbk$, they are the same and hence have the same rank. If $A_\Bbbk$ is regular at $\mathfrak{m}'$, since $\kappa(\mathfrak{m}) = \Bbbk$, then $\operatorname{rank} J_{\mathfrak{m}'} = n - \dim A_{\Bbbk,\mathfrak{m}'}$. Note that $\dim A_{\Bbbk,\mathfrak{m}'} = \operatorname{trdeg}(\mathscr{K}(A_\Bbbk)/\Bbbk) = \operatorname{trdeg}(\mathscr{K}(A)/\mathbf{k}) = \dim A_\mathfrak{m}$, we have $\operatorname{rank} J_\mathfrak{m} = n - \dim A_\mathfrak{m}$. Hence A is regular at $\mathfrak{m}$.

Conversely, suppose A is regular at $\mathfrak{m}$ and $\kappa(\mathfrak{m})$ is separable over $\mathbf{k}$. Then $\operatorname{rank} J_\mathfrak{m} = n - \dim A_\mathfrak{m}$. Hence $A_\Bbbk$ is regular at $\mathfrak{m}'$. Yang: To be modified. □

Proposition 1.5.16. Let $\mathbf{k}$ be a field and A an integral $\mathbf{k}$-algebra of finite type and of dimension n. Let $\Bbbk$ be the algebraic closure of $\mathbf{k}$ and $A_\Bbbk \coloneqq A \otimes_\mathbf{k} \Bbbk$. Then A is smooth at $\mathfrak{p} \in \operatorname{Spec} A$ if and only if $A_\Bbbk$ is regular at every $\mathfrak{m}'$ over $\mathfrak{m}$.

Proof. Since $\Omega_{A_\Bbbk/\Bbbk} \cong \Omega_{A/\mathbf{k}} \otimes_A A_\Bbbk$ is free of rank n if and only if $\Omega_{A/\mathbf{k}}$ is free of rank n, we can assume that $\mathbf{k} = \Bbbk$. If A is smooth at $\mathfrak{p}$, then $\Omega_{A_\mathfrak{p}/\mathbf{k}} \cong \bigoplus A_\mathfrak{p} \mathrm{d}f_i$ is free of rank n. Let $\mathfrak{P}_i \in \operatorname{Der}_\Bbbk(A_\mathfrak{m}, A_\mathfrak{m})$ be the derivation defined by $\mathrm{d}f_i \mapsto 1$ and $\mathrm{d}T_j \mapsto 0$ for $j \neq i$. Then we have $\partial_i f_j = \delta_{ij}$ for $1 \leq i,j \leq n$. Then similar to above argument, we have an isomorphism

$$\mathfrak{m}/\mathfrak{m}^2 \xrightarrow{(\partial_1,\dots,\partial_n)^T} \Bbbk^n.$$

This shows that $A_\Bbbk$ is regular at $\mathfrak{m}$.

Conversely, suppose $A_\Bbbk$ is regular at $\mathfrak{m}$. Note that $\mathfrak{m}/\mathfrak{m}^2 \to \Omega_{A,\Bbbk} \otimes_A \Bbbk$ is surjective since $\Omega_{A_\Bbbk/\Bbbk} = 0$. Then by Nakayama's lemma, $\Omega_{A_\mathfrak{m}/\Bbbk}$ is generated by n elements as an $A_\mathfrak{m}$-module.

Note that $\dim_{\mathscr{K}(A)} \Omega_{\mathscr{K}(A)/\mathbf{k}} = \operatorname{trdeg}(\mathscr{K}(A)/\mathbf{k}) = \dim A_\mathfrak{m} = n$. Yang: By induction on transcendental degree.

Yang: By Nakayama's Lemma, $\Omega_{A_\mathfrak{m}/\mathbf{k}}$ is free of rank n as an $A_\mathfrak{m}$-module.

Yang: To be completed. □

Example 1.5.17. Let $\mathbf{k}$ be an imperfect field of characteristic $p > 2$. Suppose $\alpha = \beta^p \in \mathbf{k}$ and β is not in $\mathbf{k}$. Let $A = \mathbf{k}[x, y]/(x^2 - y^p - \alpha)$ and $\mathfrak{m} = (x, y^p - \alpha) = (x)$. Note that $\mathfrak{m}$ is principal, so A is regular at $\mathfrak{m}$. However,

$$J_{\mathfrak{m}} = \left(\frac{\partial}{\partial x}(x^2 - y^p - \alpha), \frac{\partial}{\partial y}(y^p - \alpha)\right) = (2x, 0) = (0, 0) \in M_{1\times 2}(\kappa(\mathfrak{m})).$$

Thus, A is not smooth at $\mathfrak{m}$. From the view of differentials, we have

$$\Omega_{A_{\mathfrak{m}}/\mathbf{k}} = A_{\mathfrak{m}}\mathrm{d}x \oplus A_{\mathfrak{m}}\mathrm{d}y / A_{\mathfrak{m}} \cdot x\mathrm{d}x = \kappa(\mathfrak{m})\mathrm{d}x \oplus A_{\mathfrak{m}}\mathrm{d}y,$$

which is not free as an $A_{\mathfrak{m}}$-module.

1.6 Formal Completion

1.6.1 Formal completion of rings and modules

Definition 1.6.1. Let A be a ring and $\mathcal{T}$ a topology on A. We say that $(A, \mathcal{T})$ is a *topological ring* if the operations of addition and multiplication are continuous with respect to the topology $\mathcal{T}$. Given a topological ring A. A *topological A-module* is a pair $(M, \mathcal{T}_M)$ where M is an A-module and $\mathcal{T}_M$ is a topology on M such that the addition and scalar multiplication is continuous. The morphisms of topological A-modules are the continuous A-linear maps. They form a category denoted by $\mathbf{TopMod}_A$.

Definition 1.6.2. Let A be a ring, I an ideal of A and M an A-module. The *I-adic topology* on M is the topology defined by the basis of open sets $x + I^k M$ for all $x \in M, k \geq 0$.

Example 1.6.3. Let $A = \mathbb{Z}$ be the ring of integers and p a prime number. The p-adic topology on $\mathbb{Z}$ is defined by the metric

$$d(x, y) \coloneqq \|x - y\|_p \coloneqq p^{-v(x-y)},$$

where v is the valuation defined by the ideal $p\mathbb{Z}$.

Note that for I-adic topology, any homomorphism $f : M \to N$ of A-modules is continuous since $f(x + I^k N) \subset f(x) + I^k M$ for all $x \in M$ and $k \geq 0$. Hence the forgotten functor $\mathbf{TopMod}_A \to \mathbf{Mod}_A$ gives an equivalence of categories.

Let M be an A-module equipped with the I-adic topology. Note that M is Hausdorff as a topological space if and only if $\bigcap_{n\geq 0} I^n M = \{0\}$. In this case, we say that M is *I-adically separated.*

When M is I-adically separated, we can see that M is indeed a metric space. Fix $r \in (0, 1)$. For every $x \neq y \in M$, there is a unique $k \geq 0$ such that $x - y \in I^k M$ but $x - y \notin I^{k+1} M$. We can define a metric on M by

$$d(x, y) \coloneqq r^k.$$

This metric induces the I-adic topology on M.

To analyze the I-adic separation property of M, the following Artin-Rees Lemma is particularly useful.

Theorem 1.6.4 (Artin-Rees Lemma)**.** Let A be a noetherian ring, I an ideal of A, M a finite A-module and N a submodule of M. Then there exists an integer r such that for all $n \geq 0$, we have

$$(I^{r+n}M) \cap N = I^n(I^rM \cap N).$$

Proof. Let

$$A' := A \oplus IX \oplus I^2X^2 \oplus \cdots \subset A[X]$$

be a graded A-algebra. Note that if $I = (a_1, \dots, a_k)$, then $A' = A[a_1X, \dots, a_kX]$. Hence A' is a noetherian ring. Let

$$M' := M \oplus IMX \oplus I^2MX^2 \oplus \cdots$$

be a graded A'-module. Then M' is a finite A'-module since it is generated by M and M is finite over A. Let

$$N' \coloneqq N \oplus (IM \cap N)X \oplus (I^2M \cap N)X^2 \oplus \cdots$$

be a graded submodule of M'. Then N' is finite over A'. Suppose $N' = \sum A'x_i$ with $x_i \in I^{d_i}M \cap N$. Choose $r \geq d_i$ for all i. Then the degree $n+r$ part of N' is equal to degree n part of A' timing the degree r part of N'. That is, for all $n \geq 0$, $I^{n+r}M \cap N = I^n(I^rM \cap N)$. □

Corollary 1.6.5. Let A be a noetherian ring, I an ideal of A, M a finite A-module and N a submodule of M. Then the subspace topology on N induced by $N \subset M$ coincides with the I-adic topology on N.

Proof. This is a direct consequence of the Artin-Rees Lemma. □

Corollary 1.6.6. Let A be a noetherian ring, I an ideal of A, and M a finite A-module. Let $N = \bigcap_{n\geq 0} I^nM$. Then $IN = N$. In particular, if $I \subset \operatorname{rad}(A)$, then M is I-adically separated.

Proof. We have that

$$N = I^{n+r}M \cap N = I^n(I^rM \cap N) = I^nN \subset IN \subset N.$$

The latter conclusion follows from the Nakayama's Lemma. □

Definition 1.6.7. Let A be a ring, I an ideal of A and M an A-module. We say that M is *complete (with respect to I-adic topology)* if M is I-adically separated and complete as a metric space with respect to the metric induced by the I-adic topology.

Lemma 1.6.8. Let A be a ring, I an ideal of A and M an A-module. Then the inverse limit

$$\widehat{M} \coloneqq \varprojlim(\cdots \to M/I^nM \to M/I^{n-1}M \to \cdots \to M/IM)$$

exists in the category of A-modules. Moreover, $\widehat{A}$ is an A-algebra and $\widehat{M}$ is an $\widehat{A}$-module.

Proof. Let
$$\widehat{M} := \left\{ (x_n) \in \prod_{n\geq 0} M/I^nM \middle| x_{n+1} \mapsto x_n \right\}.$$
We claim that $\widehat{M}$ is that we desired. Yang: To be completed. □

Definition 1.6.9 (Formal Completion)**.** Let A be a ring, I an ideal of A and M an A-module. The *formal completion* of M with respect to I, denoted by $\widehat{M}$, is defined as
$$\widehat{M} := \varprojlim(\cdots \to M/I^nM \to M/I^{n-1}M \to \cdots \to M/IM),$$
where the maps are the natural projections $M/I^nM \to M/I^{n-1}M$.

Example 1.6.10. Let $A = \mathbb{Z}$ be the ring of integers and $I = p\mathbb{Z}$. The formal completion of $\mathbb{Z}$ with respect to $p\mathbb{Z}$ is the ring of p-adic integers, denoted by $\mathbb{Z}_p$. The elements of $\mathbb{Z}_p$ can be represented as infinite series of the form
$$a_0 + a_1p + a_2p^2 + \cdots,$$
where $a_i \in \{0, 1, \ldots, p-1\}$.

Example 1.6.11. Let R be a ring, $A = R[X_1, \ldots, X_n]$ and $I = (X_1, \ldots, X_n)$. The formal completion of A with respect to I is the ring of formal power series $R[[X_1, \ldots, X_n]]$. The elements of $R[[X_1, \ldots, X_n]]$ can be represented as infinite series of the form
$$\sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n},$$
where $a_{i_1,\ldots,i_n} \in R$ and the multi-index $(i_1, \ldots, i_n)$ runs over all non-negative integers.

Proposition 1.6.12. The formal completion $\widehat{M}$ of a A-module M is complete, and image of M is dense in $\widehat{M}$. Moreover, $\widehat{M}$ is uniquely characterized by above properties.

Proof. Yang: To be completed. □

By the universal property of the inverse limit, we get a covariant functor from the category of A-modules to the category of topological $\widehat{A}$-modules, which sends an A-module M to $\widehat{M}$ and a morphism $f : M \to N$ to the induced morphism $\widehat{f} : \widehat{M} \to \widehat{N}$.

Lemma 1.6.13. Let
$$0 \to M_1 \to M_2 \to M_3 \to 0$$
be an exact sequence of finite A-modules. Then the sequence of $\widehat{A}$-modules
$$0 \to \widehat{M_1} \to \widehat{M_2} \to \widehat{M_3} \to 0$$
is still exact.

Proof. Yang: To be completed. □

Proposition 1.6.14. Let $\widehat{A}$ be completion of a noetherian ring A with respect to an ideal I and M a finite A-module. Then the natural map $M \otimes_A \widehat{A} \to \widehat{M}$ is an isomorphism.

Proof. Since A is noetherian and M is finite, we have an exact sequence

$$A^m \to A^n \to M \to 0.$$

By Lemma 1.6.13, we have an exact sequence

$$\widehat{A^m} \to \widehat{A^n} \to \widehat{M} \to 0.$$

On the other hand, we have

$$A^m \otimes_A \widehat{A} \to A^n \otimes_A \widehat{A} \to M \otimes_A \widehat{A} \to 0$$

by right exactness of the tensor product. Since the inverse limit commutes with finite direct sums, we complete the proof by the Five Lemma. □

Proposition 1.6.15. Let A be a noetherian ring and I an ideal of A. Then the formal completion $\widehat{A}$ of A with respect to I is a flat A-module.

Proof. This is a direct consequence of Lemma 1.6.13 and Proposition 1.6.14. □

Lemma 1.6.16. Let $\widehat{A}$ be the formal completion of a noetherian ring A with respect to an ideal I. Suppose that I is generated by $a_1, \dots, a_n$. Then we have an isomorphism of topological rings

$$\widehat{A} \cong A[[X_1, \dots, X_n]]/(X_1 - a_1, \cdots, X_n - a_n).$$

Proof. Yang: To be completed. □

Proposition 1.6.17. Let A be a noetherian ring and I an ideal of A. Then the formal completion $\widehat{A}$ of A with respect to I is a noetherian ring.

Proof. Note that $A[[X_1, \dots, X_n]]$ is noetherian by Hilbert's Basis Theorem. Then the conclusion follows from Lemma 1.6.16. □

Proposition 1.6.18. Let A be a noetherian ring and $\mathfrak{m}$ a maximal ideal of A. Then the formal completion $\widehat{A}$ of A with respect to $\mathfrak{m}$ is a local ring with maximal ideal $\mathfrak{m}\widehat{A}$.

Proof. Yang: To be completed. □

1.6.2 Complete local rings

Let $(A, \mathfrak{m}, \mathbf{k})$ be a noetherian complete local ring with respect to the $\mathfrak{m}$-adic topology. We say that A is *of equal characteristic* if $\operatorname{char} A = \operatorname{char} \mathbf{k}$, and *of mixed characteristic* if $\operatorname{char} A \neq \operatorname{char} \mathbf{k}$. In latter case, $\operatorname{char} \mathbf{k} = p$ and $\operatorname{char} A = 0$ or $\operatorname{char} A = p^k$.

The goal of this subsection is the following structure theorem for noetherian complete local rings due to Cohen.

Theorem 1.6.19 (Cohen Structure Theorem)**.** Let $(A, \mathfrak{m}, \mathbf{k})$ be a noetherian complete local ring of dimension d. Then

(a) A is a quotient of a noetherian regular complete local ring;

(b) if A is regular and of equal characteristic, then $A \cong \mathbf{k}[[X_1, \dots, X_d]]$;

(c) if A is regular, of mixed characteristic $(0, p)$ and $p \notin \mathfrak{m}^2$, then $A \cong D[[X_1, \dots, X_{d-1}]]$, where $(D, p, \mathbf{k})$ is a complete DVR;

(d) if A is regular, of mixed characteristic $(0, p)$ and $p \in \mathfrak{m}^2$, then $A \cong D[[X_1, \dots, X_d]]/(f)$, where $(D, p, \mathbf{k})$ is a complete DVR and f a regular parameter.

To prove the Cohen Structure Theorem, we first list some preliminary results on complete local rings. They are independently important and can be used in other contexts.

Theorem 1.6.20 (Hensel's Lemma)**.** Let $(A, \mathfrak{m}, \mathbf{k})$ be a complete local ring, $f \in A[X]$ a monic polynomial and $\overline{f} \in \mathbf{k}[X]$ its reduction modulo $\mathfrak{m}$. Suppose that $\overline{f} = \overline{g} \cdot \overline{h}$ for some monic polynomials $\overline{g}, \overline{h} \in \mathbf{k}[X]$ such that $\gcd(\overline{g}, \overline{h}) = 1$. Then the factorization lifts to a unique factorization $f = g \cdot h$ in $A[X]$ such that g and h are monic polynomials.

Proof. Lift $\overline{g}$ and $\overline{h}$ to monic polynomials $g_1, h_1 \in A[X]$. We inductively construct a sequence of monic polynomials $g_n, h_n \in A[X]$ such that $\Delta_n = f - g_n h_n \in \mathfrak{m}^n[X]$ and $g_n - g_{n+1}, h_n - h_{n+1} \in \mathfrak{m}^n[X]$ for all $n \geq 1$. Suppose that g_n and h_n are constructed. Let $g_{n+1} = g_n + \varepsilon_n$ and $h_{n+1} = h_n + \eta_n$ for $\varepsilon_n, \eta_n \in \mathfrak{m}^n[X]$. Then we have

$$f - g_{n+1} h_{n+1} = \Delta_n - (\varepsilon_n h_n + \eta_n g_n) + \varepsilon_n \eta_n.$$

Hence we just need to choose ε_n and η_n such that

$$\varepsilon_n h_n + \eta_n g_n \equiv \Delta_n \mod \mathfrak{m}^{n+1}, \quad \deg \varepsilon_n < \deg g_n, \quad \deg \eta_n < \deg h_n.$$

Since $\gcd(\overline{g}, \overline{h}) = 1$, there exist $\overline{u}, \overline{v} \in \mathbf{k}[X]$ such that $\overline{u}\overline{g} + \overline{v}\overline{h} = 1$ and $\deg \overline{u} < \deg \overline{g}$, $\deg \overline{v} < \deg \overline{h}$. Lift $\overline{u}$ and $\overline{v}$ to $u, v \in A[X]$ preserving the degrees. Then we have $ug_n + vh_n \equiv 1 \mod \mathfrak{m}$. Let $\varepsilon_n = u\Delta_n$ and $\eta_n = v\Delta_n$. Then we get the desired equation. □

Proposition 1.6.21. Let $(A, \mathfrak{m}, \mathbf{k})$ be a noetherian complete local ring and M an A-module that is $\mathfrak{m}$-adically separated. Suppose $\dim_{\mathbf{k}} M/\mathfrak{m}M < \infty$. Then the basis of $M \otimes_A \mathbf{k}$ as $\mathbf{k}$-vector space can be lifted to a generating set of M as an A-module.

Proof. Let $t_1, \dots, t_n \in M$ such that their images in $M/\mathfrak{m}M$ form a basis of $M/\mathfrak{m}M$ as a $\mathbf{k}$-vector space. Then $M = t_1 A + \cdots + t_n A + \mathfrak{m}M$. For every $x \in M$, we can write

$$x = a_{0,1} t_1 + \cdots + a_{0,n} t_n + m_1$$

for some $a_{0,i} \in A$ and $m_1 \in \mathfrak{m}M$. Inductively, we have $\mathfrak{m}^k M = t_1 \mathfrak{m}^k + \cdots + t_n \mathfrak{m}^k + \mathfrak{m}^{k+1} M$. Suppose that we have constructed $m_k \in \mathfrak{m}^k M$. Then we can write

$$m_k = a_{k,1}t_1 + \cdots + a_{k,n}t_n + m_{k+1}.$$

Note that $\sum_{k\geq 0} a_{k,i}$ converges in A, denote its limit by a_i. Then we have

$$x - a_1t_1 + \cdots + a_nt_n = \sum_{i=1}^{n}\sum_{r\geq k} a_{r,i}t_i + m_k \in \mathfrak{m}^k M$$

for all k. Since M is $\mathfrak{m}$-adically separated, $x = a_1t_1 + \cdots + a_nt_n$. It follows that $M = \sum At_i$. □

The key to prove the Cohen Structure Theorem is the existence of coefficient rings.

Definition 1.6.22 (Coefficient rings)**.** Let $(A, \mathfrak{m}, \mathbf{k})$ be a noetherian complete local ring.
When A is equal-characteristic, the coefficient ring (or coefficient field) is a homomorphism of rings $\mathbf{k} \to A$ such that $\mathbf{k} \to A \to A/\mathfrak{m}$ is an isomorphism.
When A is mixed-characteristic, the coefficient ring is a complete local ring $(R, pR, \mathbf{k})$ with a local homomorphism of rings $R \hookrightarrow A$ such that the induced homomorphism $R/pR \to A/\mathfrak{m}$ is an isomorphism.

Remark 1.6.23. Recall that a homomorphism of local rings $f : (A, \mathfrak{m}_A) \to (B, \mathfrak{m}_B)$ is said to be local if $f^{-1}(\mathfrak{m}_B) = \mathfrak{m}_A$.

Theorem 1.6.24. Every noetherian complete local ring $(A, \mathfrak{m}, \mathbf{k})$ has a coefficient ring.

Assume the existence of coefficient rings, we can prove the Cohen Structure Theorem.

Proof of Cohen Structure Theorem. Let R be a coefficient ring of A and $\mathfrak{m} = (f_1, \ldots, f_d)$ a minimal generating set of $\mathfrak{m}$. Then we have a homomorphism of complete local rings

$$\Phi : R[[X_1, \ldots, X_d]] \to A, \quad X_i \mapsto f_i.$$

Let $\mathfrak{n}$ be the maximal ideal of $R[[X_1, \ldots, X_d]]$. Then $\mathfrak{n}A = \mathfrak{m}$. By Proposition 1.6.21, A is generated by 1 as an $R[[X_1, \ldots, X_d]]$-module. This implies that Φ is surjective and (a) follows.

If A is regular of equal characteristic, then $\mathfrak{m}$ is generated by a regular sequence. By consider the dimension of $R[[X_1, \ldots, X_d]]$ and A, we have that Φ is an isomorphism. This proves (b).

Note that if A is regular of mixed characteristic $(0, p)$ and $p \notin \mathfrak{m}^2$, then $\mathfrak{m}$ is generated by $p, f_1, \ldots, f_{d-1}$. Then consider the homomorphism of complete local rings

$$R[[X_1, \ldots, X_{d-1}]] \to A, \quad X_i \mapsto f_i.$$

By the same argument as above, we have that it is an isomorphism. This proves (c).

For (d), we have that $\ker \Phi$ is of height 1 by the dimension argument. Since regular local rings are UFDs, we can write $\ker \Phi = (f)$ for some $f \in R[[X_1, \ldots, X_d]]$. Then we finish. □

Existence of coefficient rings

Proof of Theorem 1.6.24 in characteristic 0. Note that for any $n \in \mathbb{Z}$, $n \notin \mathfrak{m}$. Hence $\mathbb{Q} \subset A$. Let $\Sigma := \{\text{subfield in } A\}$ and K a maximal element in Σ with respect to the inclusion. The set Σ is non-empty since $\mathbb{Q} \in \Sigma$. By Zorn's Lemma, K exists. Then K is a subfield of $\mathbf{k}$ by $K \hookrightarrow A \twoheadrightarrow A/\mathfrak{m} \cong \mathbf{k}$. We claim that K is a coefficient field of A.

Suppose there is $\bar{t} \in \mathbf{k} \setminus K$. If $\bar{t}$ is transcendent over K, lift $\bar{t}$ to an element $t \in A$. Then for any polynomial $f \neq 0 \in K[T]$, we have $f(\bar{t}) \neq 0 \in \mathbf{k}$. Hence $f(t) \notin \mathfrak{m}$. This implies that $1/f(t) \in A$, whence $K(t) \subset A$. This contradicts the maximality of K. If $\bar{t}$ is algebraic over K, let $f \in K[T]$ be the minimal polynomial of $\bar{t}$. Then f is irreducible in $K[T]$ and $f(\bar{t}) = 0$. Regard f as a polynomial in $A[T]$ by $K \hookrightarrow A$. Note that $\operatorname{char} A = 0$ implies that f is separable. By Hensel's Lemma (Theorem 1.6.20), we can lift the root $\bar{t}$ to an element $t \in A$ such that $f(t) = 0$. Then $K(t)$ is a field extension of K and $K(t) \subset A$. This contradicts the maximality of K again. □

The same strategy does not work when $\operatorname{char} \mathbf{k} = p > 0$ since there might be inseparable extensions. To fix this, we need to introduce the notion of p-basis.

Definition 1.6.25. Let $\mathbf{k}$ be a field of characteristic p. A finite set $\{t_1, \dots, t_n\} \subset \mathbf{k} \setminus \mathbf{k}^p$ is called *p-independent* if $[\mathbf{k}(t_1, \dots, t_n) : \mathbf{k}] = p^n$. A set $\Theta \subset \mathbf{k} \setminus \mathbf{k}^p$ is called a *p-independent* if its any finite subset is p-independent. A *p-basis* for $\mathbf{k}$ is a maximal p-independent set $\Theta \subset \mathbf{k} \setminus \mathbf{k}^p$.

By definition, we have that $\mathbf{k} = \mathbf{k}^p[\Theta]$ for any p-basis Θ of $\mathbf{k}$. For any $a \in \mathbf{k}$ and $\theta \in \Theta$, we can write a as a polynomial in Θ with coefficients in $\mathbf{k}^p$. The degree of θ in such polynomial representation is at most $p - 1$. Such polynomial representation is unique by definition of p-independence.

Applying the Frobenius map n times, we have that $\mathbf{k}^{p^n} = \mathbf{k}^{p^{n+1}}[\Theta^{p^n}]$. This follows that $\mathbf{k} = \mathbf{k}^{p^n}[\Theta]$ for all n. Moreover, for any $a \in \mathbf{k}$ and $\theta \in \Theta$, we can write a as a polynomial in Θ with coefficients in $\mathbf{k}^{p^n}$ and the degree of θ is at most $p^n - 1$. Such polynomial representation is unique.

Let $\mathbf{k}$ be a perfect field of characteristic p. If there is $a \in \mathbf{k} \setminus \mathbf{k}^p$, then $\mathbf{k}(a^{1/p})/\mathbf{k}$ is an inseparable extension. This contradicts the perfectness of $\mathbf{k}$. Hence $\mathbf{k} = \mathbf{k}^p$ and $\mathbf{k}$ has no nonempty p-basis.

Example 1.6.26. Let $\mathbf{k} = \mathbb{F}_p(t_1, \dots, t_n)$. Then $\mathbf{k}^p = \mathbb{F}_p(t_1^p, \dots, t_n^p)$. The set $\{t_1, \dots, t_n\}$ is a p-basis for $\mathbf{k}$.

Proof of Theorem 1.6.24 in characteristic p. Choose $\Theta \subset A$ such that its image in $A/\mathfrak{m}$ is a p-basis for $\mathbf{k}$. Let $A_n := A^{p^n} = \{a^{p^n} : a \in A\}$ and $K := \bigcap_{n \geq 0}(A_n[\Theta])$. Then we claim that K is a coefficient field of A.

First we show that $A_n[\Theta] \cap \mathfrak{m} \subset \mathfrak{m}^{p^n}$. For every $a \in A_n[\Theta]$, if the degree of θ in the polynomial representation of a is more than $p^n - 1$, we can write $\theta^k = \theta^{ap^n} \cdot \theta^b$ for some $b < p^n$. Regard $\theta^{ap^n} \in A^{p^n}$ as coefficients. Now assume that $a \in A_n[\Theta] \cap \mathfrak{m}$. Then consider the image of a in $A/\mathfrak{m}$. The image of a equals 0 implies every coefficient of a is in $\mathfrak{m}$. Such coefficients are of form b^{p^n} for some $b \in A$, whence $b \in \mathfrak{m}$. Hence $a \in \mathfrak{m}^{p^n}$. This implies that $K \cap \mathfrak{m} = \bigcap_{n \geq 0}(A_n[\Theta] \cap \mathfrak{m}) \subset \bigcap_{n \geq 0} \mathfrak{m}^{p^n} = \{0\}$. Then K is a field and hence a subfield of $\mathbf{k}$.

For any $\overline{a} \in \mathbf{k}$, note that $\mathbf{k} = \mathbf{k}^p[\overline{\Theta}] = \mathbf{k}^{p^2}[\overline{\Theta}] = \cdots = \mathbf{k}^{p^n}[\overline{\Theta}] = \cdots$. For every n, write

$$\overline{a} = \sum_{\mu_n} \overline{c}_{\mu_n}^{p^n} \mu_n =: P_{\overline{a},n}(\overline{c}_{\mu_n}),$$

where μ_n runs over all monomials in $\overline{\Theta}$ with degree at most $p^n - 1$ and $\overline{c}_{\mu_n} \in \mathbf{k}$. We call this representation the p^n-development of $\overline{a}$ with respect to $\overline{\Theta}$. Plug the p^m-development of c_{μ_n} into $P_{\overline{a},n}$, we get the p^{n+m}-development of $\overline{a}$. In formula, that is,

$$P_{\overline{a},n}(P_{\overline{a},m}(\overline{c}_{\mu_{n+m}})) = P_{\overline{a},n+m}(\overline{c}_{\mu_{n+m}}).$$

Lift $\overline{c}_{\mu_n}$ to $c_{\mu_n} \in A$ for all μ_n. Let $a_n := P_{\overline{a},n}(c_{\mu_n}) = \sum_{\mu_n} c_{\mu_n}^{p^n}\mu_n \in A_n[\Theta]$. For $m \geq n$, we have $a_n - a_m \in A_n[\Theta] \cap \mathfrak{m} \subset \mathfrak{m}^{p^n}$. Hence a_n converges to an element $a \in A$. Now we show that $a \in K$. For every μ_k, let $b_{\mu_k,n} \in A$ be the element getting by plugging $c_{\mu_{n+k}}$ into the $P_{\overline{c}_{\mu_k},n}$. Then $b_{\mu_k,n}$ converges to an element $b_{\mu_k} \in A$. By construction, we have

$$a = \lim_{n\to\infty} P_{\overline{a},n+k}(c_{\mu_{n+k}}) = \lim_{n\to\infty} P_{\overline{a},k}(b_{\mu_k,n}) = P_{\overline{a}}(b_{\mu_k}) = \sum_{\mu_k} b_{\mu_k}^{p^k}\mu_k \in A_k[\Theta], \quad \forall k.$$

It follows that $a \in K$. □

Lemma 1.6.27. Let $(A, \mathfrak{m}, \mathbf{k})$ be a noetherian complete local ring of mixed characteristic. Suppose that $\mathfrak{m}^n = 0$ for some $n \geq 1$. Then there exists a complete local ring $(R, pR, \mathbf{k})$ with $R \subset A$.

Proof. Fix a p-basis of $\mathbf{k}$ and lift it to $\Theta \subset R$. Let $q = p^{n-1}$ and

$$m := \left\{\theta_1^{k_1} \cdots \theta_d^{k_d} \mid \theta_i \in \Theta, k_i \leq q-1\right\}, \quad S := \left\{ \sum_{\mu\in m,\ \text{finite}} a_\mu \mu \middle| a_\mu \in R^q \right\}.$$

For any $a, b \in A$, we claim that $a \equiv b \mod \mathfrak{m}$ if and only if $a^q \equiv b^q \mod \mathfrak{m}^n$. If $a \equiv b \mod \mathfrak{m}$, write $a = b + m$ for some $m \in \mathfrak{m}$. Then $a^p = b^p + pb^{q-1}m + \cdots + m^q$. Hence $a^p \equiv b^p \mod \mathfrak{m}^2$. Inductively, we have $a^q \equiv b^q \mod \mathfrak{m}^n$. Conversely, if $a^q \equiv b^q \mod \mathfrak{m}^n$, then $a^q - b^q \in \mathfrak{m}^n \subset \mathfrak{m}$. Note that the Frobenius map $x \mapsto x^q$ is injective on $A/\mathfrak{m}$. It follows that $a \equiv b \mod \mathfrak{m}$. By the claim, S maps to $\mathbf{k}^q[\Theta] = \mathbf{k}$ bijectively.

Let

$$R := S + pS + p^2S + \cdots + p^{n-1}S.$$

We claim that R is a subring of A. If so, $R/pR \cong \mathbf{k}$ and we get a complete local ring $(R, pR, \mathbf{k})$.

Take $a, b \in A$. We have

$$a^q + b^q = (a+b)^q + pc \in A^q + pA.$$

Inductively, we have

$$a^q + b^q \in A^q + pA^q + \cdots + p^{n-1}A^q.$$

This implies that R is closed under addition. Note that $\theta^a = \theta^{aq} \cdot \theta^b$ with $b < q$. Then for any $\mu, \nu \in m$, we have $\mu\nu \in S$. Hence R is closed under multiplication. □

Lemma 1.6.28. Let $\mathbf{k}$ be a field of characteristic p. Then there exists a DVR $(D, p, \mathbf{k})$ of mixed characteristic $(0, p)$.

Proof. Fix a well order $\leq$ on $\mathbf{k}$ and for any $a \in \mathbf{k}$, set $\mathbf{k}_a$ be the subfield of $\mathbf{k}$ generated by all elements $b \in \mathbf{k}$ such that $b \leq a$. Then $\mathbf{k} = \bigcup_{a \in \mathbf{k}} \mathbf{k}_a$. We construct DVRs D_a with residue field $\mathbf{k}_a$ such that $D_a \subset D_b$ for $a \leq b$. Begin from $\mathbf{k}_0 = \mathbb{F}_p$ and let $D_0 = \mathbb{Z}_{(p)}$. Suppose that D_a is constructed for all $a < b$. If $\mathbf{k}_b/\mathbf{k}_a$ is transcendental, then let D_b be the localization of $D_a[b]$ at the prime ideal generated by p.

If $\mathbf{k}_b/\mathbf{k}_a$ is algebraic, then let $\overline{f} \in \mathbf{k}_a[T]$ be the monic minimal polynomial of b. Let $\mathbf{K}_a = \mathrm{Frac}(D_a)$ and $K_b = \mathbf{K}_a[T]/(f)$, where f is a monic lift of $\overline{f}$ to $D_a[T]$. Note that f is irreducible since $\overline{f}$ is irreducible. Let D_b be the integral closure of D_a in K_b. In general, D_b is a Dedekind domain. Consider the prime factorization $pD_b = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$ in D_b. For every i, $D_b/\mathfrak{p}_i$ is a field extension of $\mathbf{k}_a$ and $\overline{f}$ has a root in $D_b/\mathfrak{p}_i$. Suppose $\deg \overline{f} = \deg f = d$. It follows that $[(D_b/\mathfrak{p}_i) : \mathbf{k}_a] = d$. Note that we have $\sum_{i=1}^k e_i f_i = [\mathbf{K}_b : \mathbf{K}_a] = d$. Hence $k = 1$ and $e_1 = 1$. It follows that pD_b is prime and D_b is a DVR with residue field $\mathbf{k}_b$.

Let $D = \bigcup_{a \in \mathbf{k}} D_a$. Then $(D, pD, \mathbf{k})$ is the desired DVR. □

Example 1.6.29. Let $\mathbf{k} = \mathbb{F}_p(t)$. Then $D = \mathbb{Z}[t]_{(p)}$ is a DVR satisfying the condition in Lemma 1.6.28.

Let $\mathbf{k} = \overline{\mathbb{F}_p}$. For any $n \geq 1$, let $K_n = K_{n-1}(\zeta_{p^n - 1})$ and $K_0 = \mathbb{Q}$. Let $D_n := \mathscr{O}_{K_n, \mathfrak{p}_n}$ be the localization of the ring of integers of K_n at the prime $\mathfrak{p}_n$ lying above $\mathfrak{p}_{n-1}$. Then $D := \bigcup_n D_n$ is a DVR with residue field $\mathbf{k}$.

Lemma 1.6.30. Given $\mathbf{k}$ a field of characteristic p, there exists a unique complete local ring $(R, pR, \mathbf{k})$ of mixed characteristic (p^n, p).

Proof. The existence follows from Lemma 1.6.28. To show the uniqueness, suppose that $(R', pR', \mathbf{k})$ is another complete local ring of mixed characteristic (p^n, p). Fix a p-basis of $\mathbf{k}$ and lift it to $\Theta \subset R$ and $\Theta' \subset R'$ relatively. Let $q = p^{n-1}$ and

$$m := \left\{ \theta_1^{k_1} \cdots \theta_d^{k_d} \mid \theta_i \in \Theta, k_i \leq q - 1 \right\}, \quad S := \left\{ \sum_{\mu \in m,\ \text{finite}} a_\mu \mu \,\middle|\, a_\mu \in R^q \right\}.$$

Define m', S' similarly with Θ' and R'. Since $S \to R \to \mathbf{k}$ and $S' \to R' \to \mathbf{k}$ are bijections, we can define a bijective map $\Phi : S \to S'$.

Note that any element in S can be written as $s + pr$ with $s \in S$ and $r \in R$ uniquely since $S \to \mathbf{k}$ is bijective. Inductively, we can write any element in R as

$$r = s + ps_1 + p^2 s_2 + \cdots + p^{n-1} s_{n-1},$$

where $s_i \in S$. The similarly for R'. Extend Φ to R and we get a bijection between R and R'. Note that by construction, Φ preserves addition and multiplication. Hence we get a ring isomorphism $\Phi : R \to R'$. □

Proof of Theorem 1.6.24 in mixed characteristic. Since A is complete, we have $A = \varprojlim_n A/\mathfrak{m}^n$. By Lemma 1.6.27, there is a complete local ring $(R_n, pR_n, \mathbf{k})$ with $R_n \subset A/\mathfrak{m}^n$. By Lemma 1.6.30, such R_n is unique up to isomorphism. It follows that $R_n \cong R_m/p^{k_n}$ for $m \geq n$. We get an inverse system

$$\cdots \to R_n \to R_{n-1} \to \cdots \to R_1 \cong \mathbf{k}.$$

Let $R := \varprojlim_n R_n$. Then $(R, pR, \mathbf{k})$ is a complete local ring. The homomorphisms $R_n \hookrightarrow A/\mathfrak{m}^n$ induce a homomorphism of complete local rings $R \hookrightarrow A$. This concludes the proof. $\square$

Chapter 2

Homological Algebra

2.1 Complexes and Homology

Definition 2.1.1. Let $A_\bullet$ and $B_\bullet$ be two complexes in $\mathcal{A}$ and $\varphi_\bullet, \psi_\bullet : A_\bullet \to B_\bullet$ be two morphisms of complexes. A *homotopy* between $\varphi_\bullet$ and $\psi_\bullet$ is a collection of morphisms $h_n : A_n \to B_{n-1}$ such that

$$\varphi_n - \psi_n = \mathrm{d}_{B_{n+1}} \circ h_n + h_{n-1} \circ \mathrm{d}_{A_n}.$$

In diagram, we have

$$\begin{tikzcd}
\cdots \arrow[r] & A_{n+1} \arrow[r] & A_n \arrow[r, "\mathrm{d}_{A_n}"] \arrow[dl, "h_n"'] \arrow[d, shift right, "\psi_n"'] \arrow[d, shift left, "\varphi_n"] & A_{n-1} \arrow[r] \arrow[dl, "h_{n-1}"] & \cdots . \\
\cdots \arrow[r] & B_{n+1} \arrow[r, "\mathrm{d}_{B_{n+1}}"] & B_n \arrow[r] & B_{n-1} \arrow[r] & \cdots
\end{tikzcd}$$

2.2 Derived Functors

In this section, fix an abelian category $\mathcal{A}$.

2.2.1 Resolution

Definition 2.2.1 (Resolution)**.** Let $A \in \mathcal{A}$. A *projective resolution* (resp. *flat resolution, free resolution*) of A is an exact sequence

$$\cdots \to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to A \to 0,$$

where each P_i is a projective (resp. flat, free) object in $\mathcal{A}$.
An *injective resolution* of A is an exact sequence

$$0 \to A \to I^0 \to I^1 \to I^2 \to \cdots \to I^n \to \cdots,$$

where each I^i is an injective object in $\mathcal{A}$.

Proposition 2.2.2. Let $P_\bullet : \cdots \to P_1 \to P_0 \to A \to 0$ and $Q_\bullet : \cdots \to Q_1 \to Q_0 \to B \to 0$ be complexes in $\mathcal{A}$ such that P_i is projective and $Q_\bullet$ is exact. Given a morphism $f : A \to B$, there exists a morphism of complexes $f_\bullet : P_\bullet \to Q_\bullet$ such that $f_0 = f$. In particular, any two such morphism of complexes are homotopic.
Dually, let $I^\bullet : 0 \to A \to I^0 \to I^1 \to \cdots$ and $J^\bullet : 0 \to B \to J^0 \to J^1 \to \cdots$ be complexes in $\mathcal{A}$ such that J^i is injective and $I^\bullet$ is exact. Given a morphism $f : A \to B$, there exists a morphism of complexes $f^\bullet : I^\bullet \to J^\bullet$ such that $f^0 = f$. In particular, any two such morphism of complexes are homotopic.

Proof. Yang: To be completed. □

Definition 2.2.3. For an object $A \in \mathcal{A}$, the *projective dimension* of A, denoted $\operatorname{proj.dim} A$, is the smallest integer n such that there exists a projective resolution

$$0 \to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to A \to 0$$

of A of length n. If no such n exists, we set $\operatorname{proj.dim} A = \infty$.
Dually, the *injective dimension* of A, denoted $\operatorname{inj.dim} A$, is the smallest integer n such that there exists an injective resolution

$$0 \to A \to I^0 \to I^1 \to \cdots \to I^{n-1} \to I^n \to 0$$

of A of length n. If no such n exists, we set $\operatorname{inj.dim} A = \infty$.

2.3 Applications to Commutative Algebra

2.3.1 Homological dimension

Lemma 2.3.1. Let A be a ring and M an A-module. Then

$$\sup_M \operatorname{proj.dim} M = \sup_N \operatorname{inj.dim} N.$$

Proof. Note that

$$\operatorname{proj.dim} M \le n$$

if and only if

$$\operatorname{Ext}^A_{n+1}(M, N) = 0, \quad \forall N.$$

And this is equivalent to

$$\operatorname{inj.dim} N \le n.$$

□

Remark 2.3.2. In fact, for fix N, we have

$$\operatorname{inj.dim} N \le n$$

if and only if

$$\operatorname{Ext}^A_{n+1}(A/I, N) = 0, \quad \forall I$$

By Lemma Yang: ?. Hence we have

$$\sup_{M \text{ finite}} \operatorname{proj.dim} M = \sup_M \operatorname{proj.dim} M = \sup_N \operatorname{inj.dim} N.$$

Definition 2.3.3. Let A be a ring. The *homological dimension* of A, denoted $\operatorname{hl.dim} A$, is defined as

$$\operatorname{hl.dim} A \coloneqq \sup_M \operatorname{proj.dim} M = \sup_M \operatorname{inj.dim} M.$$

Lemma 2.3.4. Let A be a noetherian ring, B a flat A-algebra and M a finite A-module. Then we have

$$\operatorname{Ext}^i_A(M, N) \otimes B \cong \operatorname{Ext}^i_B(M \otimes B, N \otimes M), \quad \forall N.$$

Proof. Yang: To be completed. □

Proposition 2.3.5. Let A be a noetherian ring. Then

$$\operatorname{hl.dim} A = \sup_{\mathfrak{p} \in \operatorname{Spec} A} \operatorname{hl.dim} A_{\mathfrak{p}}.$$

Proof. Compute homological dimension of A using $\operatorname{Ext}^i_A(M, N)$ for finite M. The conclusion follows from Propostion 2.3.4. □

Definition 2.3.6. Let $(A, \mathfrak{m}, \mathbf{k})$ be a noetherian local ring. We say that a homomorphism of A-modules $f : M \to N$ is *minimal* if the induced map $M \otimes \mathbf{k} \to N \otimes \mathbf{k}$ is an isomorphism. Equivalently, f is minimal if and only if f is surjective and $\operatorname{Ker} f \subset \mathfrak{m}M$.

Definition 2.3.7. Let A be a noetherian local ring and M a finite A-module. A *minimal projective resolution* of M is a projective resolution

$$\cdots \to P_n \xrightarrow{d_n} P_{n-1} \xrightarrow{d_{n-1}} \cdots \to P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} M \to 0$$

such that each homomorphism $P_i \to \operatorname{Ker} d_{i-1}$ is minimal.

Proposition 2.3.8. Let $(A, \mathfrak{m}, \mathbf{k})$ be a noetherian local ring and M a finite A-module. Then M has a minimal projective resolution. Moreover, any two minimal projective resolutions of M are isomorphic.

Proof. Suppose $M \otimes_A \mathbf{k} = \bigoplus \mathbf{k} \cdot \overline{x_i}$. Lift x_i to elements of M. Then we have a minimal homomorphism $\mathrm{d}_0 : \bigoplus A \cdot x_i \to M$. Similarly choose minimal homomorphisms $\mathrm{d}_k : A^{n_i} \to \operatorname{Ker} \mathrm{d}_{i-1}$ for $i = 1, 2, \cdots$. This gives a minimal projective resolution.

Suppose we have two minimal homomorphism $f, g : A^n \to M$. After tensoring with $\mathbf{k}$, we have isomorphisms between $f \otimes \mathbf{k}$ and $g \otimes \mathbf{k}$. Lifting to A, we get an homomorphism $\varphi : f \to g$. Here homomorphism between f, g means a homomorphism $A^n \to A^n$ such that $f = g \circ \varphi$. The homomorphism φ is represented by a matrix T. We have $\det T \notin \mathfrak{m}$, whence φ is an isomorphism. □

Proposition 2.3.9. Let $L_\bullet \to M$ be a minimal projective resolution and $P_\bullet$ be an arbitrary projective resolution of M. Then we have $P_\bullet \cong L_\bullet \oplus P'_\bullet$ for some exact complexes $P'_\bullet$.

Proof. By Propostion 2.2.2, we have homomorphism

$$L_\bullet \xrightarrow{\varphi_\bullet} P_\bullet \xrightarrow{\psi_\bullet} L_\bullet.$$

between complexes. By Propostion 2.2.2 again, $T_\bullet := \psi_\bullet \circ \varphi_\bullet$ is homotopic to the identity by $h_\bullet$. Suppose $T_\bullet$ is represented by a matrix. Since $L_\bullet$ is minimal, we have

$$(T - \mathrm{id})(L_n) = (\mathrm{d}_{n+1} \circ h_n + h_{n-1} \circ \mathrm{d}_n)(L_n) \subset \mathfrak{m} L_n.$$

Then $\det T \notin \mathfrak{m}$ and hence $T_\bullet$ is an isomorphism. It follows that $\psi_\bullet$ is surjective, whence it splits $P_\bullet$ into a direct sum $L \oplus P'_\bullet$ since $L_\bullet$ is projective. By the Five Lemma, we see that $P'_\bullet$ is exact. □

Lemma 2.3.10. Let $(A, \mathfrak{m}, \mathbf{k})$ be a noetherian local ring and M a finite A-module. Then $\operatorname{proj.dim} M \leq n$ if and only if $\operatorname{Tor}^A_{n+1}(M, \mathbf{k}) = 0$.

Proof. The necessity is clear. For the sufficiency, we have a minimal projective resolution

$$\cdots \to P_{n+1} \xrightarrow{\mathrm{d}_{n+1}} P_n \xrightarrow{\mathrm{d}_n} P_{n-1} \xrightarrow{\mathrm{d}_{n-1}} \cdots \to P_1 \xrightarrow{\mathrm{d}_1} P_0 \xrightarrow{\mathrm{d}_0} M \to 0.$$

Let $C := \Im \mathrm{d}_n$. Then we have

$$0 \to P_{n+1} \xrightarrow{\mathrm{d}_{n+1}} P_n \xrightarrow{\mathrm{d}_n} C \to 0.$$

Hence $\operatorname{Tor}^A_1(C, \mathbf{k}) \cong \operatorname{Tor}^A_{n+1}(M, \mathbf{k}) = 0$. Let $K = \operatorname{Ker} \mathrm{d}_n$. Then we have the short exact sequence

$$0 \to K \to P_n \to C \to 0.$$

Since $\operatorname{Tor}^A_1(C, \mathbf{k}) = 0$, there is an exact sequence

$$0 \to K \otimes_A \mathbf{k} \to P_n \otimes_A \mathbf{k} \to C \otimes_A \mathbf{k} \to 0.$$

Since $P_n \to C$ is minimal, we have $K \otimes_A \mathbf{k} = 0$. By the Nakayama's lemma, $K = 0$. This implies that $\operatorname{proj.dim} C \leq 0$ and hence $\operatorname{proj.dim} M \leq n$. □

Proposition 2.3.11. Let $(A, \mathfrak{m}, \mathbf{k})$ be a noetherian local ring. Then $\operatorname{hl.dim} A = \operatorname{proj.dim} \mathbf{k}$ (finite or infinite).

Proof. The inequality $\operatorname{hl.dim} A \geq \operatorname{proj.dim} \mathbf{k}$ is by definition. Conversely, we can compute $\operatorname{Tor}^A_{n+1}(M, \mathbf{k})$ using minimal projective resolution of $\mathbf{k}$ for any finite A-module M. By Lemma 2.3.10, we have $\operatorname{proj.dim} M \leq n$ if and only if $\operatorname{Tor}^A_{n+1}(M, \mathbf{k}) = 0$. This implies that $\operatorname{proj.dim} M \leq n$ for all finite A-modules M if $\operatorname{proj.dim} \mathbf{k} = n$. By Remark 2.3.2, we have $\operatorname{hl.dim} A \leq n$. □

Proposition 2.3.12. Let $(A, \mathfrak{m})$ be a noetherian local ring and M a finite A-module. Let $a \in \mathfrak{m}$ be an M-regular element. Then $\operatorname{proj.dim} M/aM = \operatorname{proj.dim} M + 1$. Here we set $\infty + 1 = \infty$.

Proof. We have an exact sequence

$$0 \to M \xrightarrow{*a} M \to M/aM \to 0.$$

Take the long exact sequence with respect to $\operatorname{Tor}(-, \mathbf{k})$, we get

$$\cdots \to \operatorname{Tor}^A_{i+1}(M, \mathbf{k}) \to \operatorname{Tor}^A_{i+1}(M/aM, \mathbf{k}) \to \operatorname{Tor}^A_i(M, \mathbf{k}) \xrightarrow{*a} \operatorname{Tor}^A_i(M, \mathbf{k}) \to \cdots$$

Since the derived homomorphism of $*a$ is zero, we have $\operatorname{Tor}^A_{i+1}(M/aM, \mathbf{k}) = 0$ if and only if $\operatorname{Tor}^A_i(M, \mathbf{k}) = 0$. By Lemma 2.3.10, we have $\operatorname{proj.dim} M/aM = \operatorname{proj.dim} M + 1$. □

2.3.2 Depth and regularity by homological algebra

Proposition 2.3.13. Let $(A, \mathfrak{m}, \mathbf{k})$ be a noetherian local ring and M a finite A-module. Then

$$\operatorname{depth} M := \inf\{i : \operatorname{Ext}^i_A(\mathbf{k}, M) \neq 0\}.$$

Proof. Let $a \in \mathfrak{m}$ be M-regular and $N = M/aM$. Then we claim that

$$\inf\{i : \operatorname{Ext}^i_A(\mathbf{k}, N) \neq 0\} = \inf\{i : \operatorname{Ext}^i_A(\mathbf{k}, M) \neq 0\} - 1.$$

Indeed, we have an exact sequence

$$0 \to M \xrightarrow{a} M \to N \to 0.$$

It induces a long exact sequence

$$\cdots \to \operatorname{Ext}^{i-1}_A(\mathbf{k}, M) \to \operatorname{Ext}^{i-1}_A(\mathbf{k}, N) \to \operatorname{Ext}^i_A(\mathbf{k}, M) \xrightarrow{\operatorname{Ext}^i_A(\mathbf{k}, \operatorname{Mult}_a)} \operatorname{Ext}^i_A(\mathbf{k}, M) \to \cdots.$$

Note that $a \in \mathfrak{m}$, then $\operatorname{Ext}^i_A(\mathbf{k}, \operatorname{Mult}_a) = 0$. It follows that when $\operatorname{Ext}^{i-1}_A(\mathbf{k}, M) = 0$, we have $\operatorname{Ext}^{i-1}_A(\mathbf{k}, N) = 0$ iff $\operatorname{Ext}^i_A(\mathbf{k}, M) = 0$, whence the claim.

Let $n = \inf\{i : \operatorname{Ext}^i_A(\mathbf{k}, M) \neq 0\}$. Induct on n. Suppose first $n = 0$. Since $\mathbf{k}$ is a simple A-module, there is an injective homomorphism $\mathbf{k} \to M$. Then $\mathfrak{m} \in \operatorname{Ass} M$ and hence $\operatorname{depth} M = 0$.

Suppose $n > 0$., let $a_1, \cdots, a_m \in \mathfrak{m}$ be any M-regular sequence. Using the claim inductively on $M/(a_1, \cdots, a_m)M$, we have $n \geq$ depth. If M has no regular element, then $\mathfrak{m} \subset \bigcup_{\mathfrak{p} \in \operatorname{Ass} M} \mathfrak{p}$. Then $\mathfrak{m} = \mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Ass} M$. This show that we can find $x \neq 0 \in M$ such that $\mathfrak{p} = \operatorname{Ann} x$. It gives a homomorphism $\mathbf{k} = A/\mathfrak{m} \to M$. That is a contradiction and hence M has a regular element. Let a be M-regular and $N = M/aM$. Then $\operatorname{depth} N = n-1$ by the claim and induction hypothesis. Hence we have $\operatorname{depth} M \geq n$. □

Lemma 2.3.14. Let $(A, \mathfrak{m}, \mathbf{k})$ be a noetherian local ring. Suppose we have exact sequences

$$0 \to A^{n_r} \xrightarrow{\mathrm{d}_r} A^{n_{r-1}} \xrightarrow{\mathrm{d}_{r-1}} \cdots \to A^{n_1} \xrightarrow{\mathrm{d}_1} A^{n_0},$$

such that $A^{n_i} \to \operatorname{Ker} \mathrm{d}_{i-1}$ is minimal for all i. Then $\operatorname{depth} A \geq r$.

Proof. Since d_r is injective and its image is contained in $\mathfrak{m}A^{n_{r-1}}$, we can choose $t \in \mathfrak{m}$ that is not a zero divisor. Denote the sequence by $C_\bullet$. Then we have a short exact sequence of complexes

$$0 \to C_\bullet \xrightarrow{*t} C_\bullet \to C_\bullet/tC_\bullet \to 0.$$

Consider the long exact sequence in homology

$$\cdots \to H_i(C_\bullet) \xrightarrow{*t} H_i(C_\bullet) \to H_i(C_\bullet/tC_\bullet) \to H_{i-1}(C_\bullet) \xrightarrow{*t} H_{i-1}(C_\bullet) \to \cdots.$$

Since $C_\bullet$ is exact, we have $H_i(C_\bullet) = 0$ for all i. In particular, $H_i(C_\bullet/tC_\bullet) = 0$ for all $i \geq 2$. Inductively, we can choose a regular sequence of length r in $\mathfrak{m}$. □

Lemma 2.3.15. Let $(A, \mathfrak{m}, \mathbf{k})$ be a noetherian local ring and M a finite A-module. Suppose there is an injective homomorphism $\mathbf{k} \to M$. Then $\operatorname{proj.dim} M \geq \dim_{\mathbf{k}} T_{A,\mathfrak{m}}$.

Proof. Let $x_1, \cdots, x_n \subset \mathfrak{m} \backslash \mathfrak{m}^2$ such that their images in $\mathfrak{m}/\mathfrak{m}^2$ form a basis. Then we have a complex

$$K_\bullet := 0 \to \wedge^n A^{\oplus n} \xrightarrow{\mathrm{d}_n} \wedge^{n-1} A^{\oplus n} \xrightarrow{\mathrm{d}_{n-1}} \cdots \to \wedge^1 A^{\oplus n} \xrightarrow{\mathrm{d}_1} \wedge^0 A^{\oplus n} \xrightarrow{\mathrm{d}_0} \mathbf{k} \to 0,$$

where

$$\mathrm{d}_r : \wedge^r A^{\oplus n} \to \wedge^{r-1} A^{\oplus n}, \quad e_{i_1} \wedge \cdots \wedge e_{i_r} \mapsto \sum_{k=1}^{r} (-1)^k x_{i_k} e_{i_1} \wedge \cdots \wedge \widehat{e_{i_k}} \wedge \cdots \wedge e_{i_r}.$$

Here $\widehat{e_{i_k}}$ means that we omit the k-th element. Let $P_\bullet \to M$ be the minimal projective resolution of M. Then we have a homomorphism of complexes

$$\varphi_\bullet : K_\bullet \to P_\bullet$$

induced by the injective homomorphism $\mathbf{k} \to M$.

We claim that φ_i is injective and splits P_i into a direct sum $K_i \oplus F_i$ with F_i free for all $i \geq 0$. Since K_i and P_i are free, we just need to show that $\varphi_i \otimes_A \mathrm{id}_{\mathbf{k}}$ is injective. Induct on i. For $i = 0$, note that $\mathbf{k} \to M \otimes_A \mathbf{k}$ is injective, by the commutative diagram

$$\begin{tikzcd} A \arrow[r] \arrow[d, "\varphi_0 \otimes_A \mathrm{id}_{\mathbf{k}}"'] & \mathbf{k} \arrow[d] \\ P_0 \otimes_A \mathbf{k} \arrow[r, "\cong"] & M \otimes_A \mathbf{k} \end{tikzcd},$$

the image of $\varphi_0 \otimes_A \mathrm{id}_{\mathbf{k}}$ is not zero in $P_0 \otimes_A \mathbf{k}$.

For $i > 0$, since K_{i-1} and P_{i-1} are free, we have a natural isomorphism between

$$\mathfrak{m}K_{i-1} \otimes_A \mathbf{k} \to \mathfrak{m}P_{i-1} \otimes_A \mathbf{k}$$

and

$$K_{i-1} \otimes_A \mathfrak{m}/\mathfrak{m}^2 \to P_{i-1} \otimes_A \mathfrak{m}/\mathfrak{m}^2.$$

We have a commutative diagram

$$\begin{tikzcd} K_i \otimes_A \mathbf{k} \arrow[r] \arrow[d] & \mathfrak{m}K_{i-1} \otimes_A \mathbf{k} \arrow[d] \\ P_i \otimes_A \mathbf{k} \arrow[r] & \mathfrak{m}P_{i-1} \otimes_A \mathbf{k} \end{tikzcd} \quad (2.1)$$

Since $P_{i-1}/K_{i-1} \cong F_{i-1}$ is free, the right vertical map in (2.1) is injective. By construction of $K_\bullet$, $K_i \otimes_A \mathbf{k} \to \mathfrak{m}K_{i-1} \otimes_A \mathbf{k}$ is injective. Hence the left vertical map in (2.1) is injective. This completes the proof of the claim.

By the claim, $P_i \neq 0$ for all $i \leq n$ and the conclusion follows. □

Proposition 2.3.16 (Auslander-Buchsbaum formula)**.** Let A be a noetherian local ring and M a finite A-module. Suppose $\operatorname{proj.dim} M < \infty$. Then $\operatorname{proj.dim} M = \operatorname{depth} A - \operatorname{depth} M$.

Proof. We have a minimal projective resolution

$$0 \to A^{n_r} \to A^{n_{r-1}} \to \cdots \to A^{n_1} \to A^{n_0} \to M \to 0.$$

By Lemma 2.3.14, we have $\operatorname{depth} A \geq \operatorname{proj.dim} M$.

Induct on $\operatorname{depth} M$. Suppose $\operatorname{depth} M = 0$. Then by Proposition 2.3.13, we have $\operatorname{Hom}_A(\mathbf{k}, M) \neq 0$, whence there is an injective homomorphism $\mathbf{k} \to M$. By Lemma 2.3.15, we have

$$\operatorname{depth} A \geq \operatorname{proj.dim} M \geq \dim_{\mathbf{k}} T_{A,\mathfrak{m}} \geq \operatorname{depth} A.$$

If $\operatorname{depth} M > 0$, choose a regular element $a \in \mathfrak{m}$ that is M-regular. Then by Propostion 2.3.12, we have

$$\operatorname{depth} M + \operatorname{proj.dim} M = \operatorname{depth}(M/aM) - 1 + \operatorname{proj.dim}(M/aM) + 1 = \operatorname{depth} A.$$

□

Theorem 2.3.17. Let $(A, \mathfrak{m})$ be a noetherian local ring. Then A is regular at $\mathfrak{m}$ if and only if $\operatorname{hl.dim} A < \infty$.

Proof. Suppose A is regular at $\mathfrak{m}$. Let $x_1, \cdots, x_n$ be a minimal generating set of $\mathfrak{m}$. Then $x_1, \cdots, x_n$ is an A-regular sequence since A is regular at $\mathfrak{m}$. By Proposition 2.3.12, we have $\operatorname{proj.dim} \mathbf{k} = \operatorname{proj.dim} A/(x_1, \cdots, x_n)A = n + \operatorname{proj.dim} A = n$.

Conversely, suppose $\operatorname{hl.dim} A < \infty$. Then by Proposition 2.3.11, we have $\operatorname{proj.dim} \mathbf{k} < \infty$. We have

$$\dim_{\mathbf{k}} T_{A,\mathfrak{m}} \leq \operatorname{proj.dim} \mathbf{k} \leq \operatorname{depth} A \leq \dim_{\mathbf{k}} T_{A,\mathfrak{m}}.$$

The first "$\leq$" follows from Lemma 2.3.15. The second "$\leq$" follows from Proposition 2.3.16. Hence we see that A is regular at $\mathfrak{m}$. $\square$

Corollary 2.3.18. Let $(A, \mathfrak{m})$ be a noetherian local ring. Then A is regular if and only if it is regular at $\mathfrak{m}$.

Proof. The sufficiency is trivial. For the necessity, note that if A is regular, then $\operatorname{hl.dim} A < \infty$ by Theorem 2.3.17. For any $\mathfrak{p} \in \operatorname{Spec} A$, we have a finite projective resolution

$$0 \to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to A/\mathfrak{p} \to 0.$$

Tensoring with $A_{\mathfrak{p}}$, we have a finite projective resolution of $\kappa(\mathfrak{p})$. By Theorem 2.3.17 again, we see that $A_{\mathfrak{p}}$ is regular at $\mathfrak{p}$. $\square$

Lemma 2.3.19. Let A be a noetherian integral domain. Then A is a UFD if and only if every height 1 prime ideal of A is principal.

Proof. Yang: To be completed. $\square$

Lemma 2.3.20. Let A be a noetherian integral domain and $(x) \subset A$ a non-zero prime ideal. Then A is a UFD if and only if $A[1/x]$ is a UFD.

Proof. Yang: To be completed. $\square$

Theorem 2.3.21. Let $A, \mathfrak{m}$ be a regular noetherian local ring. Then A is UFD.

Proof. Yang: To be completed. $\square$