Lecture Notes for Commutative Algebra

Lecture delivered by Paul Nelson
Notes by Lin-Da Xiao

2017 ETH

Contents

About the Course:

Professor Paul Nelson taught a course (401-3132-00L) on commutative algebra at ETH in Fall 2017. The lectures in first and second weeks were given by Paul Steinmann and Professor Kawalski respectively. These are my "live-TEXed" notes from the course. The LATEX package tikz and tikzcd were used to generated diagrams.

Of course, these notes are not a faithful representation of the course, either in the mathematics itself or in the quotes, remarks; in particular the errors are my fault. By the same token, any virtues in the notes are to be credited to the lecturer and not the scribe.

The course website is https://metaphor.ethz.ch/x/2017/hs/401-3132-00L/.

The topic includes

- Basics about rings, ideals and modules

- Localization

- Primary decomposition

- Integral dependence and valuations

- Noetherian rings

- Basic dimension theory

Prerequisite:

Rings, homomorphism, ideals, quotient rings, zero divisors, prime/maximal ideals, fields.

Convention: Ring, we mean a commutative ring with identity. $\mathrm{Spec}(\mathcal{R})$ is the prime spectrum of a ring $\mathcal{R}$ and $Spm(\mathcal{R})$ is the maximal spectrum.

In particular for a ring homomorphism $f : R \to S$. We have $f(1_R) = 1_S$. Remark: we allow 1=0 but then R=0. Caution, by definition $1 \neq 0$ in a field .

1   Rings, Ideals, Radicals

1.1   Lecture 1. Motivation and Basics by Paul Steinmann

In differential geometry, we have the theorem of level sets:

Theorem 1.1. *Let $f : \mathbb{R}^n \to \mathbb{R}$. If $0 \in \mathbb{R}^n$ is a regular value of f then $f^{-1}(0)$ is a submanifold.*

In algebraic geometry, we look at $f^{-1}(0)$ for polynomial f. More precisely, fix an algebraically closed field K and an integer $n > 0$, consider the ring $R := K[x_1, ..., x_n]$. Define: For a subset $S \subset R$ we define the **affine algebraic variety** by

$$V(S) := \{x \in K^n | \forall f \in S, \ f(x) = 0 \subset K^n\} \tag{1}$$

Remark 1.2. *With the affine algebraic varieties defined above, we have:*

- $V(\emptyset) = K^n$

- $V(\{1\}) = \emptyset$

- *For an non empty collection of subsets $(S_i)_{i \in I}$, $S_i \subset R$ we have*

$$\cap_{i \in I} V(S_i) = V(\cup_{i \in I} S_i)$$

- *S and S' are subsets in R*

$$V(S) \cup V(S') = V(\{fg | f \in S, g \in S'\})$$

*as a consequence, $(V(S))_{S \subset R}$ form the closed sets of a topology on K^n called **Zariski topology**.*

Example 1.3. *$n=2$, $R = K[X_1, X_2]$*
   $V(\{X_1\})$ is the X_2 axis in K^2
   $V(\{X_2 - X_1^2\})$ is the parabola in K^2

Definition 1.4. *Conversely for all subset $X \subset K^n$, consider*

$$I(X) := \{f \in R | \forall x \in X : f(x) = 0\} \subset R.$$

Remark 1.5. *Fact: For S in R and X subset in K^n, we have,*

- $S \subset I(V(S))$

- $X \subset V(I(X))$

- *For $S \subset S' \subset$ in R, we have $V(S) \supset V(S')$*

- *For $X \subset X' \subset K^n$, we have $I(X) \supset I(X')$*

- *$I(X) \subset R$ is an ideal.*

Definition 1.6. *The **radical of an ideal** $\mathfrak{a} \subseteq \mathcal{A}$ is $rad(\mathfrak{a}) := \{a \in R | \exists n \geq 1 \text{ s.t. } a^n \in \mathfrak{a}\} \subseteq \mathcal{A}$. An ideal $\mathfrak{a} \subseteq \mathcal{A}$ with $rad(\mathfrak{a}) = \mathfrak{a}$ is called **radical**.*

Remark 1.7. *Fact, for every ideal $\mathfrak{a} \subseteq \mathcal{A}$ we have $\mathfrak{a} \subset rad(\mathfrak{a})$.*
   $rad(\mathfrak{a})$ is an ideal, proof in exercise.
   For $X \subset K^n$ the ideal $I(X)$ is radical.

Theorem 1.8. *(The Hilbert's Nullstellensatz) For any ideal $\mathfrak{a} \subset R$ we have*

$$I(V(\mathfrak{a})) = rad(\mathfrak{a}).$$

   An important consequence of the theorem:
   the maps V and I induce the one to one correspondence between

   {radical ideals in the polynomial ring} $\Longleftrightarrow$ {affine algebraic varieties}

and this correspondence invert the inclusion.

Example 1.9. *For any point $x = (x_1, ..., x_n) \in K^n$ the ideal*

$$I(x) = \mathfrak{m}_x := (X_1 - x_1, ..., X_n - x_n)$$

is maximal.

Proof. If not, then there exists an ideal $\mathfrak{a} \subset R$ s.t.

$$R \supsetneq \mathfrak{a} \supsetneq \mathfrak{m}_x,$$

but then by the Nullstellensatz,

$$\emptyset \subsetneq V(\mathfrak{a}) \subsetneq V(\mathfrak{m}_x) = \{x\},$$

which makes the contradiction. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\square$

   Weak Nullstellensatz says the ideals $\mathfrak{m}_x$ is are precisely the maximal ideals of $K[x_1, ..., x_n]$, where K needs to be algebraically closed.

Example 1.10. *$K = \mathbb{R}, n = 1$. $X^2 + 1$ is irreducible in $\mathbb{R}[X]$. And $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$ is maximal. Consequently, we have a bijection*

   {*maximal ideals of $R :=$ polynomial ring $K[X_1, ..., X_n]$*} $\Longleftrightarrow$ {*Points in K^n*}

Let A be a ring. Remember

An element $a \in \mathcal{A}$ is **nilpotent** if there $\exists n > 1 \in \mathbb{Z}$ s.t. $a^n = 0$.

An element $a \in \mathcal{A}$ is a **zero divisor** if there is an element $b \in \mathcal{A}, b \neq 0$ s.t. $ab = 0$.

Fact: every nilpotent element is a zero-divisor but not conversely.

Example 1.11. *take $(0,1) \in \mathcal{A} \times \mathcal{A}$ then $(0,1) \cdot (1,0) = (0,0)$*

Definition 1.12. *The ideal $Nil(\mathcal{A}) := rad((0))$ is called the **nil radical** of $\mathcal{A}$.*

Then we have:

(i) $\mathrm{Nil}(\mathcal{A})$ is the set of all nilpotent elements of $\mathcal{A}$

(ii) $\mathcal{A}/\mathrm{Nil}(\mathcal{A})$ has no nilpotent elements.

Proof. (i). From definitions.

(ii). Let $x \in \mathcal{A}$ s.t. $\bar{x} \in \mathcal{A}/\mathrm{Nil}(\mathcal{A})$ is nilpotent. Let $n > 0$ s.t. $\bar{x}^n = 0$ then $x^n \in \mathrm{Nil}(\mathcal{A})$ Thus there exists $k > 0$ s.t. $(x^n)^k = 0$ hence $x^{nk} = 0$, $x \in \mathrm{Nil}(\mathcal{A})$. $\square$

Proposition 1.13. *The nil radical of $\mathcal{A}$ is the intersection of all prime ideals of $\mathcal{A}$.*

Proof. Denote by $\mathcal{N}'$ the intersection of all prime ideals of $\mathcal{A}$. For any nilpotent element $f \in \mathcal{A}$ with $n > 0$ s.t. $f^n = 0$, We have $f^n \in \mathfrak{p}$ for every prime ideal $\mathfrak{p}$. Hence $f \in \mathfrak{p} \implies$ conclude $f \in \mathcal{N}'$.

Conversely, suppose $f \in \mathcal{A}$ is not nilpotent Define $\Sigma := \{\mathfrak{a} \subset A \text{ ideals} | \forall n > 0 : f^n \notin \mathfrak{a}\}$. We will apply Zorn's lemma. We have
1. $(0) \in \Sigma$, so Σ is nonempty,
2. Σ is partially ordered by inclusion.
3. For any chain $(\mathfrak{a}_i)_{i \in I} \subset \Sigma$, the set $\mathfrak{a} := \cup_{i \in I} \mathfrak{a}_i$ is an ideal and

for all $n > 0$, we have $f^n \notin \mathfrak{a}$, hence $\mathfrak{a} \in \Sigma$. By Zorn's lemma we conclude that there is a maximal element $\mathfrak{p} \in \Sigma$.

We show that $\mathfrak{p}$ is a prime ideal. For any $x, y \notin \mathfrak{p}$, consider the ideals $\mathfrak{p} + (x), \mathfrak{p} + (y)$. They strictly contain $\mathfrak{p}$ and are thus not in Σ. Let $n, m > 0$ s.t. $f^n \in \mathfrak{p} + (x), f^m \in \mathfrak{p} + (y)$. We conclude that $f^{n+m} \in \mathfrak{p} + (xy)$, so $\mathfrak{p} + (xy) \notin \Sigma$. Hence $xy \notin \mathfrak{p}$, which means, $\mathfrak{p}$ is a prime ideal so $f \notin \mathcal{N}'$. $\square$

Remember let $f : \mathcal{A} \to \mathcal{B}$ be a ring morphism. And $\mathfrak{p} \subset \mathcal{B}$ a prime ideal. Then $f^{-1}(\mathfrak{p})$ is a prime ideal of $\mathcal{A}$. Caution: Not true for maximal ideals in general.

Proposition 1.14. *Let* $\mathfrak{a} \subset \mathcal{A}$ *be an ideal,* $\pi : \mathcal{A} \to \mathcal{A}/\mathfrak{a}$ *There is a one to one correspondence between ideals of* $\mathcal{A}/\mathfrak{a}$ *and ideals in* $\mathcal{A}$ *which contain* $\mathfrak{a}$ *via* $\mathfrak{c} = \pi^{-1}(\mathfrak{b})$

Corollary 1.15. *Let* $\mathfrak{a} \subset \mathcal{A}$ *be an ideal, then* $\mathrm{rad}(\mathfrak{a})$ *is the intersection of all prime ideals which contain* $\mathfrak{a}$.

Proof. consider the homomorphism $\pi : \mathcal{A} \to \mathcal{A}/\mathfrak{a}$ Then $\mathrm{rad}(\mathfrak{a}) = \pi^{-1}(\mathcal{N}_{\mathcal{A}/\mathfrak{a}})$. By the above proposition $\mathcal{N}_{\mathcal{A}/\mathfrak{a}}$ is the intersection of all prime ideals of $\mathcal{A}/\mathfrak{a}$. By the correspondence we conclude the statement. $\qquad\square$

Definition 1.16. *The **Jacobson Radical** $Jac(\mathcal{A})$ of $\mathcal{A}$ is the intersection of all maximal ideals in $\mathcal{A}$.*

Proposition 1.17. *We have* $x \in Jac(\mathcal{A}) \iff \forall y \in \mathcal{A} : 1 - xy$ *is a unit.*

Proof. "$\Longrightarrow$" let $x \in \mathrm{Jac}(\mathcal{A})$ and $y \in \mathcal{A}$ s.t. $1 - xy$ is not a unit. Then $1 - xy \in \mathfrak{m}$ for some maximal ideal $\mathfrak{m} \subset \mathcal{A}$. But $x \in \mathrm{Jac}(\mathcal{A}) \subset \mathfrak{m}$, hence $1 \in \mathfrak{m}$ contradiction.

"$\Longleftarrow$" let $x \notin \mathrm{Jac}(\mathcal{A})$ then $x \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m} \subset \mathcal{A}$. Since $\mathfrak{m}$ is maximal we conclude that $(x) + \mathfrak{m} = A$. Hence there exists $y \in A$, $u \in \mathfrak{m}$ s.t. $xy + u = 1$. We conclude that $1 - xy \in \mathfrak{m}$, so in particular , $1 - xy$ is not a unit. $\qquad\square$

In particular, $x \in \mathrm{Jac}(\mathcal{A}) \implies x$ not a unit. $\mathrm{Jac}(\mathcal{A}) \subseteq \{$ non-units in $\mathcal{A}\}$. $\mathcal{A} - \mathrm{Jac}(\mathcal{A}) \supseteq \mathcal{A}^{\times}$

1.2   Lecture 2. Local Rings, Coprime Ideals, Ideal Quotients by Paul Steinmann

Definition 1.18. *A ring $\mathcal{A}$ is called a **local ring** if $\mathcal{A}$ admits precisely one maximal ideal;*

Example 1.19.

- *Every field is a local ring with maximal ideal $\mathfrak{m} = 0$, because every nonzero element is a unit.*

- *$K[[X]]$ is the ring of formal power series over a field K, it has a unique maximal ideal (X). One can check that every element with nonzero constant term is invertible. i.e. $(a_0(1 - g))^{-1} = a_0^{-1}(1 + g + g^2 + ...)$*

Proposition 1.20.

- *Let $\mathcal{A}$ be a ring and $\mathfrak{m} \neq (1)$ is an ideal of A s.t. every $x \in \mathcal{A} - \mathfrak{m}$ is a unit of A, then $\mathcal{A}$ is a local ring with maximal ideal $\mathfrak{m}$.*

- *Let $\mathcal{A}$ be ring and $\mathfrak{m} \subset \mathcal{A}$ is a maximal ideal s.t. any element of $1 + \mathfrak{m} = \{1 + a | a \in \mathfrak{m}\}$ is a unit in $\mathcal{A}$. Then $\mathcal{A}$ is a local ring with maximal ideal $\mathfrak{m}$.*

Proof. For first part, every proper ideal consists of non-units, hence is contained in $\mathfrak{m}$. In other words, an element is a unit iff it is not contained in any maximal ideal.

For the second part, let $x \in \mathcal{A} - \mathfrak{m}$. Since $\mathfrak{m}$ is maximal , we have $(x) + \mathfrak{m} = (1)$, hence , $\exists y \in \mathcal{A}, t \in \mathfrak{m}$, s.t. $xy + t = 1$, which implies $xy = 1 - t \in 1 + \mathfrak{m}$. Thus xy is a unit which implies that x is a unit. Now use the first part. $\square$

Definition 1.21. *A ring $\mathcal{A}$ is called **semilocal** if $\mathcal{A}$ admits finitely many maximal ideals.*

Example 1.22.

- *$\mathbb{Z}$ is not semilocal.*

- *Let $m \in \mathbb{Z}$. Then $\mathbb{Z}/(m\mathbb{Z})$ is a semilocal ring with maximal ideals $d\mathbb{Z}/m\mathbb{Z}$ for prime number $d|m$.*

- *In particular, for $p \in \mathbb{Z}$ prime , $\mathbb{Z}/p\mathbb{Z}$ is local ring.*

Reminder: Let $\mathfrak{a}, \mathfrak{b} \subset \mathcal{A}$ be ideals their sum is

$$\mathfrak{a} + \mathfrak{b} := \{a + b | a \in \mathfrak{a}, b \in \mathfrak{b}\},$$

which is the smallest ideal containing $\mathfrak{a} \cup \mathfrak{b}$. Also infinite sums $(\mathfrak{a}_i)_{i \in I} \subset \mathcal{A}$ ideals,

$$\sum_{i \in I} \mathfrak{a}_i := \left\{ \sum_{i \in I} x_i \,\middle|\, x_i \in \mathfrak{a}_i, x_i = 0 \text{ for almost all i} \right\}$$

And we also have

$$\mathfrak{a} \cdot \mathfrak{b} \text{ or } \mathfrak{a}\mathfrak{b} = \left\{ \sum_{i \in I} x_i y_i \,\middle|\, x_i \in \mathfrak{a}, y_i \in \mathfrak{b}, \text{all but finitely many terms are } 0 \right\}.$$

Definition 1.23. *Two ideals $\mathfrak{a}, \mathfrak{b} \subset A$ are called **coprime**[1] if $\mathfrak{a} + \mathfrak{b} = (1)$*

[1]In some literature, it is called **comaximal**

Remark 1.24. *If $\mathfrak{a}, \mathfrak{b} \subset A$ are coprime ideals then $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a} \cdot \mathfrak{b}$.*
For general ideals $\mathfrak{a}, \mathfrak{b} \subset A$:

$$(\mathfrak{a} + \mathfrak{b}) \cdot (\mathfrak{a} \cap \mathfrak{b}) \subset \mathfrak{a} \cdot \mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}.$$

However, for coprime ideals, we also have $\mathfrak{a}\mathfrak{b} \supset \mathfrak{a} \cap \mathfrak{b}$, because $1 = a + b$ for $a \in \mathfrak{a}, b \in \mathfrak{b}$, then $\forall x \in \mathfrak{a} \cap \mathfrak{b}$ we have $x = x \cdot 1 = x(a+b) = xa + xb \in \mathfrak{a} \cdot \mathfrak{b}$.

Proposition 1.25. *(Chinese Remainder Theorem) Let $\mathfrak{a}_1, ..., \mathfrak{a}_n \subset \mathcal{A}$ be ideals, denote $\varphi : \mathcal{A} \to \prod_{i \in I}^{n}(\mathcal{A}/\mathfrak{a}_i)$ for the canonical homomorphism.*
(i) if $\mathfrak{a}_i, \mathfrak{a}_j$ are coprime for $i \neq j$, then $\prod_{i=1}^{n} \mathfrak{a}_i = \cap_{i=1}^{n}\mathfrak{a}_i$.
(ii)φ is surjective iff $\mathfrak{a}_i, \mathfrak{a}_j$ are coprime for $i \neq j$.
(iii) φ is injective iff $\cap_{i=1}^{n}\mathfrak{a}_i = (0)$.

Proof. (iii) Note that $\ker\varphi = \cap_{i=1}^{n}\mathfrak{a}_i$. Then

$$\prod_{i=1}^{n} (\mathcal{A}/\mathfrak{a}_i) = \mathcal{A}/(\cap_i^n \mathfrak{a}_i)$$

(i) by induction on n. For $n = 2$ it is checked above. Suppose $n > 2$ let $\mathfrak{b} := \prod_{i=1}^{n-1} \mathfrak{a}_i = \cap_{i=1}^{n-1}\mathfrak{a}_i$ Since $\mathfrak{a}_i + \mathfrak{a}_n = (1)$ for $1 \leq i \leq n-1$. We have $x_i + y_i = 1$ for some $x_i \in \mathfrak{a}_i, y_i \in \mathfrak{a}_n$ Thus $\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1}(1 - y_i) \equiv 1 \mod \mathfrak{a}_n$ We conclude that $\mathfrak{a}_n + \mathfrak{b} = (1)$, s.t.

$$\prod_{i=1}^{n} \mathfrak{a}_i = \mathfrak{b}\mathfrak{a}_n = \mathfrak{b} \cap \mathfrak{a}_n = \cap_{i=1}^{n}\mathfrak{a}_i$$

(ii) "$\Longrightarrow$", Suppose φ is surjective. Let $i \neq j$, There exists an element $x \in A$ s.t. $\varphi(x) = (0, ..., 0, 1, 0, ..., 0)$, nonzero only at the i-th entry. Thus $x \equiv 1 \mod \mathfrak{a}_i$ and $x \equiv 0 \mod \mathfrak{a}_j$. So $1 = (1 - x) + x \in \mathfrak{a}_i + \mathfrak{a}_j$.
"$\Longleftarrow$" We show that for all $k \in \{1, ..., n\}$ there exists an element $x \in A$ s.t. $\varphi(x) = (0, ..0, 1, 0..0)$, nonzero at the k-th entry. Let $k \in \{1, ..., n\}$. For every $j \in \{1, ..., n\}\backslash\{k\}$. We have $\mathfrak{a}_k + \mathfrak{a}_j = (1)$, and thus there are elements $u_j \in \mathfrak{a}_k, v_j \in \mathfrak{a}_j$ s.t. $u_j + v_j = 1$. Define $x := \prod_{i \neq k} v_i$. Then $x \equiv 0 \mod \mathfrak{a}_j, \forall j \neq k$ and $x = \prod_{i \neq k}(1 - u_i) \equiv 1 \mod \mathfrak{a}_k$. Hence, $\varphi(x) = (0, .., 0, 1, 0, ..., 0)$ nonzero in the k-th entry.
As a result, if each pair $\mathfrak{a}_i, \mathfrak{a}_j$ is coprime, we have

$$\mathcal{A}/\left(\prod_{i=1}^{n} \mathfrak{a}_i\right) \cong \prod_{i=1}^{n} (\mathcal{A}/\mathfrak{a}_i).$$

$\square$

Proposition 1.26. *Let* $\mathfrak{a}, \mathfrak{b} \subset \mathcal{A}$ *be ideals s.t.* $rad(\mathfrak{a}), rad(\mathfrak{b})$ *are coprime. Then* $\mathfrak{a}, \mathfrak{b}$ *are coprime.*

Proof. In fact, we have

$$\mathrm{rad}(\mathfrak{a} + \mathfrak{b}) = \mathrm{rad}(\mathrm{rad}(\mathfrak{a}) + \mathrm{rad}(\mathfrak{b})) = \mathrm{rad}((1)) = (1)$$

Details in the exercise sheet. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

Proposition 1.27. *(Prime avoidance)*
(i) Let $\mathfrak{p}_1, ..., \mathfrak{p}_n \subset \mathcal{A}$ *prime ideals and let* $\mathfrak{a} \subset \mathcal{A}$ *be an ideal which is contained in* $\cup_{i=1}^n \mathfrak{p}_i$ *then* $\mathfrak{a} \subset \mathfrak{p}_j$ *for some* j.
(ii)Let $\mathfrak{a}_1, ..., \mathfrak{a}_n \subset \mathcal{A}$ *be ideals and* $\mathfrak{p} \subset \mathcal{A}$ *a prime ideal s.t.* $\mathfrak{p} \supset \cap_{i=1}^n \mathfrak{a}_i$. *Then* $\mathfrak{p} \supset \mathfrak{a}_i$ *for some* i. *If* $\mathfrak{p} = \cap_{i=1}^n \mathfrak{a}_i$, *then* $\mathfrak{p} = \mathfrak{a}_i$ *for some* i .

Proof. Induction on n. For $n = 1$, easily checked. For $n > 1$. Assume that $\mathfrak{a} \not\subset \mathfrak{p}_i$ for all $1 \leq i \leq n$. We show $\mathfrak{a} \not\subset \cup_{i=1}^n \mathfrak{p}_i$. By induction hypothesis we know that $\forall k, \mathfrak{a} \not\subset \cup_{i \neq k}^n \mathfrak{p}_i$, so there exists $x_k \in \mathfrak{a}$ s.t. $x_k \notin \mathfrak{p}_i, \forall i \neq k$. We choose an x_k for each $\mathfrak{p}_k$ in the above manner. If $x_k \notin \mathfrak{p}_k$ for some k , then we are done. If not, then $x_k \in \mathfrak{p}_k$ for all k. Consider $y := \sum_{k=1}^n \prod_{j \neq k} x_j$. We have $y \in \mathfrak{a}$ and $y \equiv \prod_{j \neq k} x_j \mod \mathfrak{p}_k, \forall k$. Since $x_j \notin \mathfrak{p}_k$ for $j \neq k$ and $\mathfrak{p}_k$ is a prime ideal, we conclude that $y \notin \mathfrak{p}_k$ for all k hence $\mathfrak{a} \not\subset \cup_{i=1}^n \mathfrak{p}_i$.
(ii) Suppose for all $i \in \{1, ..., n\}$ we have $\mathfrak{p} \not\supset \mathfrak{a}_i$. Then there are $x_i \in \mathfrak{a}_i$ with $x_i \notin \mathfrak{p}$ for all i. And thus $\prod_{i=1}^n x_i \in \prod_{i=1}^n \mathfrak{a}_i \subset \cap_{i=1}^n \mathfrak{a}_i$. Since $\mathfrak{p}$ is a prime ideal $\prod_{i=1}^n x_i \notin \mathfrak{p}$, hence $\mathfrak{p} \not\supset \cap_{i=1}^n \mathfrak{a}_i$. If $\mathfrak{p} = \cap_{i=1}^n \mathfrak{a}_i \subset \mathfrak{a}_k$ for all k, which produce the last part. $\qquad\qquad\qquad\qquad\qquad$ $\square$

Definition 1.28. *Let* $\mathfrak{a}, \mathfrak{b} \subset A$ *be two ideals. Their* **ideal quotient** *is*

$$(\mathfrak{a} : \mathfrak{b}) := \{x \in \mathcal{A} | x\mathfrak{b} \subset \mathfrak{a}\}.$$

The **annihilator** *of an ideal* $\mathfrak{a} \subset A$ *is*

$$Ann(\mathfrak{a}) := \{(0) : \mathfrak{a}\}.$$

Notation: For $x \in A$ we write $(\mathfrak{a} : x) := (\mathfrak{a} : (x))$.
Fact:

(i)The ideal quotient of two ideals is again an ideal.

(ii)The set of zero-divisors of A is

$$D = \cup_{x \neq 0} \text{Ann}(x) = \cup_{x \neq 0} \text{rad}(\text{Ann}(x))$$

Proof.

(i) Check by definition.

(ii) The first equality is just by definition. The the second equality.

$$D = \text{rad}(D) = \text{rad}(\cup_{x \neq 0} \text{Ann}(x)) = \cup_{x \neq 0} \text{rad}(\text{Ann}(x)),$$

where in the second term, we extended rad to arbitrary subsets. $\square$

Proposition 1.29. *Properties: Let $\mathfrak{a}, \mathfrak{b} \subset A$ be ideals*

(i)$\mathfrak{a} \subset (\mathfrak{a} : \mathfrak{b})$

(ii) $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subset \mathfrak{a}$

(iii)$((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b} \cdot \mathfrak{c}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$

(iv) for ideals $(\mathfrak{a}_i)_{i \in I} \subset \mathcal{A}$, $(\cap_{i \in I} \mathfrak{a}_i : \mathfrak{b}) = \cap_{i \in I} (\mathfrak{a}_i : \mathfrak{b})$

(v) for ideals $(\mathfrak{b}_i)_{i \in I} \subset \mathcal{A}$, $(\mathfrak{a} : \sum_{i \in I} \mathfrak{b}_i) = \cap_{i \in I} (\mathfrak{a} : \mathfrak{b}_i)$.

Definition 1.30. *Let $\mathfrak{a} \subset \mathcal{A}$ be an ideal $f : \mathcal{A} \to \mathcal{B}$ a ring homomorphism. We define the **extension** of $\mathfrak{a}$ by f to be the ideal*

$$\mathfrak{a}^e := f_*(\mathfrak{a}) := \mathcal{B}f(\mathfrak{a}),$$

which is just the ideal in $\mathcal{B}$ generated by $f(\mathfrak{a})$.

*For an ideal $\mathfrak{b} \subset \mathcal{B}$. We define the **contraction** of $\mathfrak{b}$ via f to be the ideal*

$$\mathfrak{b}^c := f^*(\mathfrak{b}) := f^{-1}(\mathfrak{b}).$$

By definition, the extension and contraction always preserves inclusion $\subset$, but it does not necessarily preserve the proper inclusion $\subsetneq$

Proposition 1.31. *Properties: Let $f : A \to B$ be a ring homomorphism , $\mathfrak{a} \subset A$ $\mathfrak{b} \subset B$ ideals. Then :*

(i) $\mathfrak{a} \subset f^* f_*(\mathfrak{a}) = \mathfrak{a}^{ec}, \mathfrak{b} \supset f_* f^*(\mathfrak{b}) = \mathfrak{b}^{ce}$.

(ii) $f^*(\mathfrak{b}) = f^* f_* f^*(\mathfrak{b}), f_*(\mathfrak{a}) = f_* f^* f_*(\mathfrak{a})$.

(iii) Denote by C the set of contracted ideals in A and by E the set of extended ideals in B, then

$$C = \{\mathfrak{a} \subset A | f^* f_*(\mathfrak{a}) = \mathfrak{a}\},$$

$$E = \{\mathfrak{b} \subset B | f_* f^*(\mathfrak{b}) = \mathfrak{b}\}.$$

And $f_* : C \to E$ is a bijection with inverse f^*.

Proof. For (i), $\mathfrak{a} \subset f^{-1}f(\mathfrak{a}) \subset f^{-1}f_*(\mathfrak{a}) = f^* f_*(\mathfrak{a})$. For (ii) $\mathfrak{b} \supset f(f^{-1}(\mathfrak{b}))$ and $\mathfrak{b}$ is an ideal so $\mathfrak{b} \supset f_* f^*(\mathfrak{b})$. Part (iii) is left as an exercise. $\square$

2   Modules

2.1   Lecture 3. Modules, Exact Sequences by Professor Kowalski

Outline of this chapter

- Definition, examples, and Nakayama's Lemma

- Exact sequences , snake lemma

- Tensor products

- Algebra over a ring

Roughly speaking, module is "vector spaces for rings". It is closely related to fibre bundles in geometry. For the convention, we still fix commutative ring $\mathcal{A}$ with unit.

Definition 2.1. *A **module** M over $\mathcal{A}$ is an Abelian group with a linear action of $\mathcal{A}$ on M, i.e.*

$$\mathcal{A} \times M \to M$$
$$(a, x) \mapsto ax$$

so that

$$a(x + y) = ax + ay$$
$$(a + b)x = ax + bx$$
$$a(bx) = abx$$
$$1x = x$$

Example 2.2.

1. *$\{0\}$ is an $\mathcal{A}$-module*

2. *if $\mathcal{A}$ is a field $\mathcal{A}$-module is just $\mathcal{A}$-vector space.*

3. $I \subset \mathcal{A}$ *ideal; then* I*is an* $\mathcal{A}$*-module (a submodule of* $\mathcal{A}$*)*

4. $\mathcal{A} = \mathbb{Z}$*, an* $\mathcal{A}$*-module is an abelian group.*

Definition 2.3. *M and N are* $\mathcal{A}$*-modules* $f : M \to N$ *is* $\mathcal{A}$**-linear** *if* $f(ax+by) = af(x) + bf(y)$. *The set of such* $\rho : M \to N$ *is denoted* $Hom_{\mathcal{A}}(M, N)$. *It is an* $\mathcal{A}$*-module with*

$$(f + g)(x) = f(x) + g(x),$$

$$(af)(x) = af(x).$$

If $Q \xrightarrow{h} M \xrightarrow{f} N \xrightarrow{g} P$, *then* $g \circ f \in Hom_{\mathcal{A}}(M, P)$ *and* $g \circ (f \circ h) = (g \circ f) \circ h$. *Also,* $id_M \in Hom_{\mathcal{A}}(M, M)$. *In other word,* $\mathcal{A}$*-module is a category.*

Definition 2.4. $f : M \to N$ *is an* **isomorphism** *iff* $\exists g : N \longrightarrow M$ *s.t.* $g \circ f = id_N$ *and* $f \circ g = id_M$.

Remark 2.5. $Q \xrightarrow{h} M \xrightarrow{f} N \xrightarrow{g} P$, *then for any P, we get*

$$f^* : Hom_{\mathcal{A}}(N, P) \to Hom_{\mathcal{A}}(M, P)$$

$$g \mapsto g \circ f$$

and

$$f_* : Hom_{\mathcal{A}}(Q, M) \to Hom_{\mathcal{A}}(Q, N)$$

$$h \mapsto f \circ h$$

They are $\mathcal{A}$*-linear, because for example*

$$\begin{aligned}
(f^*(ah + bg))(x) &= ((ah + bg) \circ f)(x) \\
&= (ah + bg)(f(x)) \\
&= ah(f(x)) + bg(f(x)) \\
&= (af^*(h) + bf^*(g))(x).
\end{aligned}$$

Remark 2.6. *Suppose M is an* $\mathcal{A}$*-module and* $N \subset M$ *as submodule, then* M/N *has the structure of* $\mathcal{A}$*-module such that the canonical projection* $\pi : M \to M/N$ *is* $\mathcal{A}$*-linear.* $a(x + N) = ax + N$ *is well defined because* $aN \subset N$.

Definition 2.7. $f : M \longrightarrow N$ *is a morphism of* $\mathcal{A}$*-modules.*

- $Ker(f) := f^{-1}(\{0\}) \subset M$ *is a submodule of M.*

- $Im(f) := f(M) \subset N$ *is a submodule of N.*

- *Coker(f):=N/Im(f) is an $\mathcal{A}$-module.*

Remark 2.8. *(i) $ker(f) = 0 \iff f$ is injective.*

(ii) $coker(f) = 0 \iff f$ is surjective.

(iii) if $f : M \to N$ and $M' \subset ker(f)$, then we get an induced linear map $\bar{f}$, s.t the diagram

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

commutes. It is properly defined by $\bar{f}(x + M') = f(x)$ since $f(M') = \{0\}$. Then we have

$$Im(\bar{f}) = Im(f),$$

and

$$Ker(\bar{f}) = Ker(f)/M'.$$

In particular, if $M' = Ker(f)$, we get an isomorphism

$$M/Ker(f) \overset{\bar{f}}{\cong} Im(f).$$

If M is an $\mathcal{A}$-module and $(M_i)_{i \in I}$ a family of submodules then $\cap_{i \in I} M_i$ is a submodule. If $X \subset M$ be a subset then the intersection of all submodules containing X is a submodule containing X, called the submodule generated by X, denote it by $\langle X \rangle$. One checks that

$$\langle X \rangle = \{\text{linear combination of elements of } X\}$$
$$= \left\{ \sum_i^K a_i x_i \,\middle|\, 0 \le K \in \mathbb{Z}, a_i \in \mathcal{A}, x_i \in X (\text{equivalently almost all } a_i \text{ are zero}) \right\}$$

We write

$$\sum_{i \in I} M_i = \langle \cup_{i \in I} M_i \rangle$$

Definition 2.9. *If M satisfies $M = \langle X \rangle$ with X finite, then M is called **finitely generated**.*

Warning: A submodule of a finitely generated module is not necessarily finitely generated.

Example 2.10.
$$\mathcal{A} = \mathbb{C}[X_1, ..., X_n, ...].$$

$\mathcal{A}$ *is finitely generated $\mathcal{A}$-module by* 1 *however, the ideal $I = (X_1, .., X_n, ...)$ is not a finitely generated $\mathcal{A}$-module.*

Lemma 2.11.

(i) $L \supset M \supset N$ *are $\mathcal{A}$-modules, then there is an isomorphism*

$$(L/N)/(M/N) \cong L/M$$

$$(x + N) + M/N \mapsto x + M$$

Rigorously: $\pi : L \longrightarrow L/M$ *is surjective*
$\Longrightarrow \bar{\pi} : L/N \to L/M$ *is surjective*
and $Ker(\bar{\pi}) = M/N$ *so*

$$(L/N)/(M/N) \cong Im(\bar{\pi}),$$

by Remark 2.8.

(ii) $(M_1 + M_2)/M_2 \cong M_1/(M_1 \cap M_2)$

Definition 2.12. *Let $I \subset \mathcal{A}$ be an ideal and M be a module. We define $IM := \langle \{ax | a \in I, x \in M\} \rangle \subset M$ as a submodule of M.*

Proposition 2.13. *M/IM is naturally an $\mathcal{A}/I$-module.*

Proof. An element of M/IM is of the form $m + IM$ and suppose $a + I = a' + I$ $\Longrightarrow a(m + IM) = am + IM = (a' + b)(m + IM) = a'(m + IM) + bm + IM = a'm + IM$. $\square$

Definition 2.14. *$(M_i)_{i \in I}$ is a family of $\mathcal{A}$-modules*

(i) $\prod_{i \in I} M_i$ *is an $\mathcal{A}$-module with $a(x_i) = (ax_i)$.*

(ii) $\oplus_{i \in I} M_i \subset \prod_{i \in I} M_i$ *is the submodule of $(x_i)_{i \in I}$ s.t. $x_i = 0$ for all but finitely many $i \in I$.*

Cartesian product *and* ***direct product*** *are the same when there only finitely many summand. If $M_i = M, \forall i \in I$, we denote $M^{(I)} := \oplus_i M_i$. When I is finite, we denote it by M^I.*

Definition 2.15. *An $\mathcal{A}$-module M is called **free** if there exists a set I s.t. M is isomorphic to $\mathcal{A}^{(I)}$.*

Example 2.16.

1. *if $\mathcal{A}$ is a field, then every $\mathcal{A}$-module is free.*

2. *$\mathcal{A} = \mathbb{Z}$: $\mathbb{Z}/2\mathbb{Z}$ is not free.*

3. ***Warning!** A submodule of a free module is not necessarily free.(e.g. ideals in $\mathcal{A}$)*

4. *If $\mathcal{A} \neq \{0\}$, $n, m \geq 0$ are integer and $\mathcal{A}^n \cong \mathcal{A}^m$ then $n = m$. $I \subset \mathcal{A}$ maximal ideal, then we get an isomorphism of $\mathcal{A}/I$-vector spaces,*

$$(\mathcal{A}/I)^n \cong (\mathcal{A}/I)^m \implies n = m.$$

   *This is called the **invariant basis number property**, all nontrivial commutative ring has the property.*

Proposition 2.17. *(Nakayama's lemma)*
M finitely generated $\mathcal{A}$-module, $I \subset Jac(\mathcal{A})$ the Jacobson radical of $\mathcal{A}$, which is the intersection of all maximal ideals in $\mathcal{A}$. If $IM = M$, then $M = \{0\}$. e.g. $\mathcal{A}$ being a local ring and $I = \mathfrak{m}$ the only maximal in $\mathcal{A}$.

Proof. Suppose $M \neq \{0\}$, and let $\{x_1, ..., x_n\}$ be a generating set with $n \geq 1$ minimal. Since $IM = M$, we have $x_n \in IM$, so

$$x_n = \sum_{i=1}^{k} a_i y_i, y_i \in M, a_i \in I$$

where $y_i = \sum_j b_{ij} x_j$. Then we have

$$x_n = \sum_{j=1}^{n} c_j x_j$$

$$c_j = \sum_i^{k} a_i b_{ij} \in I$$

$$\implies (1 - c_n)x_n = \sum_{j=1}^{n-1} c_j x_j$$

and $(1 - c_n) \equiv 1 \mod I \implies c_n \in$ the Jacobson radical, then $1 - c_n$ is invertible by Proposition 1.17.

$$x_n = (1 - c_n)^{-1} \sum_{j=1}^{n-1} c_j x_j,$$

which contradict the minimality of the generating set. $\qquad\qquad\square$

Corollary 2.18. *M finitely generated $\mathcal{A}$-module, $I \subset Jac(\mathcal{A}), N \subset M$. If $M = IM + N$, then $M = N$.*

Proof. $I(M/N) = IM/IN = IM/(IM \cap N) = (IM + N)/N = (M/N)$, then by Nakayama's lemma we know

$$M/N = 0.$$

$\qquad\qquad\square$

Corollary 2.19. *$\mathcal{A}$ local ring, $\mathfrak{m} \subset \mathcal{A}$ the maximal ideal. M finitely generated. Then if $(x_1, ..., x_n) \in M$ are such that their classes modulo $\mathfrak{m}$ form a basis of $M/\mathfrak{m}M$ as $\mathcal{A}/\mathfrak{m}$-vector space, then they generate M.*

Proof. $N = \langle x_1, ..., x_n \rangle$ and apply Nakayama's lemma. Specifically, consider the composite map $N \hookrightarrow M \longrightarrow M/\mathfrak{m}M$ is surjective, then we have $N + \mathfrak{m}M = M$, then we can apply the Corollary 2.18. $\qquad\qquad\square$

Exact sequences

Definition 2.20.
(1)$M' \to (f)M \to (g)M''$ is **exact** if $Im(f) = ker(g)$
(2) $M' \to (f_1)M \to (f_2)M'' \to ...$ is **exact** if it is exact at each node.

Example 2.21.

1. $0 \longrightarrow M \xrightarrow{g} M''$ is exact, is equivalent to say that g is injective

2. $M' \xrightarrow{f} M \longrightarrow 0$ is exact, it is equivalent to say that f is surjective.

3. *"Short exact sequence"* $0 \longrightarrow M' \overset{f}{\longrightarrow} M \overset{g}{\longrightarrow} M'' \longrightarrow 0$ *For instance,*

$$
\begin{array}{ccccccc}
0 & \longrightarrow & M' & \overset{f}{\longrightarrow} & M' \oplus M'' & \overset{g}{\longrightarrow} & M'' & \longrightarrow & 0 \\
 & & x & \longmapsto & (x,0) \\
 & & & & (x,y) & \longmapsto & y
\end{array}
$$

the splitting sequence is exact. In fact short exact sequence of free modules always splits.

4. $\mathcal{A} = \mathbb{Z}$, *for non-free modules, for example*

$$
\begin{array}{ccccccc}
0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathbb{Z}/4\mathbb{Z} & \longrightarrow & \mathbb{Z}/w\mathbb{Z} & \longrightarrow & 0 \\
 & & x & \longmapsto & 2x \\
 & & & & x & \longmapsto & x \bmod 2
\end{array}
$$

the exact sequence does not split.

2.2   Lecture 4. Snake Lemma, Tensor Product by Professor Kowalski

Proposition 2.22. *(Snake Lemma) Suppose we have such a commutative diagram, each row is exact,*

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} \\
0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0
\end{array}
$$

then we have a map $\delta : Ker(f'') \longrightarrow Coker(f')$ s.t.

$$0 \longrightarrow Ker(f') \longrightarrow Ker(f) \rightarrow Ker(f'') \overset{\delta}{\longrightarrow} Coker(f') \longrightarrow Coker(f) \longrightarrow Coker(f'') \longrightarrow 0$$

is exact.

Proof. Consider the kernels and cokernels with the induced map between them. For notational convenience, we write $Ker(f')$ as K' and $Coker(f')$ as C' and so

on. We have the extended commutative diagram:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & K' & \xrightarrow{\ \hat{u}\ } & K & \xrightarrow{\ \hat{v}\ } & K'' & & \\
 & & \downarrow{\scriptstyle k'} & & \downarrow{\scriptstyle k} & & \downarrow{\scriptstyle k''} & & \\
0 & \longrightarrow & M' & \xrightarrow{\ u\ } & M & \xrightarrow{\ v\ } & M'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\
0 & \longrightarrow & N' & \xrightarrow{\ u'\ } & N & \xrightarrow{\ v'\ } & N'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle q'} & & \downarrow{\scriptstyle q} & & \downarrow{\scriptstyle q''} & & \\
 & & C' & \xrightarrow{\ \bar{u}\ } & C & \xrightarrow{\ \bar{v}\ } & C'' & \longrightarrow & 0,
\end{array}
$$

where the maps k', k, k'' are inclusion of the kernels as submodules and q', q, q'' are canonical projections, hence each column become exact now. $\bar{u}, \bar{v}$ are the morphism induced on quotient modules while $\hat{u}, \hat{v}$ are restrictions of u, v on submodules. One can check the induced maps on Cokernels are well defined, for example, for $\bar{v}$ to be well defined, because $q'' \circ v' \circ f = q'' \circ f'' \circ v = 0$, thus $\mathrm{Im}(f) \subset \mathrm{Ker}(q'' \circ v')$. One can also check that the above diagram is commutative. For example $x \in K'$, we have $f(\hat{u}(x)) = f(u(x)) = u'(f'(x)) = 0 \implies \hat{u}(x) \in K$, then we have $u \circ k' = k \circ \hat{u}$.

1. Exactness at K'

   We already know $\hat{u} = u|_{\mathrm{Ker}(f')}$, u injective implies that $\hat{u}$ is injective.

2. Exactness at K

   We easily check that $\mathrm{Im}(\hat{u}) \subset \mathrm{Ker}(\hat{v})$, because $k'' \circ \hat{v} \circ \hat{u} = v \circ u \circ k' = 0$, by the fact k'' is injective, we know $\hat{v} \circ \hat{u} = 0$. For the converse inclusion, if $x \in \mathrm{Ker}(\hat{v}) = \mathrm{Ker}(v) \cap \mathrm{Ker}(f)$, then $x \in \mathrm{Im}(u) \cap \mathrm{Ker}(f)$. $\exists y \in M'$ s.t. $u(y) = x \implies f(u(y)) = 0 \implies u'(f'(y)) = 0$. Then because u' is injective, $f'(y) = 0 \implies y \in K' \implies x = \hat{u}(y)$. Then we conclude $\mathrm{Ker}(\hat{v}) \subset \mathrm{Im}(\hat{u})$, thus $\mathrm{Ker}(\hat{v}) = \mathrm{Im}(\hat{u})$.

3. Exactness at C''

   $q'' \circ v' = \bar{v} \circ q$, q'', v', q are all surjective, then we conclude that $\bar{v}$ has to be surjective.

4. Exactness at C

   We easily verify that $\bar{v} \circ \bar{u} = 0$, i.e. $\bar{v} \circ \bar{u} \circ q' = q'' \circ v' \circ u' = 0$ and q' is surjective $\implies \bar{v} \circ \bar{u} = 0$. For the converse inclusion, we choose $x + \mathrm{Im}(f) \in \mathrm{Ker}(\bar{v})$, where $x \in N$. $\bar{v}(x + \mathrm{Im}(f)) = 0 = q'' \circ v'(x)$. $v'(x) \in \mathrm{Ker}(q'') = \mathrm{Im}(f'')$.

$\exists y \in M''$ s.t. $f''(y) = v'(x)$, On the other hand, v is surjective ,$\implies \exists z \in M$ s.t. $v(z) = y$. Then, we have $f''(v(z)) = v'(x) = v'(f(z))$. Then we choose $\tilde{x} = x - f(z)$, $\implies x + \text{Im}(f) = \tilde{x} + \text{Im}(f)$ & $v'(\tilde{x}) = 0$. Then there exists $w \in N'$ s.t. $u'(w) = \tilde{x}$. Then, we check that $q \circ u'(w) = q(\tilde{x}) = \tilde{x} + \text{Im}(f)$, thus $\bar{u}(q(w)) = \tilde{x} + \text{Im}(f) \implies \bar{u}(w + \text{Im}(f')) = x + \text{Im}(f)$. Then we conclude $\text{Ker}(\bar{v}) \subset \text{Im}(\bar{u})$.

5. Construct δ

For an element $x \in K''$, $k''(x) = x \in M''$ and $f''(x) = 0$. $\because v$ is surjective, $\therefore \exists y \in M$ s.t. $v(y) = x$. Then $f''(x) = f''(v(y)) = v'(f(y)) = 0 \implies f(y) \in \text{Ker}(v') = \text{Im}(u')$. Therefore, there exists $z \in N'$ s.t. $u'(z) = f(y)$. The choice of z is unique once we fix y, because u' is injective. **We define** $\delta : K'' \longrightarrow C', x \mapsto [z] = z + \mathbf{Im}(f')$. For δ to be well defined, it can not depend on the choice of y and z. Choose another $\tilde{y} \in M$ and corresponding $\tilde{z} \in N'$ s.t. $v(\tilde{y}) = x$ and $u'(\tilde{z}) = f(\tilde{y})$. We have $v(\tilde{y} - y) = 0$, $\exists w \in M'$ s.t. $u(w) = \tilde{y} - y$. Then $f(u(w)) = u'(f'(w)) = f(\tilde{y} - y) = f(\tilde{y}) - f(y)$. Then we have $u'(\tilde{z}) - u'(z) = u'(f'(w))$. Since u' is injective, we have $\tilde{z} = z + f'(w)$, thus $\tilde{z} + \text{Im}(f') = z + \text{Im}(f')$. Then we conclude that δ is well defined.

6. Exactness at K''
   For $x \in K$, we formally write

$$\begin{aligned}
\delta(\hat{v}(x)) &= u'^{-1}(f(v^{-1}(k''(\hat{v}(x))))) + \text{Im}(f') \\
&= u'^{-1}(f(v^{-1}(v(k(x))))) + \text{Im}(f') \\
&= u'^{-1}(f(k(x))) + \text{Im}(f') \\
&= 0 \text{ because } f \circ k = 0. \\
&\implies \text{Im}(\hat{v}) \subset \text{Ker}(\delta)
\end{aligned}$$

For the converse inclusion. $\forall x \in \text{Ker}(\delta)$, we trace back to the construction of δ, and select the corresponding $y \in M$, $z \in N'$, where $v(y) = x$ and $u'(z) = f(y)$. $\because x \in \text{Ker}(\delta), \therefore z \in \text{Im}(f')$. $\Longrightarrow \exists w \in M'$ s.t. $f'(w) = z$. Then we choose another $\tilde{y} = y - u(w)$, one verifies that $v(\tilde{y}) = v(y) - v(u(w)) = v(y) = x$. (this is legal, because we know δ does not depend on the choice of y) Also, we know $f(\tilde{y}) = f(y) - f(u(w)) = f(y) - u'(f'(w)) = f(y) - u'(z) = 0$. Then we know $\tilde{y} \in \text{Ker}(f) = K$, we conclude that $\hat{v}(\tilde{y}) = x$, thus $\text{Ker}(\delta) \subset \text{Im}(\hat{v})$.

7. Exactness at C'

For $x \in K''$, we formally write

$$\begin{aligned}
\bar{u}(\delta(x)) &= \bar{u}\left(u'^{-1}(f(v^{-1}(k''(x)))) + \text{Im}(f')\right) \\
&= (q \circ u')\left(u'^{-1}(f(v^{-1}(k''(x))))\right) \\
&= q(0 + f(v^{-1}(k''(x)))) \\
&= 0 \\
&\Longrightarrow \text{Im}(\delta) \subset \text{Ker}(\bar{u})
\end{aligned}$$

For the converse inclusion, we choose an element $z + \text{Im}(f') \in \text{Ker}(\bar{u})$. Then $\bar{u}(z + \text{Im}(f')) = q \circ u'(z) = 0$, then we have $\exists y \in M$ s.t. $u'(z) = f(y)$. Also we have $v'(u'(z)) = v'(f(y)) = 0, \Longrightarrow f''(v(y)) = 0$. $v(y) \in \text{Ker}(f'') = K''$. We can check that $\delta(v(y)) = z + \text{Im}(f')$. Hence, we conclude that $\text{Ker}(\bar{u}) \subset \text{Im}(\delta)$.

$\square$

Example 2.23. *(Application of snake lemma) We have such a commutative diagram, each row is exact. Suppose the middle map is isomorphism.*

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\
& & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\
0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0
\end{array}
$$

then we have a map $\delta : Ker(f'') \longrightarrow Coker(f')$ s.t.

$$0 \longrightarrow Ker(f') \longrightarrow \{0\} \to Ker(f'') \xrightarrow{\delta} Coker(f') \longrightarrow \{0\} \longrightarrow Coker(f'') \longrightarrow 0$$

is exact. Thus we get $\delta : Ker(f'') \longrightarrow Coker(f')$ is an isomorphism.

Proposition 2.24.

If $0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$ is exact, then for any $\mathcal{A}$-module N,

$$
\begin{array}{ccccccc}
0 & \longrightarrow & Hom_{\mathcal{A}}(M'', N) & \xrightarrow{v^*} & Hom_{\mathcal{A}}(M, N) & \xrightarrow{u^*} & Hom_{\mathcal{A}}(M', N) \\
& & f & \longmapsto & f \circ v & & \\
& & & & g & \longmapsto & g \circ u
\end{array} \qquad (*)
$$

is exact, in general u^* is not surjective. Also,

$$
\begin{array}{ccccccc}
Hom_{\mathcal{A}}(N, M'') & \xrightarrow{u_*} & Hom_{\mathcal{A}}(N, M) & \xrightarrow{v_*} & Hom_{\mathcal{A}}(N, M') & \longrightarrow & 0 \\
f & \longmapsto & u \circ f & & & & \\
& & g & \longmapsto & v \circ g & &
\end{array} \qquad (**)
$$

is exact but u_* is in general not always injective.

More precisely, we have **right exactness of functor** $Hom(\_, N)$:

$$
M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0 \text{ is exact} \iff (*) \text{ is exact for all } N
$$

and **Left exactness of functor** $Hom(N, \_)$:

$$
0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \text{ is exact} \iff (**) \text{ is exact for all } N.
$$

Proof. For "$\Longrightarrow$" part of the first statement, we assume $M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$ is exact. Let N be $\mathcal{A}$-module, then we check that:

1. $u^* \circ v^* = 0$
   Let $f : M'' \longrightarrow N$, $(u^* \circ v^*)(f) = f \circ v \circ u = f \circ (v \circ u) = 0$

2. v^* is injective
   Let $f : M'' \longrightarrow N$ be such that $v^*(f) = f \circ v = 0 \implies f(\operatorname{Im}(v)) = 0 \implies f = 0$ because v is surjective.

3. $\operatorname{Ker}(u^*) \subset \operatorname{Im}(v^*)$
   Let $f : M \longrightarrow N$ be such that $u^*(f) = f \circ u = 0$. Then $f(\operatorname{Im}(u)) = 0$ so $f(\operatorname{Ker}(v)) = 0$, so there is $\bar{f} : M/\operatorname{Ker}(v) \longrightarrow N$ s.t. $\bar{f} \circ p = f$.

$$
\begin{array}{ccc}
M & \xrightarrow{\ f\ } & N \\
\downarrow{\scriptstyle p} & \nearrow{\scriptstyle \bar{f}} & \\
M/\operatorname{Ker}(v) & &
\end{array}
$$

We know that v induces an isomorphism

$$\text{Im}(v) = M'' \xleftarrow{\quad v \quad} M \xrightarrow{\quad f \quad} N$$

(diagram with $\bar{v}$, p, $\bar{f}$, $\bar{v}^{-1}$, and $M/\text{Ker}(v)$)

Let $f' = \bar{f} \circ \bar{v}^{-1} \in Hom(M'', N)$, we compute $v^*(f') = f' \circ v = \bar{f} \circ \bar{v}^{-1} \circ v = \bar{f} \circ p = f$ thus $f \in \text{Im}(v^*)$

We then give an example where the surjectivity of u^* fails
Consider $\mathcal{A} = \mathbb{Z}$, $0 \longrightarrow \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$ is exact.

$$v^* : Hom(\mathbb{Z}, N) \to Hom(\mathbb{Z}, N)$$
$$f \longmapsto f \circ (\times 2)$$

is not surjective if $N = \mathbb{Z}$, because $f = Id_{\mathbb{Z}}$, we want to find a map g such that the following diagram commutes,

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z}$$

(diagram with Id, $?$, g, and $\mathbb{Z}$)

but there is no g such that $g \circ (\times 2) = Id_{\mathbb{Z}}$ because every morphism in $Hom_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z})$ is of the form $\times q$, where $q \in \mathbb{Z}$.

Conversely, for the "$\Longleftarrow$" part of the first statement, assume (*) is always exact. We want to show that $M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$ is exact,

$$
\begin{array}{ccccccc}
0 & \longrightarrow & Hom_{\mathcal{A}}(M'', N) & \xrightarrow{v^*} & Hom_{\mathcal{A}}(M, N) & \xrightarrow{u^*} & Hom_{\mathcal{A}}(M', N) \\
 & & f & \longmapsto & f \circ v & & \\
 & & & & g & \longmapsto & g \circ u
\end{array}
$$

1. Let $N = Coker(v)$ and $[p : M'' \longrightarrow Coker(v)] \in Hom(M'', N)$, then $v^*(p = p \circ v = 0)$. Since v^* is injective, we have $p = 0$, in other words $M'' = \text{Ker}(p) = \text{Im}(v)$ so v is surjective.

2. Take $N = M''$ and $f = Id_{M''}$, $(u^* \circ v^*)(f) = 0$ means $Id_{M''} \circ v \circ u = 0 \implies v \circ u = 0$, hence $\text{Im}(u) \subset \text{Ker}(v)$.

3. Take $N = M/\mathrm{Im}(u)$, and $p : M \longrightarrow N$ projection, we have $u^*(p) = p \circ u = 0$. So $p \in \mathrm{Ker}(u^*)$, so there exists $f \in Hom(M'', N)$ s.t. $v^*(f) = f \circ v = p$.

$$M' \xrightarrow{\;f\;} N = M/\mathrm{Im}(u)$$
$$v \uparrow \quad \nearrow p$$
$$M$$

Hence $\mathrm{Ker}(v) \subset \mathrm{Ker}(p)$ and $\mathrm{Ker}(v) \subset \mathrm{Im}(u)$, then we can conclude that $\mathrm{Ker}(v) = \mathrm{Im}(u)$.

The above steps proves the first statement and proof of the second statement is similar. □

Tensor Product

Definition 2.25. *M, N, P are $\mathcal{A}$-modules, A map $f : M \times N \longrightarrow P$ is called $\mathcal{A}$-**bilinear** if*

$$f(ax + by, z) = af(x, z) + bf(y, z)$$

$$f(x, ay + bz) = af(x, y) + bf(x, z)$$

$$Bil_{\mathcal{A}}(M, N, P) = \{ \text{ all } \mathcal{A}\text{-bilinear maps form } M \times N \text{ to } P\}.$$

$Bil_{\mathcal{A}}(M, N, P)$ is an $\mathcal{A}$-module.

Definition 2.26. *M, N are $\mathcal{A}$-modules and the **tensor product** gives an $\mathcal{A}$-module $M \otimes_{\mathcal{A}} N$ such that $Bil_{\mathcal{A}}(M, N; P) = Hom_{\mathcal{A}}(M \otimes_{\mathcal{A}} N, P)$. $Bil_{\mathcal{A}}(M, N; P)$ is obviously an $\mathcal{A}$-module, with sum and scalar multiplication performed valuewise.*

Theorem 2.27. *M, N are $\mathcal{A}$-modules. There exists a pair (T, β) where T is an $\mathcal{A}$-module and $\beta : M \times N \longrightarrow T$ s.t. any $\mathcal{A}$-bilinear map $b : M \times N \longrightarrow P$ factors through (T, β), i.e. there exists a unique $f : T \longrightarrow P$ s.t. the following diagram commutes.*

$$M \times N \xrightarrow{\;b\;} P$$
$$\beta \downarrow \quad \nearrow \exists! f$$
$$T$$

*This is what we call **universal property**. One can check that if it exists, it is unique.*

2.3 Lecture 5. Properties of Tensor Product

The motivation of tensor product is to "classify" bilinear/multilinear maps between modules over some ring $\mathcal{A}$.

Definition/Theorem 2.28. *M and N are $\mathcal{A}$-modules, **there exists a best possible bilinear map** $M \times N \to M \otimes N$. That is to say : there exists a module T (denoted $M \otimes N$ or $M \otimes_{\mathcal{A}} N$) and a bilinear map $f : M \times N \longrightarrow T$. By "best possible", we mean: For all module P and all bilinear map $b : M \times N \to P$, here exists a unique $\tilde{b} : T \longrightarrow P$ s.t. the following diagram commutes.*

$$
\begin{array}{ccc}
M \times N & \xrightarrow{\ b\ } & P \\
\big\downarrow{\scriptstyle f} & \nearrow & \\
T & {\scriptstyle \exists!\tilde{b}} &
\end{array}
$$

*What's more (T, f) is **strongly unique** which means **it is unique up to unique isomorphism***

$$
\begin{array}{ccc}
M \times N & \xrightarrow{\ f'\ } & T' \\
\big\downarrow{\scriptstyle f} & {\scriptstyle \exists!k}\nearrow & \\
T & {\scriptstyle \exists!j} &
\end{array}
$$

Proof. **Uniqueness**
The uniqueness is just the direct result of universal property. By definition, f is bilinear. Apply the universal property with $P = T'$, $b = f'$, then we know $j := \tilde{b} : T \to T'$. Similarly, we can construct k by swapping T, T'. Consider $k \circ j : T \to T$, apply the universal property with $P := T$, $b := f$

$$
\begin{array}{ccc}
M \times N & \xrightarrow{\ f\ } & T \\
\big\downarrow{\scriptstyle f} & \nearrow & \\
T & {\scriptstyle \exists!\tilde{b}} &
\end{array}
$$

We know $\exists!\tilde{b}$ s.t. the diagram commutes. Then we have $\tilde{b} \circ f = f$, but another obvious map having this property is just id_T. Then, we get to the conclusion $k \circ j = id_T$ by the uniqueness of $\tilde{b}$. Similarly, we get $j \circ k = id_{T'}$. Altogether, we conclude that (T, f) is unique up to unique isomorphism.
Existence
Form the free module $C := \mathcal{A}^{M \times N}$, where

$$
\mathcal{A}^{(M \times N)} = \left\{ \sum_{(x,y) \in M \times N} a_{(x,y)}(x, y) \,\middle|\, a_{(x,y)} \in \mathcal{A}, \text{almost all } a_{(x,y)} = 0 \right\}.
$$

We'd better mention the universal property of the free module $\mathcal{A}^{(M \times N)}$, every map $q : M \times N \longrightarrow P$ can be extended to $\tilde{q} : \mathcal{A}^{(M \times N)} \longrightarrow P$

Let submodule $D \subseteq C$, then there is an induced map $\bar{g} : M \times N \longrightarrow C/D$ for defining map $g : M \times N \longrightarrow C$ of the free module. Then we consider a certain submodule D with the following two equivalent definitions

- D is the smallest submodule for which all the induced map $\bar{g} : M \times N \longrightarrow C/D$ is bilinear.

- D it the submodule generated by the following elements

$$\left\{ \begin{array}{l} (x + x', y) - (x, y) - (x', y) \\ (x, y + y') - (x, y) - (x, y') \\ a(x, y) - (ax, y) \\ a(x, y) - (x, ay) \end{array} \middle| \, \forall a \in \mathcal{A}, \forall x, x' \in M, \forall y, y' \in N \right\}$$

The equivalence of two definition can be explained by the definition of "bilinear maps".

We want to show that C/D is what we are looking for. First, we claim, for all bilinear mop $b : M \times N \to P$, $\mathrm{Ker}(\tilde{b}) \supseteq D$.

The proof is to just check it by hand, e.g.

$$\begin{aligned} &\tilde{b}((x + x', y) - (x, y) - (x', y)) \\ &= \tilde{b}((x + x', y)) - \tilde{b}((x, y)) - \tilde{b}((x', y)) \\ &= b(x + x', y) - b(x, y) - b(x', y) \\ &= 0 (\text{by } b \text{ is bilinear}) \end{aligned}$$

The characterization of $\tilde{b}$ determines its restriction of $g(M \times N) \subseteq T$. Clear by construction that $g(M \times N)$ generates T. We get the conclusion that $\bar{g} : M \times N \to C/D = T$. $\qquad\qquad\qquad \square$

Also note that, in general

$$S := \{m \otimes n | (m, n) \in M \times N\} \neq M \otimes N$$

, e.g. $\mathbb{Z}^n \otimes \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$ but S generates $M \otimes N$ as we saw in the proof.

Example 2.29. *Natural isomorphisms, $\exists!$ isomorphisms*

1. $M \otimes N \cong N \otimes M$

2. $(M \otimes N) \otimes P \cong M \otimes (N \otimes P)$

3. $M \otimes (N_1 \oplus N_2) \cong (M \otimes N_1) \oplus (M \otimes N_2)$

4. $\mathcal{A} \otimes M \cong M$

Proof. we prove part 3. Consider a map:

$$b : M \times (N_1 \oplus N_2) \rightarrow M \otimes N_1 \oplus M \otimes N_2$$
$$(m, (n_1, n_2)) \mapsto (m \otimes n_1, m \otimes n_2).$$

We can check that b is bilinear, for example

$$b(m + m', (n_1, n_2))$$
$$= ((m + m') \otimes n_1, (m + m') \otimes n_2)$$
$$= (m \otimes n_1 + m' \otimes n_1, m \otimes n_2 + m' \otimes n_2)$$
$$= (m \otimes n_1, m \otimes n_2) + (m' \otimes n_1, m' \otimes n_2)$$
$$= b(m, (n_1, n_2)) + b(m', (n_1, n_2)).$$

As a result the bilinear map b must factor through $M \otimes (N_1 \oplus N_2)$, and we denote the corresponding map $f : M \otimes (N_1 \oplus N_2) \rightarrow M \otimes N_1 \oplus M \otimes N_2$.

$$f(m \otimes (n_1, n_2)) = (m \otimes n_1, m \otimes n_2).$$

We use the terminology **pure tensor** to name the tensors like $x \otimes y \in M \otimes N$, obviously, $M \otimes N$ is linearly generated by pure tensors. We want to show that f is an isomorphism. Need to find the inverse map g of f.

define
$$g_1 : M \otimes N_1 \longrightarrow M \otimes (N_1 \oplus N_2)$$
$$(m \otimes n_1) \longmapsto m \otimes (n_1, 0)$$

similarly, we can construct

$$g_2 : M \otimes N_2 \longrightarrow M \otimes (N_1 \oplus N_2)$$
$$(m \otimes n_2) \longmapsto m \otimes (0, n_2)$$

Then, we define $g = g_1 \oplus g_2$. We want to show $f \circ g = id, g \circ f = id$.

$$f \circ g(m \otimes n, m' \otimes n_2)$$
$$= f(m \otimes (n_1, 0) + m' \otimes (0, n_2))$$
$$= (m \otimes n_1, 0) + (0, m' \otimes n_2)$$
$$= (m \otimes n_1, m' \otimes n_2)$$

Then $f \circ g = id$ on pure tensors, hence it is identity on all tensors, because $f \circ g$ is linear, and pure tensor generates the whole tensor product module. $\qquad\square$

Consider $\mathcal{A}^m = \mathcal{A} \oplus \mathcal{A} \oplus ... \oplus \mathcal{A}$ (finite free module), by the isomorphism 4 in the above example

$$\mathcal{A} \otimes \mathcal{A} \cong \mathcal{A}$$
$$x \otimes y \mapsto xy$$

also by iterating (3) and (4), we get

$$\mathcal{A}^m \otimes \mathcal{A}^n \cong \mathcal{A}^{mn},$$

compared to the known result

$$\mathcal{A}^m \oplus \mathcal{A}^n \cong \mathcal{A}^{m+n}.$$

More directly, if $e_1^{(1)}, ..., e_m^{(1)}$ standard basis for $\mathcal{A}^m$, $e_1^{(2)}, ..., e_n^{(2)}$ standard basis for $\mathcal{A}^n$, then

$$\left\{ e_i^{(1)} \otimes e_j^{(2)} \,\middle|\, m \geq i \geq 1, n \geq j \geq 1 \right\}$$

form a basis of $\mathcal{A}^m \otimes \mathcal{A}^n$ and induces $\cong \mathcal{A}^{mn}$

To see this directly, consider a bilinear map $f : \mathcal{A}^m \times \mathcal{A}^n \longrightarrow P$, where P is some module.

$$\mathcal{A}^m \ni x = x_1 e_1^{(1)} + ... + x_m e_m^{(1)}, \ x_i \in \mathcal{A}$$
$$\mathcal{A}^n \ni y = y_1 e_1^{(1)} + ... + y_m e_m^{(1)}, \ y_i \in \mathcal{A}$$

Then

$$f(x, y) = \sum_{\substack{i = 1...m \\ j = 1...n}} x_i y_j f(e_i^{(1)} \otimes e_j^{(2)}),$$

where we can define $f(e_i^{(1)} \otimes e_j^{(2)}) =: a_{ij} \in P$ Generally, given an mn-tuple (a_{ij}) in P we may define a bilinear $f : \mathcal{A}^m \times \mathcal{A}^n \longrightarrow P$ by the above formula.

$$
\begin{array}{ccc}
& (e_i^{(1)}, e_j^{(2)}) \longmapsto e_i^{(1)} \otimes e_j^{(2)} & \\
\mathcal{A}^m \times \mathcal{A}^n & \longrightarrow & \mathcal{A}^{\oplus \{e_i^{(1)} \otimes e_j^{(2)}\}} \\
\downarrow f & & \\
P & \xleftarrow{\quad \exists! \tilde{f} \ s.t. \ \tilde{f}(e_{ij}) = a_{ij} \quad} &
\end{array}
$$

Remark 2.30. *More generally, we may define the n-fold tensor products $M_1 \otimes \ldots \otimes M_n$.*

$\{multilinear\ maps : M_1 \times \ldots \times M_n \longrightarrow P\} \leftrightarrow \{linear\ maps : M_1 \otimes \ldots \otimes M_n \longrightarrow P\}$

Let $V = \mathbb{R}^n$, then

$$\{inner\ products\ on\ V\} \leftrightarrow \{linear\ functions\ on\ V \otimes V\}$$

Remark 2.31. ***Extension of scalars*** *Consider a ring morphism $f : \mathcal{A} \to \mathcal{B}$ and an $\mathcal{A}$-module M, we can construct a $\mathcal{B}$-module*

$$M_{\mathcal{B}} := M \otimes_{\mathcal{A}} \mathcal{B},$$

where $\mathcal{B}$ is regarded as an $\mathcal{A}$-module via f, i.e. $a \cdot b = f(a)b$. And the $\mathcal{B}$ action on $M_{\mathcal{B}}$ is like $b \cdot (m \otimes z) := m \otimes bz$

Example 2.32.

- $M = \mathcal{A}^m \Longrightarrow M_{\mathcal{B}} = \mathcal{B}^m$

- $\mathcal{A} = \mathbb{R}, \mathcal{B} = \mathbb{C} \Longrightarrow (\mathbb{R}^n)_{\mathbb{C}} := (\mathbb{R}^n) \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C}^n$

2.4   Lecture 6. Flatness

The meaning of $x \otimes y$ depends on the modules to which we regard x and y are belonging. In fact, one can have $x \in M' \subseteq M$ and $y \in N' \subset N$ but

$$M' \otimes N' \ni x \otimes y \neq x \otimes y \in M \otimes N$$

Example 2.33. $\mathcal{A} = \mathbb{Z}$, $M' = 2\mathbb{Z} \subseteq M = \mathbb{Z}$, $N' = \mathbb{Z}/2 = N$, then $2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \ni 2 \otimes 1 \neq 0$, but $\mathbb{Z} \otimes \mathbb{Z}/w\mathbb{Z} \ni 2 \otimes 1 = 0$

In summary, we no $M' \subset M, N' \subset N$ does not indicate that $M' \otimes N' \subset M \otimes N$, which means the simple inclusion is not an injective morphism.

But $\otimes$ is indeed a **bifunctor**. Given module morphisms

$$f : M' \longrightarrow M$$
$$g : N' \longrightarrow N$$
$$\exists! f \otimes g : M' \otimes N' : \longrightarrow M \otimes N$$
$$x \otimes y \longmapsto f(x) \otimes g(y)$$

and
$$(f \circ f') \otimes (g \circ g') = (f \otimes g) \circ (f' \otimes g')$$

For example, we alway consider the case $g = 1_N$ with N $\mathcal{A}$-module, then each morphism $f : M' \longrightarrow M$ is mapped to $f \otimes 1_N : M' \otimes N \longrightarrow M \otimes N$.

Definition 2.34. *N is **flat** if $\forall f : M' \longrightarrow M$ s.t.*

$$f : injective \implies f \otimes 1_N \ is \ injective$$

In other words,
$$M' \subset M \implies \text{``} M' \otimes N \subset M \otimes N \text{''}$$

Example 2.35.

- *$\{0\}$ is a flat $\mathcal{A}$-module*

- *$\mathcal{A}$ is a flat $\mathcal{A}$-module, because $M \otimes_{\mathcal{A}} \mathcal{A} = M$ and $f = f \otimes 1_{\mathcal{A}}$*

Lemma 2.36. *Let $(N_i)_{i \in I}$ be a family of modules over $\mathcal{A}$, then $\oplus_{i \in I} N_i$ is flat iff each N_i is flat.*

Proof. Suppose each N_i is flat. Let $M' \xrightarrow{f} M$ be injective. Suppose,

$$M' \otimes (\oplus_i N_i) \xrightarrow{f \otimes 1} M \otimes (\oplus_i N_i)$$

is not injective, i.e. $z \in \mathrm{Ker}(f \otimes 1_N) \neq 0$. Let N denote $\oplus_i N_i$ and the i-th projection $\pi_i : N \longrightarrow N_i$.

$$
\begin{array}{ccc}
0 \neq z \quad \in \quad \oplus_i (M' \otimes N_i) & \xrightarrow{\rho'_i} & M' \otimes N_i \\
\| & & \| \\
M' \otimes (\oplus_i N_i) & \xrightarrow{1_{M'} \otimes \pi_i} & M' \otimes N_i \\
\downarrow{\scriptstyle f \otimes 1_N} & & \downarrow{\scriptstyle f \otimes 1_{N_i}} \\
M \otimes (\oplus_i N_i) & \xrightarrow{1_M \otimes \pi_i} & M \otimes N_i \\
\| & & \| \\
\oplus_i (M \otimes N_i) & \xrightarrow{\rho_i} & M \otimes N_i
\end{array}
$$

$z \neq 0 \implies \exists i \in I$ s.t. $\rho'_i(z) \neq 0 \implies (f \otimes 1_{N_i})(\rho'_i(z)) \neq 0 \in M \otimes N_i$. But $(f \otimes 1_{N_i})(\rho'_i(z)) = \rho_i(f \otimes 1_N(z))$ is the i-th component of $(f \otimes 1_N)(z) = 0$ by assumption, which gives the contradiction. The converse is simpler. $\qquad \square$

Corollary 2.37. *If M is a free $\mathcal{A}$-module, then it is a flat module.*

Proof. We already know $\mathcal{A}$ is flat, then by the previous lemma, we know $\oplus_{i \in I} \mathcal{A}$ is flat. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\square$

Example 2.38. *Consider a system of linear equations*

$$S : f_1(x_1, ..., x_n) = ... = f_m(x_1, ..., x_n) = 0,$$

where these f_i's has coefficients in $\mathbb{R}$. Then S has solution over $\mathbb{R}$ iff S has solution over $\mathbb{C}$ (This claim works for any field extension L/K instead of $\mathbb{C}/\mathbb{R}$) A simple proof goes like: "$\Longrightarrow$" is trivial, for the converse, we take the real or the imaginary part of a complex solution.

For a second proof:

$$M' = \mathbb{R}^n \xrightarrow{f} M = \mathbb{R}^m,$$

where $f = (f_1, ..., f_m)$. $\mathcal{A} = \mathbb{R}$, $N = \mathbb{C} \cong \mathbb{R} \oplus \mathbb{R}i$ is free, then by the above corollary, we know N is flat. Then S has a solution over $\mathbb{R}$ iff $Ker(f) \neq 0$, and S has a solution over $\mathbb{C}$ iff $Ker(f \otimes 1_{\mathbb{C}}) \neq 0$. If $f \otimes 1$ is not injective, by the definition of flat module, we know f is not injective, which conclude the proof. This second proof works for arbitrary field extension, because the field extensions are always free modules over the initial field.

Proposition 2.39. *(Right exactness of $\otimes N$)*
Consider an exact sequence of $\mathcal{A}$-modules

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

Then we have

$$M' \otimes N \xrightarrow{f \otimes 1} M \otimes N \xrightarrow{g \otimes 1} M'' \otimes N \longrightarrow 0$$

is exact for arbitrary $\mathcal{A}$-module N.

Proof. Obviously $g \otimes 1$ is surjective. We only need to prove the exactness at $M \otimes N$. As for the easier inclusion, $\text{Im}(f \otimes 1) \subseteq \text{Ker}(g \otimes 1)$ because $(g \otimes 1) \circ (f \otimes 1) = (g \circ f) \otimes 1 = 0$. Then it remains to show

$$\frac{M \otimes N}{\text{Im}(f \otimes 1)} \xrightarrow{\psi} M'' \otimes N$$

is an isomorphism. ψ is induced by $g \otimes 1$, well defined because $\text{Im}(f \otimes 1) \subseteq \text{Ker}(g \otimes 1)$.

Now, we construct a two-sided inverse φ of ψ.

$$
\begin{array}{ccc}
M'' \otimes N & \xrightarrow{\ \exists\varphi\ } & \frac{M \otimes N}{\mathrm{Im}(f \otimes 1)} \\
\big\uparrow & \nearrow^{\exists\varphi_0} & \nearrow \\
M'' \times N & & \\
\big\uparrow{\scriptstyle g \times 1} & \nearrow_{\varphi_1} & \\
M \times N & &
\end{array}
$$

Consider the map φ_1, it is the composition of the canonical projection and the defining map of tensor product. $\varphi_1(x,y) \mapsto x \otimes y + \mathrm{Im}(f \otimes 1)$. Consider $(x'', y) \in M'' \times N$, which is the image of (x,y) under $g \times 1$. Then we can define $\varphi_0(x'', y) := \varphi_1(x,y)$. It is well-defined, because if there is another (x_1, y) also map to (x'', y), the difference

$$
x - x_1 \in \mathrm{Ker}(g) = \mathrm{Im}(f),
$$

hence $\exists z \in M'\ x - x_1 = f(z). \implies (x - x_1) \otimes y = (f \otimes 1)(z \otimes y)$ Then

$$
\varphi_1(x, y) - \varphi(x_1, y) = (x - x_1) \otimes y + \mathrm{Im}(f \otimes 1) = 0.
$$

Then it remains to check φ_0 is bilinear so that φ_0 lifts to a φ on $M'' \otimes N$. Also we need to check the φ is indeed the two-sided inverse of ψ.

Consider $\varphi_0(x'', ay+bv)$ and $\varphi_0(ax''+bw'', y)$. Chose x and w in the preimages $g^{-1}(x'')$ and $g^{-1}(w'')$. By the linearity of g, we can safely choose $ax + bw$ in the pre-image of $ax'' + bw''$ Knowing that φ_1 is bilinear (because the defining map of tensor product is bilinear and canonical projection is linear), we have

$$
\begin{aligned}
\varphi_0(x'', ay + bv) &= \varphi_1(x, ay + bv) \\
&= a\varphi_1(x, y) + b\varphi_1(x, v) = a\varphi_0(x'', y) + b\varphi_0(x'', v)
\end{aligned}
$$

and

$$
\begin{aligned}
\varphi_0(ax'' + bw'', y) &= \varphi_1(ax + bw, y) \\
&= a\varphi_1(x, y) + b\varphi(w, y) = a\varphi_0(x'', y) + b\varphi_0(w'', y).
\end{aligned}
$$

Explicitly, with $x \in g^{-1}(x'')$,

$$
\varphi(x'' \otimes y) = x \otimes y + \mathrm{Im}(f \otimes 1)
$$

and

$$
\psi(x \otimes y + \mathrm{Im}(f \otimes 1)) = g(x) \otimes y
$$

$$\implies$$
$$\psi \circ \varphi(x'' \otimes y) = g(x) \otimes y = x'' \otimes y$$
$$\varphi \circ \psi(x \otimes y + \text{Im}(f \otimes 1)) = x_1 \otimes y + \text{Im}(f \otimes 1) = x \otimes y + \text{Im}(f \otimes 1),$$

where in the last line x_1 is another representative in $g^{-1}(x'')$. $\qquad\square$

Corollary 2.40. *N is flat iff $\otimes N$ preserves the exactness of any sequence of modules*

Proof. Any exact sequence can be split up into short exact sequence, and the flatness does indicate it preserve the exactness of short exact sequence. $\qquad\square$

Example 2.41. *An ideal $\mathfrak{a} \subset \mathcal{A}$, and M is an $\mathcal{A}$-module,*

$$M \otimes_{\mathcal{A}} \mathcal{A}/\mathfrak{a} \cong M/\mathfrak{a}M,$$

where $\mathfrak{a}M := \{\sum x_i m_i | x_i \in \mathfrak{a}, m_i \in M\}$. $\mathfrak{a}M$ is a submodule of M.

Proof.
$$0 \longrightarrow \mathfrak{a} \longrightarrow \mathcal{A} \longrightarrow \mathcal{A}/\mathfrak{a} \longrightarrow 0$$

is an exact sequence (of A-modules). Tensorring it with M, we have

$$\mathfrak{a} \otimes M \xrightarrow{\psi} M \longrightarrow M \otimes \mathcal{A}/\mathfrak{a} \longrightarrow 0$$

is exact, where ψ is induced by the inclusion $\mathfrak{a} \hookrightarrow \mathcal{A}$, $\psi : x \otimes m \mapsto xm$. $\text{Im}(\psi) = \mathfrak{a}M$ Then by the exactness, we have

$$M \otimes \mathcal{A}/\mathfrak{a} \cong M/\text{Im}(\psi) = M/\mathfrak{a}M.$$

$\qquad\square$

Example 2.42.
$$\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/gcd(m,n)\mathbb{Z}.$$

Pf. Take $M = \mathbb{Z}/m\mathbb{Z}$, $\mathcal{A} = \mathbb{Z}$, $\mathfrak{a} = n\mathbb{Z}$. Then $\mathfrak{a}M = (n\mathbb{Z} + m\mathbb{Z})/m\mathbb{Z} = gcd(m,n)\mathbb{Z}/m\mathbb{Z}$. $\mathcal{A}/\mathfrak{a} = \mathbb{Z}/n\mathbb{Z}$

Then by the result of Example 2.41, we have

$$M \otimes \mathcal{A}/\mathfrak{a} = \frac{\mathbb{Z}}{m\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{n\mathbb{Z}} \cong \frac{\mathbb{Z}/m\mathbb{Z}}{gcd(m,n)\mathbb{Z})/m\mathbb{Z}} = \frac{\mathbb{Z}}{gcd(m,n)\mathbb{Z}} = M/\mathfrak{a}M.$$

Let $n \in \mathbb{Z}$. Then $\mathbb{Z}/n\mathbb{Z}$ is flat iff $n = \pm 1, 0$, i.e. $\mathbb{Z}/n\mathbb{Z} = \{0\}$ or $\mathbb{Z}$. This is easy to prove, consider the following short exact sequence for $|n| \geq 2$,

$$0 \longrightarrow n\mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0,$$

Suppose $\mathbb{Z}/n\mathbb{Z}$ is flat. Tensorring it with the above exact sequence, we get

$$0 \longrightarrow 0 \longrightarrow \mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0,$$

which gives the contradiction.

Fact

Any finitely generated $\mathbb{Z}$-module is of the form

$$M = \mathbb{Z}^r \left(\oplus_{i \in I} (\mathbb{Z}/n_i\mathbb{Z}) \right)$$

, the second part of M is denoted M_{tors}, then we get the corollary that a finitely generated $\mathbb{Z}$-module is flat iff M_{tors} vanishes.

Definition 2.43. *$\mathcal{A}$ a ring, M an $\mathcal{A}$-module, we call M **torsion free** if $\forall a \in \mathcal{A}$ non-zerodivisor. $m \in M$ $am = 0 \implies m = 0$*

Theorem 2.44.

1. *M if flat $\implies M$ is torsion free*

2. *If $\mathcal{A}$ is PID, M is torsion free $\implies M$ is flat.*

Proof. Bosch section 4.2 $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ □

Some other facts about tensor product

Example 2.45. *For $\mathcal{A} = \mathbb{F}$ being a field, V, W finite dimensional vector space over $\mathbb{F}$*

$$V^* \otimes W \cong Hom_{\mathbb{F}}(V, W)$$
$$l \otimes w \mapsto [v \mapsto l(v)w]$$

3 Localization

3.1 Lecture 7. Localization of Rings

Motivation For $\mathcal{A}$ an integral domain, we defined the quotients field $Frac(\mathcal{A})$. In general, one may want to invert part of $\mathcal{A}$. For example, we may consider $\mathbb{Z}[1/2] = \{a/(2^n)|a \in \mathbb{Z}, n \in \mathcal{N}\}$. Each $2^n \in \mathbb{Z}[1/2]$ is invertible. For a subset $0 \notin S \subseteq \mathcal{A}$, we can define $\mathcal{A}[1/S]$ to be the subring of $Frac(\mathcal{A})$ generated by $\mathcal{A}$ and $\{1/s|s \in S\}$.

Definition 3.1. *A set of $\mathcal{A}$, S is **multiplicatively closed** if*

- $1 \in S$

- $s, t \in S \implies st \in S$

*For a set $S \subset \mathcal{A}$, we can define its **multiplicative closure***

$$\overline{S} := \left\{ s_I = \prod_{i_n} s_{i_n} \,\middle|\, I = (i_1, ..., i_n), \forall n, s_{i_n} \in S \right\}$$

A set S is multiplicatively closed iff $S = \overline{S}$. And we see that $\mathcal{A}[1/S] = \mathcal{A}[1/\overline{S}]$.

Definition 3.2. *Let $\mathcal{A}$ be a ring $S \subseteq \mathcal{A}$ a multiplicatively closed set, define a relation $\sim$ on $\mathcal{A} \times S$:*

$$(a, s) \sim (a', s') \iff \exists t \in S \text{ s.t. } as't = a'st$$

Lemma 3.3. *"$\sim$" is indeed a equivalence relation.*

Proof. reflectivity and symmetricity are trivial, for the transtivity

$$(a, s) \sim (a', s') \sim (a'', s'')$$

$$\implies$$

$$\exists t \in S : as't = a'st$$
$$\exists t' \in S : a's''t' = a''s't'$$
$$as''(tt's') = as'ts''t' = a's''t'st = a''s(tt's')$$
$$\implies (a, s) \sim (a'', s'')$$

$\square$

Definition 3.4. *We define **localization of $\mathcal{A}$ with respect to** S, $S^{-1}\mathcal{A} : (\mathcal{A} \times S)/\sim$. And we denote the equivalence class of (a, s) by a/s.*

Proposition 3.5. *There are well defined maps:*

$$(+) : S^{-1}\mathcal{A} \times S^{-1}\mathcal{A} \longrightarrow S^{-1}\mathcal{A}, \ (a/s, a'/s') \mapsto \frac{as' + a's}{ss'}$$

$$(\cdot) : S^{-1}\mathcal{A} \times S^{-1}\mathcal{A} \longrightarrow S^{-1}\mathcal{A}, \ (\frac{a}{s}, \frac{a'}{s'}) \mapsto \frac{aa'}{ss'}$$

$$0_{S^{-1}\mathcal{A}} = \frac{0}{1} \text{ and } 1_{S^{-1}\mathcal{A}} = \frac{1}{1}$$

Then $(S^{-1}\mathcal{A}, 0_{S^{-1}\mathcal{A}}, 1_{S^{-1}\mathcal{A}}, +, \cdot)$ is a ring.

Proof. One can check that the above ring operation and $0, 1$ are well-defined. e.g.

$$\frac{a}{b} \cdot \frac{0}{1} \overset{?}{=} \frac{0}{1}$$
$$\Longleftrightarrow \frac{a \cdot 0}{b \cdot 1} \overset{?}{=} \frac{0}{1}$$
$$\Longleftrightarrow \frac{0}{b} \overset{?}{=} \frac{0}{1}$$
$$\Longleftrightarrow \exists t \in S : 0 \cdot 1 \cdot t = 0 \cdot b \cdot t \checkmark$$

and if $(a, s) \sim (b, t)$, then

$$\frac{a}{s} + \frac{a'}{s'} \overset{?}{=} \frac{b}{r} + \frac{a'}{s'}$$
$$\Longleftrightarrow \frac{as' + a's}{ss'} \overset{?}{=} \frac{bs' + a'r}{rs'}$$
$$\Longleftrightarrow \exists t \in S : tss'(bs' + a'r) = trs'(as' + a's)$$
$$\Longleftrightarrow \exists t \in S : tsbs'^2 = tras'^2 \checkmark$$

$\square$

Remark 3.6. *The above definition does not exclude the possibility that S contains zero. But if $0 \in S$ then we trivially have $\frac{a}{s} = \frac{0}{1}$, thus $S^{-1}\mathcal{A} = \{0\}$.*

We say $S^{-1}\mathcal{A}$ is **localization of $\mathcal{A}$ with respect to** S. When $\mathcal{A}$ is an integral domain, $S = \mathcal{A} - \{0\}$ is multiplicative closed, the $S^{-1}\mathcal{A} = Frac(\mathcal{A})$.

Lemma 3.7. *There exists a ring morphism ι from $\mathcal{A}$ to $S^{-1}\mathcal{A}$ s.t each $a \in \mathcal{A}$ maps to $a/1 \in S^{-1}\mathcal{A}$. It has the following properties:*

(a) $\iota(S) \subset (S^{-1}\mathcal{A})^{\times}$

(b) $Ker(\iota) = \{a \in \mathcal{A} | sa = 0 \text{ for some } s \in S\}$

(c) Suppose $\mathcal{A} \neq \{0\}$. Then ι is injective $\Longleftrightarrow S$ contains no zero divisors.

(d) $S^{-1}\mathcal{A} = \{0\} \Longleftrightarrow S \ni 0$

(e) ι is isomorphism $\Longleftrightarrow S \subseteq \mathcal{A}^{\times}$

Proof. We can easily check that ι thus defined is indeed a ring morphism.

   (a) $s \in S$. $\iota(s) = s/1$ and $s/1 \cdot 1/s = 1$, then s is a unit in $S^{-1}\mathcal{A}$.

   (b) $a \in \text{Ker}(\iota) = \{b \in \mathcal{A} | \frac{b}{1} = \frac{0}{1}\} \Longleftrightarrow \exists t \in S : t(a1 - 01) = ta = 0$.

(c) derived from (a) and (b).

(d) $S^{-1}\mathcal{A} = \{0\} \iff \frac{0}{1} = \frac{1}{1} \iff$ there exists an element $t \in S$ s.t. $t \cdot 1 = 0$, $\iff t = 0 \in S$.

(e) "$\implies$" Suppose $\mathcal{A} \neq \{0\}$, then ι is isomorphism $\iff \iota$ is surjective and injective. The surjectivity is equivalent to $\forall \frac{a}{s} \in S^{-1}\mathcal{A} : \exists c \in \mathcal{A}$ s.t. $\frac{a}{s} = \frac{c}{1}$ while the injectivity is equivalent to S has no zero-divisors according to (c). Then we know, $\frac{1}{s} = \frac{c}{1} \implies \exists t \in S$, such that $t(s \cdot c - 1) = 0$, and by the fact S has no zero-divisors $s \cdot c = 1$, which means $S \subseteq \mathcal{A}^{\times}$.
"$\impliedby$" Assume $\mathcal{A} \neq \{0\}$. $S \subseteq \mathcal{A}^{\times}$, then S does not contain any zero divisors. $\forall \frac{a}{s} \in S^{-1}\mathcal{A}$. Because $S \subseteq \mathcal{A}^{\times} \exists v \in \mathcal{A}$ s.t. $sv = 1$. Then $\frac{a}{s} = \frac{av}{1} \in \mathrm{Im}(\iota)$, because $asv = a$.

If $\mathcal{A} = \{0\}$, the claim is trivially true.

$\square$

Example 3.8. *X any set, $U \subseteq X$ any subset. $\mathcal{A} := \{functions\ f : X \longrightarrow \mathbb{R}\}$ is a ring of the the multiplication is defined value-wisely, $S := \{f \in \mathcal{A} | f(x) \neq 0, \forall x \in U\}$ is multiplicatively closed. Question, what is the localization $S^{-1}\mathcal{A}$?*

Lemma 3.9. *X any set, $U \subseteq X$ any subset. $\mathcal{A} := \{functions\ f : X \longrightarrow \mathbb{R}\}$. Let $\mathcal{B} := \{functions\ U \longrightarrow \mathbb{R}\}$. Then the natural map $j : S^{-1}\mathcal{A} \longrightarrow \mathcal{B}$ is an isomorphism $\frac{a}{s} \mapsto [U \ni x \mapsto \frac{a(x)}{s(x)} \in \mathbb{R}]$*

Proof. j is well-defined: Say $\frac{a}{s} = \frac{a'}{s'}$. Thus $\exists t \in S, as't = a'st$. Then $(a(x)s(x) - a'(x)s'(x))t(x) = 0$, where $t(x) \neq 0 \forall x \in U$. Then by the properties of real numbers $\frac{a(x)}{s(x)} = \frac{a'(x)}{s'(x)}$.

Try defining $k : \mathcal{B} \longrightarrow S^{-1}\mathcal{A}$, $b \longmapsto \tilde{b}/1$, where

$$\tilde{b} : X \longrightarrow \mathbb{R}$$

$$\tilde{b} = \begin{cases} b(x), & x \in U \\ 0, & x \notin U \end{cases}$$

$j \circ k = \mathbb{1}$, $b \in \mathcal{B}$ $\frac{\tilde{b}(x)}{1(x)} = b(x) \forall x \in U$.

$k \circ j = \mathbb{1}$. Say $b = j(\frac{a}{s})$ is an element in $\mathcal{B}$, $k(b) = \frac{\tilde{b}}{1}$, what we want is $\tilde{b}/1 = a/s$, i.e. $\exists t \in S : (a \cdot 1 - \tilde{b} \cdot s)t = 0$.

Take $t : 1_U = [x \mapsto 1$ for $x \in U$ and 0 for $x \notin U]$. Done. $\square$

Universal property of localization

Lemma 3.10. $Hom(S^{-1}\mathcal{A}, \mathcal{B}) \cong \{f : \mathcal{A} \longrightarrow \mathcal{B} \text{ s.t. } f(S) \subseteq \mathcal{B}^\times\}$. *For an element* $\tilde{f} \in Hom(S^{-1}\mathcal{A}, \mathcal{B})$

$$\tilde{f}\left(\frac{a}{s}\right) := f(a)f(s)^{-1}$$

$$f(a) := \tilde{f}\left(\frac{a}{1}\right).$$

i.e. For every morphism $f : \mathcal{A} \longrightarrow \mathcal{B}$ *s.t.* $f(S) \subseteq \mathcal{B}^\times$, *there exists a unique morphism* $\tilde{f} : S^{-1}\mathcal{A} \longrightarrow \mathcal{B}$ *s.t.* $f = \tilde{f} \circ \iota$, *where* ι *is the canonical morphism* $\iota : \mathcal{A} \longrightarrow S^{-1}\mathcal{A} : a \mapsto \frac{a}{1}$.

$$S \lhook\joinrel\longrightarrow \mathcal{A} \xrightarrow{f} \mathcal{B}$$
$$\downarrow{\scriptstyle\iota} \quad \nearrow_{\exists!\tilde{f}}$$
$$S^{-1}\mathcal{A}$$

This universal property of localization can serve as an alternative definition of localization, where $S^{-1}\mathcal{A}$ *is defined to be a pair* (T, ι) *so that any morphism* f, $f : \mathcal{A} \longrightarrow \mathcal{B}, f(S) \subseteq \mathcal{B}^\times$ *would factor through* T *by* $f = \tilde{f} \circ \iota$.

Proof. Want: $\forall f$ as above $\exists! \tilde{f}$ s.t. $\tilde{f} \circ \iota = f$

    Uniqueness:
$\tilde{f}(a/s) = \tilde{f}(a/1)\tilde{f}(s/1)^{-1} = f(a)f(s)^{-1}$.

    Existence :

Take $\tilde{f}(a/s) := f(a)f(s)^{-1}$, check that it is well defined:

$$\frac{a}{s} = \frac{a'}{s'} \overset{?}{\Longrightarrow} f(a)f(s)^{-1} = f(a')f(s')^{-1}.$$

This is guaranteed, $\exists t \in S : as't = a'st \Longrightarrow (f(a)f(s') - f(a')f(s))f(t) = 0$ and $f(t) \in \mathcal{B}^\times \Longrightarrow f(a)f(s') - f(a')f(s) = 0$. $\qquad\square$

Example 3.11. *(Most Important Examples)*

- $\mathcal{A} \ni f$, $S_f := \{f^n | n \geq 0\}$ *is multiplicatively closed.* $\mathcal{A}_f := S_f^{-1}\mathcal{A}$.

- $\mathfrak{p} \subset \mathcal{A}$ *is a prime ideal, then* $S_{\mathfrak{p}} := \mathcal{A} - \mathfrak{p}$ *is multiplicatively closed (In fact then* $\mathcal{A} - \mathfrak{p}$ *being multiplicatively closed is equivalent to* $\mathfrak{p}$ *being prime). We can define* $\mathcal{A}_{\mathfrak{p}} := S_{\mathfrak{p}}^{-1}\mathcal{A}$.

Caution that if $\mathfrak{p} = (f)$, *usually* $\mathcal{A}_{(f)} \neq \mathcal{A}_f$.

Consider $\varphi : \mathcal{A} \longrightarrow \mathcal{B}$ and $\mathfrak{a} \subseteq \mathcal{A}, \mathfrak{b} \subseteq \mathcal{B}$. We have defined in Definition 1.30 the extension and contraction of ideals as $\mathfrak{b}^c = \varphi^*(\mathfrak{a}) := \varphi^{-1}(\mathfrak{b})$ and $\mathfrak{a}^e = \varphi_*(\mathfrak{a}) := \mathcal{B}\varphi(\mathfrak{a})$. **Notice that $\mathfrak{q} \subseteq \mathcal{B}$ prime $\implies \varphi^*(\mathfrak{q})$ prime, thus $\varphi^* : \mathbf{Spec}(\mathcal{B}) \longrightarrow \mathbf{Spec}(\mathcal{A})$.**

Back to the special case $\iota : \mathcal{A} \longrightarrow S^{-1}\mathcal{A}$.

Lemma 3.12. *S is a multiplicative set in a ring $\mathcal{A}$, then for the canonical morphism $\iota : \mathcal{A} \longrightarrow S^{-1}\mathcal{A}$:*

(a) *For any ideal $\mathfrak{a} \subseteq \mathcal{A}$, $\iota_*(\mathfrak{a}) = \{a/s | a \in \mathfrak{a}, s \in S\}$.*

(b) *For a general ideal $\mathfrak{q} \subseteq S^{-1}\mathcal{A}, \iota^*(\mathfrak{q}) \xleftrightarrow{bij} \mathfrak{q} \cap \{\frac{a}{1} | a \in \mathcal{A}\}$.*

(c) *$\iota_*(\mathfrak{a}) = S^{-1}\mathcal{A} \iff \mathfrak{a} \cap S \neq \emptyset$.*

(d) *For any ideal $\mathfrak{b} \subseteq S^{-1}\mathcal{A}$, $\iota_*(\iota^*(\mathfrak{b})) = \mathfrak{b}$.*

Proof.

(a) Denote $V := \iota(\mathfrak{a}) = \{\frac{a}{1} | a \in \mathfrak{a}\}$, and then we check that $\iota_*(\mathfrak{a}) := S^{-1}\mathcal{A} \cdot V = \{\frac{a}{s} | a \in \mathfrak{a}, s \in S\}$.

(b) Similarly, we choose an ideal $\mathfrak{q} \subseteq S^{-1}\mathcal{A}$ and check that $\iota^*(\mathfrak{q}) := \iota^{-1}(\mathfrak{q}) \ni a \longmapsto \frac{a}{1} \in \mathfrak{q}$ and for an $\frac{b}{1} \in \mathfrak{q} \cap \{\frac{c}{1} | c \in \mathcal{A}\} \longmapsto b \in \mathcal{A}$, which gives the one to one correspondence.

(c) $\iota_*(\mathfrak{a}) = S^{-1}\mathcal{A} \iff \exists a \in \mathfrak{a}, s \in S$ s.t. $a/s = 1/1 \iff \exists t \in S$ s.t. $\mathfrak{a} \ni ta = ts \in S$, then $\mathfrak{a} \cap S \neq \emptyset$. Conversely, $\mathfrak{a} \cap S \neq \emptyset$, any $a \in \mathfrak{a}, a = s \in S$, then $a/s = 1/1$.

(d) See Proposition 1.31, $\iota_*(\iota^*(\mathfrak{b})) \subset \mathfrak{b}$ in general. For the converse inclusion, if $a/s \in \mathfrak{b}$, then $a/s \cdot s/1 = a/1 \in \mathfrak{b}$, which means $a \in \iota^*(\mathfrak{b}) \implies a/s \in \iota_*(\iota^*(\mathfrak{b}))$. This claims means every ideal in $S^{-1}\mathcal{A}$ is extension of an ideal in $\mathcal{A}$.

$\square$

Remark by TeXer 3.13. *Notice that $\mathfrak{q} \cap \{\frac{a}{1} | a \in \mathcal{A}\}$ is not necessarily an ideal in $S^{-1}\mathcal{A}$. Explicit example shows that ι_* does not in general preserves the proper inclusion "$\subsetneq$". Let $\mathcal{A} := \mathbb{Z}$, $S := \{2^n : n \in \mathbb{Z}_{\geq 0}\}$, then $S^{-1}\mathcal{A} = \mathbb{Z}[1/2]$, $(2) \supsetneq (4)$ in $\mathcal{A}$ but $\iota_*((2)) = \iota_*((4)) = S^{-1}(\mathcal{A})$. But however, unlike general φ^*, ι^* indeed preserves the proper inclusion. $\iota_*(\iota^*(\mathfrak{b})) = \mathfrak{b} \subsetneq \mathfrak{a} = \iota_*(\iota^*(\mathfrak{a})) \implies \iota^*(\mathfrak{b}) \subsetneq \iota^*(\mathfrak{a})$. Or equivalently, $\frac{c}{s} \notin \mathfrak{a} \implies \frac{c}{1} \notin \mathfrak{a} \implies c \notin \iota^*(\mathfrak{a})$. The fact that ι^* preserves proper inclusion is crucial for the claim $dim(\mathcal{A}_\mathfrak{p}) = ht(\mathfrak{p})$.*

Lemma 3.14. *$\mathcal{A}$ a ring and S is a multiplicative set in $\mathcal{A}$. Let $\iota : \mathcal{A} \longrightarrow S^{-1}\mathcal{A}$, then we have*

    (a) $\iota^*\iota_*(\mathfrak{a}) = \cup_{s \in S}(\mathfrak{a} : s)$

    (b) ι_* commutes with formation of finite sums, products, intersections and taking radicals.

Proof.   (a) $x \in \iota^*\iota_*(\mathfrak{a}) \Longrightarrow \frac{x}{1} \in \iota_*\mathfrak{a} = \left\{ \frac{y}{s} : y \in \mathfrak{a}, s \in S \right\}$

       "$\subseteq$": Suppose $\frac{x}{1} = \frac{y}{s}$ for some $y \in \mathfrak{a}, s \in S$. Then $\exists t \in S$ s.t. $t(xs - y) = 0$ $\Longrightarrow stx = yt \in \mathfrak{a} \Longrightarrow x \in (\mathfrak{a} : st)$, where $st \in S$.

       "$\supseteq$": Say $x \in (\mathfrak{a} : s)$ for some $s \in S$. Thus $xs =: y \in \mathfrak{a}$. Then $\frac{x}{1} = \frac{y}{s} \in \iota^*\iota_*\mathfrak{a}$.

    (b) We know form exercise that in general $\mathrm{rad}(\varphi_*\mathfrak{a}) \supseteq \varphi_*(\mathrm{rad}(\mathfrak{a}))$, then in particular, we have $\mathrm{rad}(\iota_*\mathfrak{a}) \supseteq \iota_*(\mathrm{rad}(\mathfrak{a}))$. For the reverse inclusion, we check if $\frac{x}{s} \in \mathrm{rad}(\iota_*\mathfrak{a})$, then exists $n \in \mathbb{N}$, s.t. $\left(\frac{x}{s} \right)^n \in \iota_*\mathfrak{a}$. $\frac{x^n}{s^n} = \frac{y}{t} \in \iota_*\mathfrak{a}$, $\exists u \in S$ s.t. $ux^nt = us^ny \in \mathfrak{a}$, then $(uxt)^n \in \mathfrak{a} \Longrightarrow uxt \in \mathrm{rad}(\mathfrak{a}) \Longrightarrow \frac{x}{s} \in \iota_*(\mathrm{rad}(\mathfrak{a}))$.
                                                                  $\square$

3.2   Lecture 8.   Properties of Localization of Rings

Recall $\iota : \mathcal{A} \longrightarrow S^{-1}\mathcal{A}$

- $\iota_*(\mathfrak{a}) = \left\{ \frac{a}{s} | a \in \mathfrak{a}, s \in S \right\}$

- $\iota_*\iota^*(\mathfrak{b}) = \mathfrak{b}, \forall \mathfrak{b} \subseteq S^{-1}\mathcal{A}$

- $\iota_*\mathfrak{a} = (1) \Longleftrightarrow \mathfrak{a} \cap S \neq \emptyset$

Proposition 3.15. *S is a multiplicative set in a ring $\mathcal{A}$, then for the canonical morphism $\iota : \mathcal{A} \longrightarrow S^{-1}\mathcal{A}$:*

$$\iota_* : \left\{ \mathfrak{p} \in Spec(\mathcal{A}) | \mathfrak{p} \cap S = \emptyset \ (S \subseteq \mathcal{A} - \mathfrak{p}) \right\} \longleftrightarrow \left\{ Spec(S^{-1}\mathcal{A}) \right\}$$

is bijection with the inverse ι^*.

Proof. The proof contains the following points

    (a) $\mathfrak{p}$ prime $\Longleftrightarrow \iota_*\mathfrak{p}$ prime,

    (b) $\iota^*\iota_*\mathfrak{p} = \mathfrak{p}$, (True for only prime ideal $\mathfrak{p}$ which satisfies $\mathfrak{p} \cap S = \emptyset$. If $\mathfrak{p} \cap S \neq \emptyset$, $\iota^*\iota_*\mathfrak{p} = \mathcal{A}$)

(c) $\iota_*(\mathfrak{a}) = S^{-1}\mathcal{A} \iff \mathfrak{a} \cap S \neq \emptyset$, (True for any ideals)

(d) $\iota_*\iota^*\mathfrak{q} = \mathfrak{q}$ (True for any ideal of $S^{-1}\mathcal{A}$, not necessarily prime),

of which (c) and (d) have been proved in Lemma 3.12.

We prove point (b). See Proposition 1.31, $\iota^*\iota_*\mathfrak{p} \supseteq \mathfrak{p}$ is a general fact. For the converse inclusion, $\iota^*\iota_*\mathfrak{p} = \iota^{-1}(\iota_*\mathfrak{p}) \overset{?}{\subseteq} \mathfrak{p}$, choose an $a \in \iota^{-1}(\iota_*\mathfrak{p})$. $\iota(a) = \frac{a}{1} \in \iota_*\mathfrak{p} \implies \exists b \in \mathfrak{p}, s \in S$ s.t. $\frac{a}{1} = \frac{b}{s} \implies ast = bt \in \mathfrak{p}$ and $s, t \in S \subseteq \mathcal{A} - \mathfrak{p} \implies a \in \mathfrak{p}$ because $\mathfrak{p}$ is a prime ideal.

As for point (a), $\mathfrak{p}$ prime $\overset{?}{\implies} \iota_*\mathfrak{p}$ prime. Consider $\frac{a}{s} \cdot \frac{b}{t} \in \iota_*\mathfrak{p}$, then $\frac{ab}{st} = \frac{c}{u}, c \in \mathfrak{p}, u \in S$, then $\exists v \in S : abuv = cstv$, where $uv \in S$ $cstv \in \mathfrak{p}$, $uv \notin \mathfrak{p} \implies ab \in \mathfrak{p} \implies$ at least one of $a, b \in \mathfrak{p} \implies$ at least one of $\frac{a}{s}, \frac{b}{t} \in \iota_*\mathfrak{p}$. $\square$

Remark by TeXer 3.16. *With the one to one correspondence, we can see that ι^* and ι_* preserve the inclusion, whats more, they preserve proper inclusion "$\subsetneq$" of $\{$prime ideals $\mathfrak{p}$, s.t. $\mathfrak{p} \cap S = \emptyset\}$ and $\{$prime ideals in $S^{-1}\mathcal{A}\}$.*

- $\mathfrak{q}_1 \subsetneq \mathfrak{q}_2 \iff \iota^*\mathfrak{q}_1 \subsetneq \iota^*\mathfrak{q}_2$,

- $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \iff \iota_*(\mathfrak{p}_1) \subsetneq \iota_*(\mathfrak{p}_2)$.

Definition 3.17. $k(\mathfrak{p}) := Frac(\mathcal{A}/\mathfrak{p})$ *is called the **residue field at (the point) prime ideal** $\mathfrak{p}$. Then the above bijection induces isomorphism $k(\iota^*\mathfrak{q}) \cong k(\mathfrak{q})$.*

$$k(\iota^*\mathfrak{q}) = Frac(\mathcal{A}/\iota^*\mathfrak{q}) \cong Frac(S^{-1}\mathcal{A}/\mathfrak{q}) = k(\mathfrak{q})$$

Proof. Claim: there is an injective homomorphism form the integral domain $\mathcal{A}/\iota^*\mathfrak{q}$ to $S^{-1}\mathcal{A}/\mathfrak{q}$.

$$\bar{\iota} : \mathcal{A}/\iota^*\mathfrak{q} \longrightarrow S^{-1}\mathcal{A}/\mathfrak{q}$$
$$a + \iota^*\mathfrak{q} \longmapsto \frac{a}{1} + \mathfrak{q}$$

$\iota_*\iota^*\mathfrak{q} = \mathfrak{q} \implies \mathrm{Ker}(\bar{\iota}) = 0 + \iota^*\mathfrak{q}$. And see for example this StackExchange answer, a injective morphism of integral domains induces a injective morphism of fraction fields. The induced morphism of fraction field is

$$Frac(\bar{\iota}) : \frac{a + \iota^*\mathfrak{q}}{b + \iota^*\mathfrak{q}} \longmapsto \frac{\frac{a}{1} + \mathfrak{q}}{\frac{b}{1} + \mathfrak{q}}$$

Lets check that it is in fact surjective:

$$\frac{\frac{f_1}{s_1} + \mathfrak{q}}{\frac{f_2}{s_2} + \mathfrak{q}} \sim \frac{\frac{f_1 s_2}{1} + \mathfrak{q}}{\frac{f_2 s_1}{1} + \mathfrak{q}} = Frac(\bar{\iota}) \left(\frac{f_1 s_2 + \iota^* \mathfrak{q}}{f_2 s_1 + \iota^* \mathfrak{q}} \right)$$

$\square$

Example 3.18. $\mathcal{A} = \mathbb{Z}$, and $\mathfrak{p} = (p)$ where p is a prime number. $k(\mathfrak{p}) = Frac(\mathbb{Z}/p) = \mathbb{Z}/p$.

If $\mathfrak{p} = (0)$, $k(\mathfrak{p}) = Frac(\mathbb{Z}) = \mathbb{Q}$.

If $\mathfrak{p} = \mathfrak{m}$ a maximal ideal. $\Longleftrightarrow \mathcal{A}/\mathfrak{p}$ is a field and $k(\mathfrak{p}) = \mathcal{A}/\mathfrak{p}$

Example 3.19. $\mathfrak{p} = (y) \subseteq \mathcal{A} = \mathbb{C}[x,y]$, $\mathcal{A}/\mathfrak{p} \cong \mathbb{C}[x], k(\mathfrak{p}) \cong \mathbb{C}(x)$

Example 3.20. $S = S_f = \{f^n : n \geq 0\} \implies S^{-1}\mathcal{A} = \mathcal{A}_f = \mathcal{A}[1/f]$. Let $\mathfrak{p} \cap S \neq \emptyset \iff$ some $f^n \in \mathfrak{p} \leftrightarrow f \in \mathfrak{p}$. Then $Spec(\mathcal{A}_f) \cong \{\mathfrak{p} \in Spec(\mathcal{A}) | f \notin \mathfrak{p}\}$

Example 3.21. $\mathcal{A} = \mathbb{Z}, f = 2, \mathcal{A}_f = \mathbb{Z}[1/2]$

$\{primes\ in\ \mathbb{Z}[1/2]\} \cong \{(0), (3), (5)....\} \subseteq Spec(\mathbb{Z})$.

Example 3.22. $\mathcal{A} = \mathbb{C}[X,Y]$, there is a bijection between $\{maximal\ ideals\ in\ \mathcal{A}\}$ and $\mathbb{C}^2$. The maximal ideal $\{f \in \mathbb{C}[X,Y] | f(x_0, y_0) = 0\} = (X - x_0, Y - y_0)$ corresponds to the point $(x_0, y_0) \in \mathbb{C}^2$.

Fix $f \in \mathbb{C}[X,Y], f \neq 0, e.g. f = Y - X^2$. Then

$$\{maximal\ ideals\ in\ \mathcal{A}_f = \mathbb{C}[X, f, 1/f]\}$$

$$\overset{bij}{\longleftrightarrow} \{maximal\ ideals\ \mathfrak{m} \in \mathbb{C}[X,Y] s.t. f \notin \mathfrak{m}\}$$

$$\overset{bij}{\longleftrightarrow} \{(x, y) \in \mathbb{C}^2 | f(x, y) \neq 0\}$$

Then we know that the $Spm(\mathcal{A}) \cong \mathbb{C}^2$ while $Spm(\mathcal{A}_f)$ is bijective to the complement of zero loci of f.

Remark 3.23. *The localization at an element has the functorial property, for $f, g \in \mathcal{A}$*

$$\mathcal{A} \longrightarrow \mathcal{A}_f \overset{\iota'}{\longrightarrow} \mathcal{A}_{fg}$$

where ι' means localize $\mathcal{A}_f$ at the image of g in $\mathcal{A}_f$.

Example 3.24. $\mathcal{A}$ *an integral domain,* $\mathcal{A}_f \subseteq \mathcal{A}_{fg}$ $\left(\frac{a}{(f)^n} = \frac{ag^n}{(fg)^n}\right)$. *Then we know* $Frac(\mathcal{A}) = colim_{f \in \mathcal{A} - \{0\}} \mathcal{A}_f$.

For any $\mathfrak{p} \in Spec(\mathcal{A}_f) \subseteq Spec(\mathcal{A})$,

$\mathcal{A}_f \hookrightarrow k(\mathfrak{p})$ *as subring,* $\frac{a}{f^n} \longmapsto \frac{a(\mathfrak{p})}{f(\mathfrak{p})^n}$.

$\{f \in \mathcal{A} : f \notin \mathfrak{p}\} = \{f \in \mathcal{A} : f(\mathfrak{p}) \neq 0\}$, *where* $f(\mathfrak{p}) \in k(\mathfrak{p})$ *is the image of* f, $f(\mathfrak{p}) := f \mod \mathfrak{p}$.

Aside: $\mathcal{A}$ is a local ring $\iff \exists! \mathfrak{m} \in \mathrm{Spec}(\mathcal{A}) \iff \exists$ ideal $\mathfrak{m}$ with $1 + \mathfrak{m} \subseteq \mathcal{A}^\times$, $\mathfrak{m}$ maximal, $\iff \mathcal{A} - \mathfrak{m} \subseteq \mathcal{A}^\times$

Proposition 3.25.

(a) $Spec(\mathcal{A}_\mathfrak{p}) \cong \{\mathfrak{q} \in Spec(\mathcal{A}) | \mathfrak{q} \subseteq \mathfrak{p}\}$

(b) *For* $\iota : \mathcal{A} \longrightarrow S_\mathfrak{p}^{-1}\mathcal{A}$, $\mathcal{A}_\mathfrak{p}$ *is a local ring with maximal ideal* $\mathfrak{p}_\mathfrak{p} := \iota_*(\mathfrak{p}) = \mathfrak{p}\mathcal{A}_\mathfrak{p}$,

$\mathcal{A}_\mathfrak{p}$ *is called the* **localization of** $\mathcal{A}$ **at** $\mathfrak{p}$. ι_* *is inclusion preserving.*

Proof. By Proposition 3.15,

$$\mathrm{Spec}\left(S_\mathfrak{p}^{-1}\mathcal{A}\right) \stackrel{\iota_*}{\cong} \{\mathfrak{q} \in \mathrm{Spec}(\mathcal{A}) | \mathfrak{q} \cap S_\mathfrak{p} = \emptyset \ (\mathfrak{q} \subseteq \mathfrak{p})\},$$

which finishes the proof of part (a). On the other hand, ι_* is inclusion preserving, $\implies$ every prime ideal in $\mathcal{A}_\mathfrak{p}$ is contained in $\mathfrak{p}_\mathfrak{p}$. using this and the fact that any ideal is contained in some maximal ideal, we see that $\mathfrak{p}_\mathfrak{p} \subseteq \mathcal{A}_\mathfrak{p}$ is the maximal ideal. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\square$

Example 3.26. $\mathfrak{p} = (p) \subseteq \mathbb{Z} = \mathcal{A}$, *then* $\mathcal{A}_\mathfrak{p} = \mathbb{Z}_{(p)}$ *is local ring with maximal ideal* $\mathfrak{p}_\mathfrak{p}$ *generated by image of* $\mathfrak{p}$. $Spec(\mathbb{Z}_{(p)}) \cong \{\mathfrak{q} \in Spec(\mathbb{Z}) | \mathfrak{q} \subseteq \mathfrak{p}\} = \{(0), (p)\})$

For residue field $\mathbb{Z}_{(p)}/\mathfrak{p}_\mathfrak{p} \cong \mathbb{Z}/(p)$, *this isomorphism is by the first part of the first prop of today's lecture. And in general*

$$\mathcal{A}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} = k(\mathfrak{p})$$

Definition 3.27. *A* **germ at** p *is an equivalence class* $[(U, f)]$ *of pairs* (U, f), *where* $p \in U \subseteq \Omega$ *and* $f : U \longrightarrow \mathbb{C}$ *holomorphic. And* $(U_1, f_1) \sim (U_2, f_2)$ *iff* $f_1 = f_2$ *on some open neighborhood of* p *inside* $U_1 \cap U_2$

Lemma 3.28. $\Omega \subseteq \mathbb{C}$ *open* $\mathcal{A}$ *is the set of holomorphic germs* $f : \Omega \longrightarrow \mathbb{C}$. *Fix* $p \in \Omega$. *and set* $\mathfrak{p} = \{f \in \mathcal{A} | f(p) = 0\}$. *Then* $\mathcal{A}$ *is a local ring with maximal ideal* $\mathfrak{p}$

Proof. <u>Want</u> $\mathcal{A} - \mathfrak{p} \subseteq \mathcal{A}^\times$

 This is just a way of saying : if $f(p) \neq 0$, then there is an open neighborhood of p on which $1/f$ is defined and holomorphic. $\square$

Example 3.29. $\mathcal{A} = \mathbb{C}[X, Y], \mathfrak{p} = (Y)$, $\mathcal{A}_\mathfrak{p} = \mathbb{C}(X)[Y]$

$$Spec(\mathcal{A}_\mathfrak{p}) \cong \{\mathfrak{q} \in Spec(\mathcal{A}) | \mathfrak{q} \subseteq (Y)\}$$

Then, the only choice of $\mathfrak{q}$ is just $(Y), (0)$. $\mathcal{A}_\mathfrak{p}$ is a local ring with two primes, and residue field $\mathbb{C}(X)$.
  $\mathcal{A} = \mathbb{C}[X, Y], \mathfrak{p} = (X, Y)$

$$Spec(\mathcal{A}_\mathfrak{p}) \cong \{\mathfrak{q} \in Spec(\mathcal{A}) | \mathfrak{q} \subseteq (X, Y)\}$$

Then

$$Spec(\mathcal{A}_\mathfrak{p}) \cong \{(X, Y)\} \cup \{(f) : 0 \neq f \in \mathbb{C}[X, Y] \ irreducible \ , f(0, 0) = 0\} \cup \{(0)\}.$$

The second set is just the set of plane curves passing through 0.

Localization of Module

Definition 3.30. *$S \subseteq \mathcal{A}$ and M is an $\mathcal{A}$-module. Then we define the **localization of module***

$$(m, s) \in M \times S, (m, s) \sim (m', s') \iff \exists t \in S : tsm' = ts'm$$

and we denote the equivalence class of (m, s) by $\frac{m}{s}$, and we see that $S^{-1}M$ is in fact an $S^{-1}\mathcal{A}$-module:
$$\frac{a}{s} \cdot \frac{m}{t} = \frac{am}{st}$$

Lemma 3.31. *$S^{-1}\mathcal{A} \otimes_\mathcal{A} M \cong S^{-1}M$, where the map is $\frac{a}{s} \otimes m \mapsto \frac{am}{s}$*

Proof. We can define the inverse

$$\frac{1}{s} \otimes m \longleftarrow \frac{m}{s}$$

and then check it is well-defined. $\square$

 Moreover, we can also define the localization of morphisms,

Definition 3.32. *Given $f : M \longrightarrow N$ a morphism of $\mathcal{A}$-module. S^{-1}. We define*

$$S^{-1}f :S^{-1}M \longrightarrow S^{-1}N$$

$$\frac{m}{s} \longmapsto \frac{f(m)}{s}.$$

It is a well-defined morphism of $S^{-1}\mathcal{A}$-modules and it has the functorial property

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

e.g. $\mathfrak{p} \in Spec(\mathcal{A})$, then we have the localization $\mathcal{A}_{\mathfrak{p}}$ and the localization of module:
$M_{\mathfrak{p}} := S_{\mathfrak{p}}^{-1}M \cong \mathcal{A}_{\mathfrak{p}} \otimes_{\mathcal{A}} M.$

Next time: we will focus other local properties i.e.properties of M that depends only on $M_{\mathfrak{p}}, \forall \mathfrak{p} \in \mathrm{Spec}(\mathcal{A})$

3.3   Lecture 9-1. Localization of Modules and Local Properties

Recall that given a multiplicative closed set $S \subseteq \mathcal{A}$, we can define $S^{-1}\mathcal{A}$. Also we can define **localization of modules:** $S^{-1}M \cong S^{-1}\mathcal{A} \otimes_{\mathcal{A}} M$. The localization of module defines a functor S^{-1}: $f : M \longrightarrow N$, induces a morphism of $S^{-1}\mathcal{A}$-modules $S^{-1}f : S^{-1}M \longrightarrow S^{-1}N$ and $S^{-1}(f \circ g) = S^{-1}f \circ S^{-1}g$. Moreover S^{-1} is an exact functor:

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

is exact, then so is

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

Proof. $g \circ f = 0 \implies S^{-1}g \circ S^{-1}f = 0$, then we have $\mathrm{Ker}(S^{-1}g) \supseteq \mathrm{Im}(S^{-1}f)$. For the converse inclusion, consider an element $\frac{x}{s} \in \mathrm{Ker}(S^{-1}g) x \in M s \in S$, $\implies S^{-1}g(\frac{x}{s}) = \frac{g(x)}{s} = \frac{0}{1}, \implies \exists t \in S$ s.t. $g(tx) = tg(x) = 0$. $\mathrm{Im}(f) = \mathrm{Ker}(g) \implies \exists y : f(y) = tx$. Then we check that $\frac{x}{s} = (S^{-1}f)(\frac{y}{st}) = \frac{f(y)}{st} = \frac{tx}{ts} = \frac{x}{s}$, which concludes the proof. $\square$

Corollary 3.33. $S^{-1}\mathcal{A}$ *is flat $\mathcal{A}$-module.*

Proof. Let $0 \longrightarrow M' \longrightarrow M$ be injective(exact). What we want is

$$0 \longrightarrow S^{-1}\mathcal{A} \otimes_{\mathcal{A}} M' \longrightarrow S^{-1}\mathcal{A} \otimes_{\mathcal{A}} M$$

is exact because it is just

$$0 \longrightarrow S^{-1}M \longrightarrow S^{-1}M$$

$\square$

Lemma 3.34. S^{-1} *commutes with:*

- *finite sums*

- *finite intersections*

- *Kernel* $(Ker(S^{-1}M \longrightarrow S^{-1}N) \cong S^{-1}(Ker(M \longrightarrow N)))$

- *quotients*

- *tensor products* $(S^{-1}(M \otimes_{\mathcal{A}} N) \cong S^{-1}M \otimes_{S^{-1}\mathcal{A}} S^{-1}N)$

Proof. We just prove the last one of it by constructing the isomorphism explicitly,

$$\frac{x \otimes_{\mathcal{A}} y}{s} \longmapsto \frac{x}{s} \otimes_{S^{-1}\mathcal{A}} \frac{y}{1} \sim \frac{x}{1} \otimes_{S^{-1}\mathcal{A}} \frac{y}{s}$$

$$\frac{x}{s} \otimes_{S^{-1}\mathcal{A}} \frac{y}{t} \longmapsto \frac{x \otimes_{\mathcal{A}} y}{st}$$

$\square$

Local Properties

M is an $\mathcal{A}$-module

Lemma 3.35. ***Being zero is a local property*** *i.e. the followings are equivalent:*

(a) $M = 0$

(b) $M_{\mathfrak{p}} = 0, \forall \mathfrak{p}$ *primes*

(c) $M_{\mathfrak{m}} = 0, \forall \mathfrak{m}$ *maximals*

Claim 1: Let $x \in M$, then $x \neq 0 \iff \mathrm{Ann}(x) := \{a \in \mathcal{A} | ax = 0\} \neq (1)$

Proof. $x \neq 0 \iff 1 \cdot x \neq 0 \iff 1 \notin \mathrm{Ann}(x) \iff \mathrm{Ann}(x) \neq (1)$. $\square$

Calim 2: $\mathfrak{m}$ maximal $x \in M$. Then $x \notin \mathrm{Ker}(M \longrightarrow M_{\mathfrak{m}}) \iff \mathrm{Ann}(x) \subseteq \mathfrak{m}$.

Proof. $x \in \mathrm{Ker}(M \longrightarrow M_{\mathfrak{m}}) \iff \exists s \in \mathcal{A} - \mathfrak{m}$ s.t. $\frac{x}{1} = \frac{0}{s} \implies \exists t \in \mathcal{A} - \mathfrak{m} : tsx = 0$
$\iff \mathrm{Ann}(x) \not\subseteq \mathfrak{m}$.

$\square$

Proof. (of Lemma 3.35). It suffices to prove that (c)$\Longrightarrow$(a), which amounts to show that $M \neq 0 \Longrightarrow \exists \mathfrak{m} \subset \mathcal{A}$ s.t. $M_\mathfrak{m} \neq 0$

Let $0 \neq x \in M$, by Claim 1,

$\Longrightarrow \mathrm{Ann}(x) \neq (1) \Longrightarrow \exists maxmal\ ideal\ \mathfrak{m} \supseteq \mathrm{Ann}(x)$. Then by Claim 2,

$x \notin \mathrm{Ker}(M \longrightarrow M_\mathfrak{m}) \Longrightarrow M_\mathfrak{m} \neq 0$ $\qquad\qquad\square$

Proposition 3.36. *(Injectivity/Surjectivity are local)*

M is an $\mathcal{A}$-module, then the following are equivalent.

(a) $M \xrightarrow{\phi} N$ *is injective/surjective*

(b) $M_\mathfrak{p} \xrightarrow{\phi_\mathfrak{p}} N_\mathfrak{p}$ *is injective/surjective for all $\mathfrak{p}$ primes*

(c) $M_\mathfrak{m} \xrightarrow{\phi_\mathfrak{m}} N_\mathfrak{m}$ *is injective/surjective for all $\mathfrak{m}$ maximals.*

Proof. We prove the statements about surjectivity.

$M \longrightarrow N \longrightarrow K := N/\phi(M) \longrightarrow 0$ is exact.

$\Longrightarrow M_\mathfrak{p} \longrightarrow N_\mathfrak{p} \longrightarrow K_\mathfrak{p} \longrightarrow 0$ is exact $\forall \mathfrak{p}$.

ϕ is surjective $\longleftrightarrow K = 0$

$\Longleftrightarrow K_\mathfrak{p} = 0, \forall \mathfrak{p}$ by Lemma 3.35

$\Longleftrightarrow K_\mathfrak{p} = 0 \forall \mathfrak{p}$

$\Longleftrightarrow \phi_\mathfrak{p}$ surjective $\forall \mathfrak{p}$ prime. We can replace the prime ideal by maximal ideal and prove it similarly.

For the statement of injectivity, we can analogously prove it by starting from the exact sequence $0 \longrightarrow \mathrm{Ker}(\phi) \longrightarrow M \xrightarrow{\phi} N$. $\qquad\qquad\square$

Proposition 3.37. *(Flatness is local)*

M is an $\mathcal{A}$-module, then the followings are equivalent.

(a) $\mathcal{A}$-module M is flat

(b) $\mathcal{A}_\mathfrak{p}$-module $M_\mathfrak{p}$ is flat $\forall \mathfrak{p}$ prime

(c) $A_\mathfrak{m}$-module $M_\mathfrak{m}$ is flat $\forall \mathfrak{m}$ maximal ideals.

Proof. We prove e.g. (a)$\Longleftrightarrow$(b): Suppose $N \hookrightarrow P$.

<u>Want:</u> $[N \otimes M \hookrightarrow P \otimes M] \Longleftrightarrow [(N \otimes M)_\mathfrak{m} = (N_\mathfrak{m} \otimes_{\mathcal{A}_\mathfrak{m}} M_\mathfrak{m}) \hookrightarrow P_\mathfrak{m} \otimes_{\mathcal{A}_\mathfrak{m}} M_\mathfrak{m} = (P \otimes M)_\mathfrak{m} \forall \mathfrak{m}]$

$\Longleftarrow N_\mathfrak{m} \hookrightarrow P_\mathfrak{m} \forall \mathfrak{m}$

$\Longleftrightarrow N \hookrightarrow P$ by Proposition 3.36. $\qquad\qquad\square$

4 Noetherian Rings and Nullstellensatz

4.1 Lecture 9-2. Chain Conditions and Noetherian Rings

Definition 4.1. *(Lemma) The following characterizations are equivalent:*

(a) *$\mathcal{A}$ satisfies the* **ascending chain condition on ideals (ACC)** *(All the sequence $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq ...$ stabilizes, i.e. $\exists n_0$ s.t. $\mathfrak{a}_n = \mathfrak{a}_{n_0} \forall n \geq 0$)*

(b) *Every ideal of $\mathcal{A}$ is finitely generated.*

(c) *$\{$ideals in $\mathcal{A}\}$ satisfies the* **maximal property***: i.e. Every subset contains a maximal element. That is : For any nonempty collection S of ideals in $\mathcal{A}$, $\exists \mathfrak{a} \in S$ s.t. $\forall \mathfrak{b} \in S \Longrightarrow \mathfrak{b} \not\supsetneq \mathfrak{a}$*

Then, $\mathcal{A}$ is called **Noetherian**

Proof.
(a)$\Longrightarrow$(b). Let $\mathfrak{a}$ be an ideal. we may assume that $\mathfrak{a}$ is **NOT** finitely generated. Inductively construct $x_1, x_2, x_3... \in \mathfrak{a}$ such that $(x_1) \neq 0$ and $\mathfrak{a} \supsetneq (x_1, x_2) \supsetneq (x_1)$ an also $\mathfrak{a} \supsetneq (x_1, x_2, x_3) \supsetneq (x_1, x_2)$, but then this sequence contradict the **ACC**.

(a)$\Longrightarrow$(c). Let $\emptyset \neq S \subseteq \{$ideals in $\mathcal{A}\}$. If S violates the maximal property, then start from arbitrary ideal $\mathfrak{a}_1$, we can find $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \in S$. Similarly, we can find $\mathfrak{a}_{j+1} \supsetneq \mathfrak{a}_j, \forall j \in \mathbb{Z}_{\geq 0}$ by the countable choice axiom. Then the ACC fails.

(c)$\Longrightarrow$(a). If ACC fails, $\exists \mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq ...$ Take $S := \{\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3...\}$. Then S violates maximal property.

(b)$\Longrightarrow$(a). Let $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq ...$ <u>Want:</u>show that $\exists n_0, \mathfrak{a}_n = \mathfrak{a}_{n_0} \forall n \geq n_0$. Define $\mathfrak{a} := \cup_n \mathfrak{a}_n$. We know that every ideal of $\mathcal{A}$ is finitely generated. Then $\mathfrak{a}$ is also finitely generated by assumption (b). Then Assume it to be finitely generated by r elements $\{x_1, ..., x_r\}$, with $x_j \in \mathfrak{a}_{n_j}$. Choose $n_0 = \max\{n_1, ..., n_r\}$, then we have $x_1, ..., x_r \in \mathfrak{a}_{n_0} \Longrightarrow \mathfrak{a} = \mathfrak{a}_{n_0}. \Longrightarrow \mathfrak{a}_n = \mathfrak{a}_{n_0}, \forall n \geq n_0.$ $\qquad \square$

Definition 4.2. *(Lemma)*
M is an $\mathcal{A}$-module. The following characterizations are equivalent:

(a) *M has* **ACC** *on submodules*

(b) *Every submodule of M is finitely generated*

(c) *M has the* **maximal property** *on submodules*

Then, we call M a **Noetherian $\mathcal{A}$-module**.

Proof. The proof is just identical. ☐

Note that $\mathcal{A}$ Noetherian ring $\iff \mathcal{A}$ is a Noetherian $\mathcal{A}$-module.

Lemma 4.3. *Let* $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ *be a short exact sequence of* $\mathcal{A}$*-modules. Then* M *is Noetherian* $\iff$ *both* M', M'' *Noetherian.*

Proof. "$\Longleftarrow$". Use ACC. Let $N_1 \subseteq N_2 \subseteq ...$ be submodules of M. <u>Want:</u> show that $\exists n_0 : (n \geq n_0) \Longrightarrow N_n = N_{n_0}$. Consider $N_j'' :=$ Image of N_j in M''. $N_1'' \subseteq N_2'' \subseteq ...$ By ACC of M'', $N_{n_0}'' = N_n'' \forall n \geq n_0$. Do the same for $N_j' := M' \cap N_j$ $(M' \hookrightarrow M)$ Need: if $N_i \subseteq N_j \subseteq M$ and $N_i'' = N_j'', N_i' = N_j'$, then $N_i = N_j$. (Five Lemma)

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & N_i' & \longrightarrow & N_i & \longrightarrow & N_i'' & \longrightarrow & 0 \\
 & & \| & & \downarrow & & \| & & \\
0 & \longrightarrow & N_j' & \longrightarrow & N_j & \longrightarrow & N_j'' & \longrightarrow & 0
\end{array}
$$

For the "$\Longrightarrow$" direction, we can use the definition of Noetherian module to prove directly that **Any submodule of a Noetherian module is Noetherian** and **Any quotient module of Noetherian module is Noetherian**. ☐

Corollary 4.4. *In particular, any finitely generated module* M *over a Noetherian ring* $\mathcal{A}$ *is Noetherian* $\mathcal{A}$*-module.*

Proof. Suppose M is generated by $\{x_1, ..., x_n\}$ We always have a SES

$$0 \longrightarrow Ker(\varphi) \longrightarrow \mathcal{A}^n \xrightarrow{\varphi} M \longrightarrow 0,$$

then apply the above lemma. ☐

4.2 Lecture 10. Hilbert Basis Theorem

In general, any finitely generated module over an Noetherian ring is Noetherian.

Theorem 4.5. *(Hilbert basis theorem)* $\mathcal{A}$ *Noetherian* $\Longrightarrow$ *the polynomial ring* $\mathcal{A}[X]$ *is Noetherian.*

Proof. Let $\mathfrak{a} \subseteq \mathcal{A}[X]$. <u>Want:</u> show $\mathfrak{a}$ finitely generated.

$$
\begin{aligned}
\mathfrak{a}' &= \{\text{Leading coefficients of } \mathfrak{a}\} \\
&= \cup_{n \geq 0} \{\mathfrak{a} \in \mathcal{A} : \exists a X^n + ... \in \mathfrak{a}\}
\end{aligned}
$$

Because $\mathcal{A}$ is Noetherian, $\mathfrak{a}'$ is finitely generated. $\implies \mathfrak{a}' = (a_1, ..., a_r), a_i \in \mathfrak{a}'$
$\implies \exists f_1, ..., f_r \in \mathfrak{a} : f_j = a_j X^{n_j} + ...$

Set $N := max(n_1, .., n_r)$ and we construct $\mathcal{A}$-module $M := \oplus_{j=0}^N \mathcal{A} X^j \subseteq \mathcal{A}[X]$.
$M \cap \mathfrak{a}$ is finitely generated because $M \cong \mathcal{A}^N$ as $\mathcal{A}$-module, and $\mathcal{A}$ is a Noetherian
$\mathcal{A}$-module $\implies \mathcal{A}^n$ is Noetherian $\mathcal{A}$-module:

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

Using the above exact sequence, we can apply Lemma 4.3 and induct on n.

And finally, we claim that

$$\mathfrak{a} = (f_1, ..., f_r) + M \cap \mathfrak{a}$$

The $\supseteq$ part is obvious.

Let $f \in \mathfrak{a}$ with $f = aX^n + ...$, where $n \geq (n_1, ..., n_r)$. Then $a \in \mathfrak{a}'$ by definition

$$\mathfrak{a}' = (a_1, ..., a_r)$$
$$\implies a = c_1 a_1 + ... + c_r a_r \text{ with } c_1, ..., c_r \in \mathcal{A}$$
$$\implies \exists f_1 = a_1 X^{n_1} +, ..., f_r = a_r X^{n_r} \in \mathfrak{a}$$
$$\text{know } f - (c_1 X^{n-n_1} f_1 + ... + c_r x^{n-n_r} f_r) = (a - \sum c_j a_j)x^n + ...$$
$$= 0 + \text{some terms in } \mathfrak{a} \text{ of degree less than } n - 1$$

Then we can induct from $n, n-1, ...$ to N, we get that $f \in (f_1, ..., f_r) + M \cap \mathfrak{a}$

$$\mathfrak{a} \subseteq (f_1, ..., f_r) + M \cap \mathfrak{a} \subseteq \mathfrak{a}$$
$$\implies \mathfrak{a} = (f_1, ..., f_r) + M \cap \mathfrak{a}'$$

hence we know $\mathfrak{a}$ is finitely generated. $\square$

Remark by TeXer 4.6. *The converse of Hilbert basis theorem is also true:*
$\mathcal{A}$ Noetherian $\iff \mathcal{A}[X]$ is Noetherian. The converse can be easily proved by
Lemma 4.10.

Remark by TeXer 4.7. *With some modification, we can prove that the formal*
prower series $\mathcal{A}[[X]]$ is Noetherian if $\mathcal{A}$ is Noetherian. The basic idea is to replace
the leading term coefficients with coefficients of least degree term, see for example:
this online text.

Applications:

- By induction on n, we can prove that $\mathcal{A}[X_1, ..., X_n]$ is also Noetherian.

- Any finitely generated $\mathcal{A}$-algebra $\mathcal{A}[x_1, ..., x_r] = \mathcal{A}[X_1, ..., X_r]/\mathfrak{a}$ Noetherian if $\mathcal{A}$ is Noetherian.

- Recall that a variety $V \subseteq \mathbb{C}^d$ is a subset defined by polynomial equations, i.e. $V = V(S)$ for some $S \subseteq \mathbb{C}[X_1, ..., X_d] =: \mathcal{A}$. $V(S) = \{x \in \mathbb{C}^d : f(x) = 0 \forall f \in S\}$. Note $V(S) = V(\langle S \rangle)$, where $\langle S \rangle$ is the ideal generated by S. Hilbert basis theorem $\implies \forall$varieties $V \exists$ finite $S \subseteq \mathbb{C}[x_1, ..., x_d]$ such that $V = V(S)$. **Any set of polynomial equations is the same as some finite system.**

   Proof. Given S, we have $\mathfrak{a} = \langle S \rangle \subseteq \mathbb{C}[X_1, ..., X_d]$. By Hilbert basis theorem 4.5, $\mathbb{C}[X_1, ..., X_d]$ Noetherian $\implies \mathfrak{a}$ finitely generated $\iff \mathfrak{a} = (f_1, ..., f_r)$ $\qquad \square$

Example 4.8. *Any field is Noetherian in that it have only two ideals (0) and itself. A field is finitely generated as an ideal in it self with the generating set $\{1\}$.*

   Any principal ideal domain is Noetherian, because all the ideals are finitely generated by definition.

Non-example 4.9. *$\mathcal{A} = \mathbb{C}[x_1, x_2, ...]$ is not Noetherian: $\mathfrak{m} := (x_1, x_2, ...)$ is Not finitely generated. If $S \subseteq \mathfrak{m}$ is finite, we may find some x_n not occurring in any element of S: $\implies x_n \notin \langle S \rangle, x_n \in \mathfrak{m}$.*

   The ring of algebraic integers in not Noetherian, for example, it contains an infinite ascending chain of principal ideals: $(2) \subsetneq (2^{1/2}) \subsetneq (2) \subsetneq (2^{1/4})...$

Lemma 4.10. *$\mathcal{A}$ Noetherian $\implies$ any homomorphic image of $\mathcal{A}$ is Noetherian:*

Proof. The image if of the form $\mathcal{A}/\mathfrak{a}$ for some $\mathfrak{a} \subseteq \mathcal{A}$. $0 \longrightarrow \mathfrak{a} \longrightarrow \mathcal{A} \longrightarrow \mathcal{A}/\mathfrak{a} \longrightarrow 0$. Because there is a one to one inclusion preserving correspondence between the $\{$ideals in $\mathcal{A}$ that contains $\mathfrak{a}\}$ and $\{$ ideals in $\mathcal{A}/\mathfrak{a}\}$. The maximal condition also holds in $\mathcal{A}/\mathfrak{a}$. $\qquad \square$

Lemma 4.11. *Localization of Noetherian ring are Noetherian. $S \subseteq \mathcal{A}$ is multiplicative set $S^{-1}\mathcal{A}$, e.g. $\mathcal{A}_\mathfrak{p}, \mathcal{A}_f$ are Noetherian if $\mathcal{A}$ is Noetherian.*

Proof. Remember that $S^{-1}\mathcal{A}$ is not a homomorphic image of $\mathcal{A}$. By Proposition 3.15, there is a one to one inclusion preserving correspondence between $\{$ideals in $\mathcal{A}$ which does not intersect $S\}$ and $\{$ideals in $S^{-1}\mathcal{A}\}$. Then the maximal property is also inherited to $S^{-1}\mathcal{A}$. $\qquad \square$

Remark by TeXer 4.12. *Notices that "the localizations of $\mathcal{A}$ is Noetherian at every primes does not imply "that $\mathcal{A}$ it self is Noetherian ". See for example this* [StackExchange answer](). *In other words, being Noetherian is not a local property.*

Definition 4.13. *An $\mathcal{A}$-**algebra** is a ring $\mathcal{B}$ together with a homomorphism $f : \mathcal{A} \longrightarrow \mathcal{B}$.*

Example 4.14. *$\mathcal{A}[X_1, ..., X_n]$ and $\mathcal{A}[x_1, ..., x_n]$ are an $\mathcal{A}$-algebra, with the obvious choice of f.*

Example 4.15.

Any ring is a $\mathbb{Z}$-algebra:

$$\mathbb{Z} \longrightarrow \mathcal{B}$$
$$n \longmapsto n \cdot 1_{\mathcal{B}}$$

Example 4.16. *If $\mathcal{A}$ is a field $\mathbb{F}$, any ring homomorphism between $\mathbb{F}$ and a nonzero ring $\mathcal{B}$ is injective, $\mathbb{F} \hookrightarrow \mathcal{B}$. Thus an $\mathbb{F}$-algebra $\mathcal{B}$ is "the same as" a ring $\mathcal{B}$ that contains $\mathbb{F}$ as a subfield.*

Example 4.17. *Let $\mathcal{B}$ be any field of characteristic p, if $p = 0$, then $\mathcal{B}$ is a $\mathbb{Q}$-algebra, if $p > 0$, $\mathcal{B}$ is an $\mathbb{F}_p$-algebra.*

Definition 4.18. *We say that an $\mathcal{A}$-algebra $\mathcal{B}$ if a **finitely generated $\mathcal{A}$-algebra** is there exists $x_1, ..., x_n \in \mathcal{B}$ s.t. $\mathcal{B}$ is $\mathcal{A}[x_1, .., x_n]$.*

*Given two $\mathcal{A}$-algebra $\mathcal{A} \xrightarrow{f} \mathcal{B}$ and $\mathcal{A} \xrightarrow{g} \mathcal{C}$. A **morphism of $\mathcal{A}$-algebra** is defined to be a ring homomorphism that commutes with f, g*

$$\mathcal{B} \xrightarrow{t} \mathcal{C}$$
$$f \uparrow \quad \nearrow g$$
$$\mathcal{A}$$

Proposition 4.19. *By the Hilbert basis theorem 4.5, we know if $\mathcal{A}$ is Noetherian, the finitely generated $\mathcal{A}$-algebra $\mathcal{B}$ is Noetherian.*

Proof. $\mathcal{B}$ is a finitely generated $\mathcal{A}$-algebra

$$\Longleftrightarrow \exists n \geq 0 \quad \exists h : \mathcal{A}[X_1, ..., X_n] \longrightarrow \mathcal{B}, h \text{ surjective}$$

then we have the derivation: $\mathcal{A}$ Noetherian $\Longrightarrow \mathcal{A}[X_1, ..., X_n]$ Noetherian, it surjectively maps to $\mathcal{B}$, $\mathcal{B}$ is a homomorphism image of a Noetherian ring. By Lemma 4.10 we have $\mathcal{B}$ is Noetherian. $\qquad \square$

Definition 4.20. *Let $\mathcal{B}$ be an $\mathcal{A}$-algebra. We say that $\mathcal{B}$ is a* **finite $\mathcal{A}$-algebra** *if it is finitely generated as $\mathcal{A}$-module.*

Remark 4.21. *Equivalently, we say $\mathcal{B}$ is finite $\mathcal{A}$-algebra iff there exists a surjective $\mathcal{A}$-module homomorphism from $\mathcal{A}^n$ to $\mathcal{B}$. In general, $\mathcal{B}$ is finite $\mathcal{A}$-algebra implies $\mathcal{B}$ is a finitely generated $\mathcal{A}$-algebra.*

In general, we say $\mathcal{B}$ is **finite over** *$\mathcal{A}$ iff there exists $x_1, ..., x_n \in \mathcal{B}$ s.t., $\mathcal{B} = \{\mathcal{A}$-linear combinations of $x_1, .., x_n\}$.*

Also, we say $\mathcal{B}$ is **finitely generated over** *$\mathcal{A}$ iff there exists $x_1, ..., x_n \in \mathcal{B}$ s.t., $\mathcal{B} = \{$polynomials in $x_1, ..., x_n$ with coefficients in $\mathcal{A}\}$.*

Example 4.22. *Assume $\mathcal{A} := \mathbb{Z}$:*

$\mathcal{B}$	$finite$	$fintely\ generated$
$\mathbb{Z}$	✓	✓
$\mathbb{Z}\left[\frac{1}{2}\right]$	✗	✓
$\mathbb{Q}$	✗	✗
$\frac{1}{2}\mathbb{Z}$	✓	N/A

The last row is somehow not a good example because $\frac{1}{2}\mathbb{Z}$ is not a ring.

Theorem 4.23. *(Zariski's Lemma) Assume K a field, $K \subseteq L$, where L is also a field. Assume L is a finitely generated K-algebra, then L is a finite K-algebra which is equivalent to L/K being a finite algebraic field extension.*

Corollary 4.24. *The maximal ideal of $\mathcal{A} = \mathbb{C}[X_1, ..., X_d]$ are all of the form $\mathfrak{m}_x = (X_1 - x_1, ..., X_d - x_d)$ for some $x \in \mathbb{C}^d$.*

Proof. Theorem 4.23 $\implies$ Cor, Let $\mathfrak{m} \subseteq \mathcal{A}$ be any maximal ideal, then $L = \mathcal{A}/\mathfrak{m}$ is a field.

$$\mathbb{C} \longrightarrow \mathbb{C}[X_1, ..., X_d] = \mathcal{A} \xrightarrow{\ q\ } L = \mathcal{A}/\mathfrak{m}$$
$$j$$

Note: L is a finitely generated $\mathbb{C}$-algebra, generated by $q(X_1), ..., q(X_d)$

$$\text{Theorem 4.23} \implies L/j(\mathbb{C}) \text{ is finite field extension}$$
$$\implies L \cong \mathbb{C}(\mathbb{C} \text{ algebraically closed})$$

Set $x := (j^{-1}(q(X_1)), ..., j^{-1}(q(X_d))) \in \mathbb{C}^d$. Check $\mathfrak{m} = \mathfrak{m}_x$. We know j is surjective because q is, and j is always injective because $\mathbb{C}$ is a field. Suppose

$P \in \mathfrak{m} \implies q(P) = 0 \implies j^{-1}(P(q(X))) = 0 \implies P(j^{-1}(P(X))) = P(x) = 0$, hence $\mathfrak{m}_x \in \mathfrak{m}$, but we already know $\mathfrak{m}_x$ is maximal, then $\mathfrak{m} = \mathfrak{m}_x$. The above proof also works for all algebraically closed fields. $\qquad\square$

Corollary 4.25. *Let $d \geq 1$. Then $\mathbb{C}(X_1, ..., X_d)$ is **NOT** a finitely generated $\mathbb{C}$-algebra.*

Proof. $K = \mathbb{C}, L = \mathbb{C}(X_1, .., X_d)$. Obviously $\mathbb{C}(X_1, ..., X_d)$ can not be a finite $\mathbb{C}$-algebra, for example $\{X_1^n\}$ are $\mathbb{C}$-linear independent. Then L/K not finite field extension $\implies L$ is NOT finitely generated $\mathbb{C}$-algebra (by Theorem 4.23).

This proof also works when $\mathbb{C}$ replaced with any field K.

Alternatively, we can also prove this directly. Suppose $K(X_1, ..., X_d)$ is finitely generated by $f_1, .., f_n \in K(X_1, .., X_d)$, each $f_i = \frac{g_i}{h_i} \in K[X_1, ..., X_d]$. Set $u :=$ $1 + X_1 h_1 \cdots h_n \implies 1/u \notin K[f_1, .., f_n]$ because denominator is coprime to the denominators of the f_j. We get the contradiction. $\qquad\square$

Then we come back to the proof of the Theorem 4.23

Proof. Any L generated by $x_1, ..., x_n$. Any L/K NOT finite. Then the transcendence degree d is larger than $1 \iff$ after reordering $x_1, ..., x_n$, $x_1, ..., x_d$ algebraically independent over K and $x_{d+1}, ..., x_n$ is algebraic over $K(x_1, ..., x_d)$. $x_{d+1}, ..., x_n$ is algebraic over $K(x_1, .., x_d)$ which means L is algebraic field extension over $K(x_1, ..., x_d)$. Also, $x_1, ..., x_d$ are transcendental over $K \implies K[x_1, ..., x_d] \cong K[X_1, ..., X_d]$ where the capital X_i means indeterminates, hence $K(x_1, ..., x_d) \cong K(X_1, ..., X_d)$. But by the alternative proof (not dependent on this Theorem) of Corollary 4.25, we know $K(x_1, ..., x_d) \cong K(X_1, ..., X_d)$ is not finitely generated K-algebra. The rest part of the proof is postponed until the next lecture. $\qquad\square$

4.3   Lecture 11. Nullstellensatz

Recall, F a field. V a vector space over F. $S \subseteq F$ is linear independent. $\forall$ distinct $\{s_1, ..., s_n\} \subseteq S$, $\forall c_1, ..., c_n \in F$, $c_1 s_1 + ... + c_n s_n = 0 \implies c_i = 0$

Theorem 4.26. $S \subseteq V$, *vector space over F.*

(a) *Suppose S is linear independent. Then S is **maximal**$\iff S$ spans V.*

(b) *Suppose $\{v_1, ..., v_n\} \subseteq V$ is maximal linear independent $=:$ "basis", Suppose $\{w_1, ..., w_m\} \subseteq V$ linearly independent. Then $m \leq n$*

(c) *Any two bases have the same cardinality($=$ the dimension of V).*

(d) *Every vector spaces has a basis.*

(e) *Every linearly independent subset $S \subseteq V$ extends to a basis.*

(f) *If $S \subseteq V$ spans V, then $\exists$ basis $T \subseteq S$*

   Then what will happen when we replace "linearly independent " by "algebraic independent"? Now let E/F be a field extension call $S \subseteq E$ **algebraically independent over** F, if $\forall$ distinct $\{s_1, ..., s_n\} \subseteq S$, $\forall p \in F[X_1, ..., X_n]$ $p(s_1, ..., s_n) = 0 \implies p = 0$.

Theorem 4.27. *E/F field extension.*

(a) *Suppose $S \subseteq E$ is algebraic independent. Then S is maximal $\iff E/F(S)$ is an algebraic field extension (Union of finite field extension).*

(b) *If $\{v_1, .., v_n\} \subseteq E$(algebraic independent maximal)=: "**transcendence basis**" and $\{w_1, ..., w_m\} \subseteq E$ algebraic independent then $m \leq n$*

(c) *Any two transcendence bases have the same cardinality(Then we can define the transcendence degree of E/F, denote it by tr.deg(E/F))*

(d) *Every E/F has a transcendence basis.*

(e) *Any algebraic independent $S \subseteq E$ extends to a transcendence basis.*

(f) *If $S \subseteq E$ and $E/F(S)$ is algebraic, then exists transcendence basis T of E/F and $T \subseteq S$*

Proof. (a) "$\implies$" Assume S maximal algebraic independent. <u>Want</u>: $E/F(S)$ is algebraic. Let $\alpha \in E$, want: $F(\alpha, S)/F(S)$ is finite. If $\alpha \in S$, then done. If not, $S \cup \{\alpha\}$ is not algebraic independent. So we can find $s_1, ..., s_n \in S$ and a nontrivial polynomial relation between $\alpha, s_1, ..., s_n$. This relation must involve α. Then $\exists m \geq 1$, $p_0, ..., p_m \in F[X_1, ..., X_n]$ s.t $\alpha^m p_m(s_1, ..., s_n) + ... + \alpha p_1(s_1, ..., s_n) + p_0(s_1, ..., s_n) = 0$ with $p_m \neq 0 \implies [F(\alpha, s_1, ..., s_n) : F(s_1, ..., s_n)] \leq m \implies \alpha$ is algebraic over $F(S)$.

"$\impliedby$", If $E/F(S)$ is algebraic, <u>Want:</u> S maximal. Indeed, suppose otherwise $\exists \alpha \in E, \alpha \notin S$ s.t. $S \cup \{\alpha\}$ is algebraic independent. Then α is algebraic over $F(S)$, by assumption. $\exists m \geq 1$

$$\alpha^m + \frac{p_{m-1}(s_1, ..., s_n)}{q_{m-1}(s_1, .., s_n)} \alpha^{m-1} + ... = 0$$

for some $s_1, ..., s_n \in S, p_i, q_i \in F[X_1, ..., X_n]$ Multiply the denominators in the above equation, we get a nontrivial polynomial relation involving $s_1, ..., s_m, \alpha$. Contrary to the assumed algebraic independence of $S \cup \{\alpha\}$

$\square$

Example 4.28.
$tr.deg(\overline{\mathbb{Q}}/\mathbb{Q}) = 0$
$tr.deg(\mathbb{C}/\mathbb{Q}) = \infty$
$tr.deg(F(t_1, ..., t_n)/F) = n$
If $E/F(t_1, ..., t_n)$ is algebraic, then $tr.deg(E/F)$ is n
    $tr.deg(F/F) = 0 \iff (E/F)$ is algebraic.

And then we resume our proof of Zariski's Lemma (Theorem 4.23) in last lecture. Give a field extension L/K such that L is finitely generated as K-algebra, then L/K is finite.

Proof. (of Theorem 4.23) Write $L = K[x_1, ..., x_n]$ and denote $r := \text{tr.deg}(L/K)$. The conclusion that L is a finite algebraic field extension is equivalent to $r = 0$. Suppose not. Then $r \geq 1$. By part (f) of the Theorem 4.27 that after relabeling, $\{x_1, ..., x_r\}$ is a transcendence basis of L/K. Each $x_{r+1}, ..., x_n$ is algebraic over $K(x_1, .., x_r) =: A \implies L/A$ is finite field extension, i.e., L is a finite dimensional A-vector space. Now we know

$$\underbrace{\overbrace{K \hookrightarrow A := K(x_1, ..., x_r)}^{(?)} \overbrace{\hookrightarrow L}^{\text{f.g. } A\text{-vec.sp}}}_{\text{f.g. } K\text{-algebra}} .$$

<u>Want</u>: A is a finitely generated K-algebra.

Then we incorporate the following lemma by Artin-Tate.

Lemma 4.29. *Let $\mathcal{A} \subseteq \mathcal{B} \subseteq \mathcal{C}$ be rings s.t. $\mathcal{C}$ is finitely generated as $\mathcal{A}$-algebra and $\mathcal{C}$ is also finitely generated $\mathcal{B}$-module. Then $\mathcal{B}$ is a finitely generated $\mathcal{A}$-algebra. In other word, we have*

$$\underbrace{\overbrace{\mathcal{A} \longrightarrow \mathcal{B}}^{(*)} \overbrace{\longrightarrow \mathcal{C}}^{\text{f.g. } \mathcal{B}\text{-module}}}_{\text{f.g. } \mathcal{A}\text{-algebra}},$$

and $(*)$ is indeed a finitely generated $\mathcal{A}$-algebra.

Proof. (Of Lemma 4.29) $\mathcal{C} = \langle y_1, ..., y_m \rangle_{\mathcal{B}-mod}$ and $\mathcal{C} = \langle x_1, ..., x_n \rangle_{\mathcal{A}-alg}$ write $x_i = \sum_j b_{ij} y_j$ for some $b_{ij} \in \mathcal{B}$. $y_i \cdot y_j = \sum_k b_{ijk} y_k$. Define $\mathcal{B}_0 := \mathcal{A}[\{b_{ij}\} \cup \{b_{ijk}\}] \subseteq$

$\mathcal{B}$. We know $\mathcal{B}_0$ is a finitely generated $\mathcal{A}$-algebra, by Hilbert basis theorem 4.5, $\mathcal{B}_0$ is Noetherian. On the other hand, we know

$$\mathcal{C} = \{\text{polynomials in } \{x_j\} \text{ with coefficients in } \mathcal{A}\}$$

and by the above substitution,

$$\mathcal{C} = \{\text{linear combinations of } y_i \text{ with coefficients in } \mathcal{B}_0\}$$

$\Longrightarrow \mathcal{C}$ is a finitely generated $\mathcal{B}_0$-module.
$\Longrightarrow \mathcal{C}$ is a Noetherian $\mathcal{B}_0$-module.
$\Longrightarrow$ the $\mathcal{B}_0$-submodule $\mathcal{B} \subseteq \mathcal{C}$ is finitely generated.
$\Longrightarrow \mathcal{B}$ is finitely generated $\mathcal{A}$-algebra (Still by the substitution). $\qquad\square$

But by the alternative proof (not dependent on Theorem 4.23) of Corollary 4.25, we know $K(x_1, ..., x_d) \cong K(X_1, ..., X_d)$ is not finitely generated K-algebra, which contradicts the above lemma. $\qquad\square$

We can derive the Nullstellensatz form Zariski's Lemma.

Corollary 4.30. *(Hilbert's Nullstellensatz)*

$$rad(\mathfrak{a}) = I(V(\mathfrak{a})),$$

where $K = \overline{K}$ is an algebraically closed field. $\mathfrak{a} \subseteq K[X_1, ..., X_d] = \mathcal{A}$. $V(\mathfrak{a}) : \{x \in K^d, f(x) = 0 \forall f \in \mathfrak{a}\}$. $I(S) = \{f \in \mathcal{A} : f(x) = 0 \forall x \in S\}$ and $rad(\mathfrak{a} := \{f \in \mathcal{A} : f^n \in \mathfrak{a} \text{ for some } n\}$

Proof. $rad(\mathfrak{a}) \subseteq I(V(\mathfrak{a}))$, $f \in rad(\mathfrak{a}) \Longrightarrow f^n \in \mathfrak{a} \Longrightarrow f^n|_{V(\mathfrak{a})=0}$, and K is an integral domain $\Longrightarrow f|_{V(\mathfrak{a})} = 0 \Longrightarrow f \in I(V(\mathfrak{a}))$.

For the converse inclusion recall that $rad(\mathfrak{a}) = \cap_{\mathfrak{p} \supseteq \mathfrak{a}, prime} \mathfrak{p}$. suppose $f \notin rad(\mathfrak{a})$. <u>Want:</u> $f \notin I(V(\mathfrak{a}))$. Choose $\mathfrak{p} \supseteq \mathfrak{a}, \mathfrak{p} \not\ni f$. Then $0 \neq \overline{f} \in \mathcal{A}/\mathfrak{p}$. $\Longrightarrow (\mathcal{A}/\mathfrak{p})_{\overline{f}} = (\mathcal{A}/\mathfrak{p})[1/\overline{f}] \neq 0$. Choose a maximal ideal $\mathfrak{m} \subseteq (\mathcal{A}/\mathfrak{p})_{\overline{f}} =: \mathcal{B}$. Set $L := \mathcal{B}/\mathfrak{m}$ a field, L is finitely generated K-algebra. $\Longrightarrow L/K$ is finite $\Longrightarrow L = K$ because $\overline{K} = K$. Set $x := (x_1, ..., x_d)$, $x_j :=$ image of X_j in L. Check that $f(x) \neq 0$ and $x \in V(\mathfrak{a}) \Longrightarrow f \notin I(V(\mathfrak{a}))$.

$$K[X_1, ..., X_d] = \mathcal{A} \xrightarrow{\pi} \mathcal{A}/\mathfrak{p} \xrightarrow{\iota} \mathcal{B} = (\mathcal{A}/\mathfrak{p})[1/\overline{f}] \xrightarrow{\pi'} L = \mathcal{B}/\mathfrak{m} = K$$

$$j$$

We denote $j : \mathcal{A} \longrightarrow L$. Indeed, $x \in V(\mathfrak{a})$ because $\forall g \in \mathfrak{a}$ $g(x) = g(j(X)) = j(g(X)) = \pi' \circ \iota \circ \pi(g) = 0$. And $f(x) = j(f) = \pi' \circ \iota \circ \pi(f) = \pi' \circ \iota(\overline{f}) \neq 0$ because $\iota(\overline{f})$ is a unit in $\mathcal{B}$ thus $\iota(\overline{f}) \notin \mathfrak{m}$. $\qquad \square$

5 Primary Decomposition

Consider $\alpha \in \mathcal{A}$ a PID. We may write uniquely $\alpha = \epsilon (p_1)^{n_1} \cdots (p_k)^{n_k}$ where ϵ unit and p_j distinct primes and $(\alpha) = (p_1^{n_1}) \cap ... \cap (p_k^{n_k})$ We call this the primary decomposition of (α). What happens to a general ring?

Definition 5.1. *$\mathcal{A}$ is a general ring. An ideal $\mathfrak{q} \subseteq \mathcal{A}$ is **primary** iff every zero-divisor in $\mathcal{A}/\mathfrak{q}$ is nilpotent.*

Recall $\mathfrak{p} \subseteq \mathcal{A}$ is prime iff the only zero-divisor in $\mathcal{A}/\mathfrak{p}$ is 0. We know

$$\text{prime} \implies \text{primary}$$

Equivalently, we can define: an ideal $\mathfrak{q}$ is primary if, whenever $xy \in \mathfrak{q}$, we have either $x \in \mathfrak{q}$ or $y \in \mathrm{rad}(\mathfrak{q})$. This two definitions are equivalent

Proof. "$\implies$": $xy \in \mathfrak{q} \implies \overline{xy} = \overline{x}\,\overline{y} = 0 \in \mathcal{A}/\mathfrak{q}$. Then both $\overline{x}$ and $\overline{y}$ are zero-divisors in $\mathcal{A}/\mathfrak{q}$, hence $\exists n \in \mathbb{Z}$ s.t. $\overline{y}^n = 0 \in \mathcal{A}/\mathfrak{q} \implies y^n \in \mathfrak{q}$.

"$\impliedby$" $u = x + \mathfrak{q}$ is a zero-divisor in $\mathcal{A}/\mathfrak{q} \implies uv = (x+\mathfrak{q})(y+\mathfrak{q}) = 0 \iff xy \in \mathfrak{q}$, $\implies (y + \mathfrak{q})^n = 0 \in \mathcal{A}/\mathfrak{q} \rightsquigarrow y^n \in \mathfrak{q}$ $\qquad \square$

Remark by TeXer 5.2. *A tautology of the first definition says: $\mathfrak{q} \in \mathcal{A}$ is primary iff $\overline{(0)} \in \mathcal{A}/\mathfrak{q}$ is primary.*

Definition 5.3. *An ideal $\mathfrak{a} \subseteq \mathcal{A}$ is **decomposable** if we may write $\mathfrak{a} = \mathfrak{q}_1 \cap ... \cap \mathfrak{q}_n$, where each $\mathfrak{q}_i$ is primary. We call this a **primary decomposition.***

Proposition 5.4. *$\mathcal{A}$ is Noetherian, $\implies$ every $\mathfrak{a} \subseteq \mathcal{A}$ is decomposable.*

As part of the proof, we discuss the **Noetherian induction** first.
recall the idea of induction in general. **Induction:** $S \subseteq \mathbb{N}$
(I) S has a minimal element.
(II) $1 \in S$ and "$n \in S \implies n + 1 \in S$)"
$\implies S = \mathbb{N}$
Similarly, we can consider **Noetherian Induction**. For $\mathcal{A}$ a Noetherian ring
(I)Every $S \subseteq \{\text{ideals in } \mathcal{A}\}$ has maximal element.
(II) Let $S \subseteq \{\text{ideals in } \mathcal{A}\}$ s.t.

(a) $(1) \in S$

(b) $\mathfrak{a}$ is an ideal in $\mathcal{A}$, $[\forall \mathfrak{b} \supsetneq \mathfrak{a}, \mathfrak{b} \in S] \implies [\mathfrak{a} \in S]$

Then $S = \{\text{ideals in } \mathcal{A}\}$.

This indeed works, because if we can find an ideal $\mathfrak{a} \notin S$ then there $\exists \mathfrak{b} \supsetneq \mathfrak{a}$ s.t. $\mathfrak{a} \notin S$. Repeating this, we can construct an infinite strictly increasing chain of ideals in $\mathcal{A}$, which contradicts the fact that $\mathcal{A}$ is Noetherian.

5.1   Lecture 12. Associated Ideals and First Uniqueness Theorem

Definition 5.5. *An ideal $\mathfrak{a}$ is **irreducible** if whenever $\mathfrak{a} = \mathfrak{a}' \cap \mathfrak{a}''$, we have either $\mathfrak{a} = \mathfrak{a}'$ or $\mathfrak{a} = \mathfrak{a}''$.*

Lemma 5.6. *$\mathcal{A}$ is Noetherian, $\mathfrak{a} \subseteq \mathcal{A}$ is an ideal. $\implies$ $\mathfrak{a}$ **decomposable**: $\exists$ primary ideals $\mathfrak{q}_1, ..., \mathfrak{q}_n \subseteq \mathcal{A}$ s.t. $\mathfrak{a} = \mathfrak{q}_1 \cap ... \cap \mathfrak{q}_n$, where $\mathfrak{q}$ primary $\iff xy \in \mathfrak{q} \implies x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some n.*

Notice $(6) = (2)(3)$ is not irreducible.

Proof.
Claim1: $\mathcal{A}$ Noetherian. Then irreducible $\implies$ primary.

Proof of Claim1

Let $\mathfrak{a}$ be irreducible. Let $x, y \in \mathcal{A}$ with $xy \in \mathfrak{a}$. Assume $x \notin \mathfrak{a}$. <u>Want</u>: $\exists n, y^n \in \mathfrak{a}$. For notational simplicity, we may replace $\mathcal{A}$ by $\mathcal{A}/\mathfrak{a}$ and reduce to the case $\mathfrak{a} = (0)$. (We want to construct a ascending sequence of ideals.) Consider the ideals $\mathrm{Ann}(y^n)$. Theses ideals goes up as n increases $\implies$, $\mathrm{Ann}(y^n) = \mathrm{Ann}(y^{n+1})$ for some n because $\mathcal{A}$ is Noetherian. Then we know, $xy = 0$, $x \in \mathrm{Ann}(y)$, $(x) \subseteq \mathrm{Ann}(y)$.
Subclaim: $\mathrm{Ann}(y) \cap (y^n) = 0$.

Assuming the subclaim,(since (0) is irreducible) deduce that either $\mathrm{Ann}(y) = (0) \implies x \in (0)$ or $(y^n) = (0) \implies y^n = 0$.

Now we turn to prove the subclaim: Let $z \in \mathrm{Ann}(y) \cap (y^n)$. Then $z = y^n t, t \in \mathcal{A}$ and $zy = 0 \implies t y^{n+1} = 0 \implies t \in \mathrm{Ann}(y^{n+1}) = \mathrm{Ann}(y^n) \implies z = t y^n = 0$. This finishes the proof of subclaim thus also the proof of Claim1.
Calim2: $\mathcal{A}$ Noetherian, every ideals in $\mathcal{A}$ is finite intersection of irreducible ideals.

Proof of Claim2: Define:

$$S := \{\text{ideals in } \mathcal{A} \text{ that are finite intersections of irreducible ideals}\}.$$

Consider the complement

$S^c := \{$ideals in $\mathcal{A}$ that are not finite intersections of irreducible ideals$\}.$

<u>Want:</u>$S^c = \emptyset$. If not, then it contains a maximal element $\mathfrak{a}$. Claim $\mathfrak{a} \neq (1)$, because $\mathfrak{a}$ not irreducible.

$\implies \mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}, \mathfrak{b} \supsetneq \mathfrak{a}$, and $\mathfrak{c} \supsetneq \mathfrak{a}$

$\mathfrak{a}$ maximal in S^c, $\mathfrak{b}, \mathfrak{c} \notin S^c$. $\implies \mathfrak{b}, \mathfrak{c} \in S$. So $\mathfrak{b}$ and $\mathfrak{c}$ are finite intersections of irreducible ideals $\implies \mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ is a finite intersection of irreducible ideals. contradiction.

Alternatively, by Noetherian induction, it suffice to show if $\mathfrak{a}$ has the property that " **all strictly larger ideals $\mathfrak{b} \supsetneq \mathfrak{a}$ belongs to** S" $\rightsquigarrow$ "$\mathfrak{a} \in S$". If $\mathfrak{a}$ irreducible, then we are done. If not, there exists $\mathfrak{b} \cap \mathfrak{c}$ s.t. $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$. and $\mathfrak{c}, \mathfrak{b} \supsetneq \mathfrak{a}$. $[\mathfrak{b}, \mathfrak{c} \in S]$ indeed implies $[\mathfrak{a} \in S]$. $\qquad \square$

Basics on primary ideals:

Lemma 5.7. *Let $\mathfrak{q}$ primary. Then $\mathfrak{p} := rad(\mathfrak{q})$ is prime. It is the smallest prime containing $\mathfrak{q}$.*

Proof. 1It suffices to show $\mathfrak{p}$ is prime. ($\mathfrak{p}=$ intersection of all prime ideals containing $\mathfrak{q}$, hence contained in any such prime, hence is the minimal of such primes.) Let $x, y \in \mathcal{A}$, $xy \in \mathfrak{p}, x \notin \mathfrak{p}$. Want $y \in \mathfrak{p}$.
$(xy)^n \in \mathfrak{q}$ for some n. $x^n \notin \mathfrak{q} \implies (y^n)^m \in \mathfrak{q}$ for some $m \implies y \in \mathfrak{p}$. $\qquad \square$

The converse statement is not true.

Definition 5.8. *If $\mathfrak{q}$ is primary with radical $\mathfrak{p}$, we say $\mathfrak{q}$ is $\mathfrak{p}$-**primary**.*

Example 5.9. *All the primary ideals in $\mathbb{Z}$ are of the form (0) and (p^n) , where p is a prime number and n a positive integer. We can check immediately that (p^n) is (p)-primary*

Lemma 5.10. *If $\mathfrak{q}_1, ..., \mathfrak{q}_n$ are all $\mathfrak{p}$-primary, then $\mathfrak{q} = \mathfrak{q}_1 \cap ... \cap \mathfrak{q}_n$ is also $\mathfrak{p}$-primary.*

Proof. $rad(\mathfrak{q}) = rad(\mathfrak{q}_1 \cap ... \cap \mathfrak{q}_n) = rad(\mathfrak{q}_1) \cap ... \cap rad(\mathfrak{q}_n) = \mathfrak{p} \cap ... \cap \mathfrak{p} = \mathfrak{p}$. Then it left to show $\mathfrak{q}_1 \cap ... \cap \mathfrak{q}_n$ is primary.

Suppose $xy \in \mathfrak{q}, x \notin \mathfrak{p}$. <u>Want:</u> $y \in \mathfrak{q}$. We have $xy \in \mathfrak{q}_i, x \notin \mathfrak{p} \implies y \in \mathfrak{q}_i \forall i \implies y \in \mathfrak{q}$. $\qquad \square$

Remark 5.11. *Let $\mathfrak{p}$ prime. In general, a $\mathfrak{p}$-primary ideal $\mathfrak{q}$ need not be a power of $\mathfrak{p}$, and a power of $\mathfrak{p}$ need not be primary.*

Proposition 5.12. *If $\mathcal{A} \supseteq \mathfrak{m}$ is a maximal ideal, $\mathfrak{q}$ any ideal, and $\mathfrak{m} = rad(\mathfrak{q})$, then $\mathfrak{q}$ is $\mathfrak{m}$-primary.*

Proof. Then $\mathfrak{m}/\mathfrak{q} = \mathrm{rad}(\mathfrak{q})/\mathfrak{q} = \mathrm{Nil}(\mathcal{A}/\mathfrak{q})$ is both a maximal ideal and the intersection of all prime ideals $\Longrightarrow \mathcal{A}/\mathfrak{q}$ has exactly one prime ideal, $\mathfrak{m}/\mathfrak{q}$. $(\mathcal{A}/\mathfrak{q}, \mathfrak{m}/\mathfrak{q})$ is a local ring. To show that $\mathfrak{q}$ is primary, we must show any zero-divisors in $\mathcal{A}/\mathfrak{q}$ is nilpotent (belongs to $\mathrm{Nil}(\mathcal{A}/\mathfrak{q}) = \mathfrak{m}/\mathfrak{q}$). In other words, want if $x \in \mathcal{A}/\mathfrak{q}, x \notin \mathfrak{m}/\mathfrak{q}$, then x not a zero divisor. Because $x \in \mathcal{A}/\mathfrak{q}$ and $x \notin \mathfrak{m}/\mathfrak{q} \Longrightarrow \mathcal{A}/\mathfrak{q}$ is local ring with unique prime $\mathfrak{m}/\mathfrak{q} \Longrightarrow x$ is a unit. $\qquad\square$

Corollary 5.13. *In particular, $\mathfrak{m}$ maximal, $\Longrightarrow \mathfrak{m}^n$ is $\mathfrak{m}$-primary $\forall n$.*

Example 5.14. $\mathfrak{m} = (X, Y) \subseteq K[X, Y] \Longrightarrow \mathfrak{m}^n$ *is primary.*

Example 5.15. $\mathfrak{q} = (X^2, Y) \subseteq K[X, Y]$ *is $\mathfrak{m}$-primary. $\mathfrak{m}$-primary ideals are not necessarily powers of maximal ideals.*

Example 5.16. $\mathfrak{a} = \prod_{j=1}^{J}(X - z_j)^{n_j} \subseteq \mathbb{C}[X]$ *for some distinct $z_1, ..., z_J \in \mathbb{C}$. Then $\mathfrak{a} = \mathfrak{q}_1 \cap ... \cap \mathfrak{q}_J$, $\mathfrak{q}_j = ((X - z_j)^{n_j})$, $\mathfrak{p}_j = rad(\mathfrak{q}_j) = (X - z_j)$*

Example 5.17. $\mathfrak{q}_1 = (X, Y)^2 = (X^2, XY, Y^2) \subseteq K[X, Y], \mathfrak{p}_1 = (X, Y)$. $\mathfrak{q}_2 = (Y) \Longrightarrow \mathfrak{p}_2 = (Y)$
$\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 = (XY, Y^2)$

How do we talk about the uniqueness of primary decomposition? Sometimes you shrink a primary decomposition $\mathfrak{q} = \mathfrak{q}_1 \cap ... \cap \mathfrak{q}_n$. $\mathfrak{p}_j = \mathrm{rad}(\mathfrak{q}_j)$

(a) If $\mathfrak{p}_i = \mathfrak{p}_j$ for some $i \neq j$, then we can replace $\mathfrak{q}_i$ with $\mathfrak{q}_i \cap \mathfrak{q}_j$ and delete $\mathfrak{q}_j$.

(b) $\mathfrak{q}_j \supseteq \cap_{i \neq j}\mathfrak{q}_i$, then we can delete $\mathfrak{q}_j$.

Definition 5.18. *If we can't do (a) or (b), we call the resulting decomposition **minimal**. Let $\mathfrak{a}$ ideal, we define $Ass(\mathfrak{a}) :=\{$prime ideals of the form $rad(\mathfrak{a} : x)$ for some $x \in \mathcal{A}\}$ to be **the set of associated ideals of** $\mathfrak{a}$.(recall $y \in (\mathfrak{a} : x) \iff y$ maps x into $\mathfrak{a} \iff yx \in \mathfrak{a}$)*

Theorem 5.19. *(First Uniqueness Theorem of minimal primary decomposition) Let $\mathfrak{a} = \mathfrak{q}_1 \cap ... \cap \mathfrak{q}_n$ be a minimal primary decomposition. Then $\{\mathfrak{p}_1, ..., \mathfrak{p}_n\} = Ass(\mathfrak{a})$. In particular, the set $\{\mathfrak{p}_1, ..., \mathfrak{p}_n\}$ is independent of the choice of minimal primary decomposition.*

Lemma 5.20. *Let $\mathfrak{q}$ be $\mathfrak{p}$-primary, $x \in \mathcal{A}$.*

(a) $x \in \mathfrak{q} \Longrightarrow (\mathfrak{q} : x) = (1)$

(b) $x \notin \mathfrak{q} \Longrightarrow (\mathfrak{q} : x)$ *is $\mathfrak{p}$-primary and there for $rad(\mathfrak{q} : x) = \mathfrak{p}$.*

(c) $x \notin \mathfrak{p} \Longrightarrow (\mathfrak{q} : x) = \mathfrak{q}$

We first show that the Lemma 5.20 leads to the Theorem 5.19.

Proof. $\{\mathfrak{p}_j\} \supseteq \mathrm{Ass}(\mathfrak{a})$:
Let $x \in \mathcal{A}$ s.t. $\mathrm{rad}(\mathfrak{a} : x) = \mathfrak{p}$ is prime. <u>Want</u>: $\mathfrak{p}$ equals some $\mathfrak{p}_j$. $\mathrm{rad}(\mathfrak{a} : x) = \cap_j \mathrm{rad}(\mathfrak{q}_j : x) = \cap_{x \notin \mathfrak{q}_j} \mathfrak{p}_j$. Then by prime avoidance 1.27, we know $\mathfrak{p} =$ some $\mathfrak{q}_j$.

For the converse inclusion, <u>Want</u>: $\mathfrak{p}_j$ is of the form $\mathrm{rad}(\mathfrak{a} : x)$ for some x. By Lemma 5.20, we can choose $x_j \notin \mathfrak{q}_j$ and $x_j \notin \cap_{i \neq j} \mathfrak{q}_i$. This x_j always exists because $\mathfrak{p}_1 \cap ... \cap \mathfrak{p}_n$ is a minimal primary decomposition and such choice of x would make $\mathrm{rad}(\mathfrak{a} : x) = \cap_i \mathrm{rad}(\mathfrak{q}_i : x_j) = \cap_{x_j \notin \mathfrak{q}_i} \mathfrak{p}_i = \mathfrak{p}_j$. $\qquad\square$

And now we come back to the proof of the Lemma 5.20

Proof.

(a) follows directly from the definition of quotient of ideals and we want to prove a general fact that **if $\mathfrak{q}$ is primary, then so is $(\mathfrak{q} : x), \forall x$.** Altogether, this means $(\mathfrak{q} : x)$ is $\mathfrak{p}$-primary. Let $yz \in (\mathfrak{q} : x), y \notin (\mathfrak{q} : x)$.

<u>Want</u>: some $z^n \in (\mathfrak{q} : x)$

Know: $xyz \in \mathfrak{q}, xy \notin \mathfrak{q}$ because $\mathfrak{q}$ is primary $\Longrightarrow$ some $z^n \in \mathfrak{q}$.
$\Longrightarrow (\mathfrak{q} : x)$ is primary.

(b) $x \notin \mathfrak{q} \overset{?}{\Longrightarrow} \mathrm{rad}(\mathfrak{q} : x) = \mathfrak{p}$

Suppose $y^n \in (\mathfrak{q} : x)$

<u>Want</u>: $y \in \mathfrak{p}$.
Know $xy^n \in \mathfrak{q}, x \notin \mathfrak{q} \Longrightarrow y \in \mathrm{rad}(\mathfrak{q}) = \mathfrak{p}$

(c) $x \notin \mathfrak{p} \Longrightarrow (\mathfrak{q} : x) = \mathfrak{q}$, the $\supseteq$ part is obvious. For the "$\subseteq$" suppose $y \in (\mathfrak{q} : x)$, i.e. $xy \in \mathfrak{q}$. Know $x \notin \mathfrak{p}$ because $\mathfrak{q}$ is primary, $\Longrightarrow y \in \mathfrak{q}$

$\qquad\square$

5.2   Lecture 13. Second Uniqueness Theorem

Recall the First uniqueness theorem for Minimal Primary Decomposition(MPD).

Let $\mathfrak{a} = \mathfrak{q}_1 \cap ... \cap \mathfrak{q}_n$ be a minimal primary decomposition. Then $\{\mathfrak{p}_1, ..., \mathfrak{p}_n\} = \mathrm{Ass}(\mathfrak{a})$. In particular, the set $\{\mathfrak{p}_1, ..., \mathfrak{p}_n\}$ is independent of the choice of minimal primary decomposition.

$\mathfrak{a}$ decomposable with $\mathfrak{q}_1 \cap ... \cap \mathfrak{q}_n$ being any of the MPD. take $\mathfrak{p}_i = \mathrm{rad}(\mathfrak{q}_i)$
$\mathrm{Ass}(\mathfrak{a}) = \{\mathfrak{p}_1, ..., \mathfrak{p}_n\}$

Example 5.21. *MPD's need not be unique:*

$$\begin{aligned}
\mathfrak{a} &= (xy, x^2) \\
&= (x) \cap (x, y)^2 \\
&= (x) \cap (x^2, y)
\end{aligned}$$

but $\mathfrak{p}_1 = (x)$ *and* $p_2 = (x, y)$.

Proposition 5.22. *If $\mathcal{A}$ is Noetherian and $\mathfrak{q}$ is a $\mathfrak{p}$-primary ideal, then $\exists x \in \mathcal{A}$ s.t. $(\mathfrak{q} : x) = \mathfrak{p}$ (necessarily $x \notin \mathfrak{q}$)*

Proof. $\mathfrak{p}$ finitely generated ideal $\forall x_i \in \mathfrak{p} \implies$ some $x_i^m \in \mathfrak{q} \implies$ some $\mathfrak{p}^n \subseteq \mathfrak{q}$ Any $n \geq \sum_i (m_i - 1) + 1$ would work.
Choose $n \geq 1$ minimal with this property. Then $\mathfrak{p}^{n-1} \not\subseteq \mathfrak{q} \implies \exists x \in \mathfrak{p}^{n-1}, x \notin \mathfrak{q}$.

Claim: $(\mathfrak{q} : x) = \mathfrak{p}$.
"$\subseteq$": True, because we have seen that $(\mathfrak{q} : x)$ is $\mathfrak{p}$-primary.
"$\supseteq$": If $y \in \mathfrak{p}$, then $xy \in \mathfrak{p}^n \subseteq \mathfrak{q} \implies y \in (\mathfrak{q} : x)$ $\square$

Example 5.23. *k is field, and $\mathcal{A} = k[t]$, $\mathfrak{q} = (t^N), N \geq 1$, $\mathfrak{p} = (t)$.*
$x \in \mathcal{A} \implies x = ct^n + c't^{n+1} + ...$, *where $c \neq 0, n \geq 0, n =: ord_t(x)$ for example:*
$x = t^4 + 4t^2$, $ord_t(x) = 2$. $\frac{x}{1} \in \mathcal{A}_\mathfrak{p}$, $\left(\frac{x}{1}\right) = \left(\frac{t^n}{1}\right)$.
Then $(\mathfrak{q} : x) = (t^m)$, where $m = max(N - n, 0)$
$x \in \mathfrak{q} \iff n \geq N \iff m = 0$.
$x \notin \mathfrak{q} \iff m \geq 1 \implies (\mathfrak{q} : x)$ *is $\mathfrak{p}$-primary.*
$x \in (t^{N-1})$, *but $x \notin (t^N) \implies (\mathfrak{q} : x) = \mathfrak{p}$.*
$x \notin \mathfrak{p} \iff n = 0 \iff m = N \implies (\mathfrak{q} : x) = \mathfrak{q}$.

Now we come to the proof of Theorem 5.19

Proof. Given a MPD $\mathfrak{a} = \mathfrak{q}_1 \cap ... \cap \mathfrak{q}_n$, $x \in \mathcal{A}$, we can compute $(\mathfrak{a} : x) = \cap_j (\mathfrak{q}_j : x)$

$$\mathrm{rad}(\mathfrak{a} : x) = \underset{j : \mathfrak{q}_j \not\ni x}{\cap} \mathfrak{p}_j$$

Since this decomposition is minimal, we may find for each i an element $x \in \cap_{j \neq i} \mathfrak{q}_j$, $x \notin \mathfrak{q}_i$

$\Longrightarrow \operatorname{rad}(\mathfrak{a} : x) = \mathfrak{p}_i$

$\Longrightarrow \mathfrak{p}_i \in \operatorname{Ass}(\mathfrak{a})$.

$(\mathfrak{q}_i \nsubseteq \cap_{j \neq i} \mathfrak{q}_j)$

Conversely, if $\mathfrak{p}$ is a prime of the form $\mathfrak{p} = \operatorname{rad}(\mathfrak{a} : x)$ for some x, then $\mathfrak{p} = \cap_{j : \mathfrak{q}_j \not\ni x} \mathfrak{p}_j \Longrightarrow \mathfrak{p} = \mathfrak{p}_j$ for some j. $\Longrightarrow \operatorname{Ass}(\mathfrak{a}) \subseteq \{\mathfrak{p}_1, ..., \mathfrak{p}_n\}$ $\qquad \square$

This completes the proof the Theorem 5.19. Moreover, if $\mathcal{A}$ is Noetherian, we may find for each i an element x_i with $(\mathfrak{a} : x_i) = \mathfrak{p}_i$, by applying the final part of Proposition 5.22.

Proposition 5.24. *(Definition)* $rad(\mathfrak{a}) = \cap \mathfrak{p}_j$, *if* $\mathfrak{a} = \cap \mathfrak{q}_j$ *is a MPD. We want to define* **Zero-divisors modulo** $\mathfrak{a}$*:*

$$Z(\mathfrak{a}) := \{x \in \mathcal{A} | \exists y \in \mathcal{A} - \mathfrak{a} \text{ s.t. } xy \in \mathfrak{a}\}$$
$$= \{x \in \mathcal{A} | (\mathfrak{a} : x) \nsubseteq \mathfrak{a}\}$$
$$= \cup_{y \in \mathcal{A} - \mathfrak{a}} (\mathfrak{a} : y)$$
$$\overset{(*)}{=} \cup_{y \in \mathcal{A} - \mathfrak{a}} rad(\mathfrak{a} : y)$$

Proof. of the $(*)$. It suffices to prove that $= \cup_{y \in \mathcal{A} - \mathfrak{a}} (\mathfrak{a} : y) \supseteq \cup_{y \in \mathcal{A} - \mathfrak{a}} \operatorname{rad}(\mathfrak{a} : y)$. <u>Want</u>: if some prower x^n of x satisfies $x^n \in (\mathfrak{a} : y)$ then $\exists y'$ s.t. $x \in (\mathfrak{a} : y')$. $x^n \in (\mathfrak{a} : y) \Longleftrightarrow x^n y \in \mathfrak{a}$, then we may choose $n \geq 1$ minimal with this property. Then $x \cdot x^{n-1} y \in \mathfrak{a}$ but $x^{n-1} y \notin \mathfrak{a}$. As $x \in (\mathfrak{a} : x^{n-1} y)$. Choose $y' = x^{n-1} y$, we are done. $\qquad \square$

Proposition 5.25. $\mathfrak{a} = \cap \mathfrak{q}_j$ *MPD,* $\Longrightarrow Z(\mathfrak{a}) = \cup \mathfrak{p}_j$.

Proof. $Z(\mathfrak{a}) \subseteq \cup \mathfrak{p}_j$: Let $x \in Z(\mathfrak{a})$.

<u>Want</u>: to show that x is contained in some $\mathfrak{p}_j$.

<u>Know</u>: $x \in Z(\mathfrak{a}) \Longrightarrow (\mathfrak{a} : x) \nsubseteq \mathfrak{a}$. On the other hand, we know $(\mathfrak{a} : x) = \cap_j (\mathfrak{q}_j : x)$ and we know $(\mathfrak{q}_j : x)$ is $\mathfrak{p}_j$-primary ideal if $x \notin \mathfrak{q}_j$, or $(\mathfrak{q}_j : x) = \mathfrak{q}_j$ if $x \notin \mathfrak{p}_j$.

If $x \notin \mathfrak{p}_j \forall j$, then $(\mathfrak{q}_j : x) = \mathfrak{q}_j \Longrightarrow (\mathfrak{a} : x) = \cap \mathfrak{q}_j = \mathfrak{a}$, contrary to the hypothesis that $x \in Z(\mathfrak{a})$.

In fact, this can be seen directly from

$$\color{red}{Z(\mathfrak{a}) = \cup_{y \in \mathcal{A} - \mathfrak{a}} \operatorname{rad}(\mathfrak{a} : y) = \cup_{y \in \mathcal{A} - \mathfrak{a}} \cap_{j : \mathfrak{q}_j \notin y} \mathfrak{p}_j \subseteq \cup \mathfrak{p}_j}$$

For the reverse inclusion, we might try to show $\cup \mathfrak{p}_j \subseteq Z(\mathfrak{a})$.

Recall:$\mathrm{rad}(\mathfrak{a} : y) = \cap_{j:\mathfrak{q}_j \not\ni y}\mathfrak{p}_j$. Give j, we can find y s.t. $\mathrm{rad}(\mathfrak{a} : y) = \mathfrak{p}_j$. See the proof of Theorem 5.19, each i an element $x \in \cap_{i \neq j}\mathfrak{q}_i$, $x \notin \mathfrak{q}_j$. Necessarily, $y \notin \mathfrak{a}$. So if $x \in \mathfrak{p}_j$, then $x \in \mathrm{rad}(\mathfrak{a} : y) \subseteq Z(\mathfrak{a})$ because $Z(\mathfrak{a}) = \cup_{y \in \mathcal{A} - \mathfrak{a}}\mathrm{rad}(\mathfrak{a} : y)$.   □

Example 5.26. *A good example for intuition,* $\{z_1, ..., z_n\} \subseteq k$ *where k is a field.* $\mathfrak{a} = \cap \mathfrak{q}_j, \mathfrak{q}_j = (t - z_j)^{N_j}$ *and* $\mathcal{A} = k[t]$. $0 \neq x \in \mathcal{A} \Longrightarrow n_j := ord_{t-z_j}(x) :=$*largest* $n_j \geq 0$ *such that* $(t - z_j)^{n_j}$ *divides x.*
Then $x \in Z(\mathfrak{a}) \Longleftrightarrow \exists j : n_j \geq 1$.
$x \in rad(\mathfrak{a}) \Longleftrightarrow \forall j, n_j \geq 1$.
N.b. $n_j =$ *order of vanishing of x at z_j,* $n_j > c \Longleftrightarrow$ *first c Taylor coefficients of x all vanish at z_j.*

Definition 5.27. $Ass(\mathfrak{a}) \ni \mathfrak{p}$ *is either **minimal/isolated** if $\mathfrak{p}$ is a minimal element of $Ass(\mathfrak{a})$ (under the partial order of inclusion) or*
embedded *if the $\mathfrak{p}$ strictly contains some other ideals in $Ass(\mathfrak{a})$. Geometrically,* $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \Longrightarrow V(\mathfrak{p}_1) \supseteq V(\mathfrak{p}_2)$ *embedded in $V(\mathfrak{p}_1)$.*
    We usually denote the set of isolated primes in $Ass(\mathfrak{a})$ by $Ass'(\mathfrak{a})$

Example 5.28. $\mathfrak{p}_1 = (x), \mathfrak{p}_2 = (x, y)$
$\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2^2 = (xy, x^2)$, $\mathfrak{p}_1$ *is isolated/minimal while $\mathfrak{p}_2$ is embedded.*

Then we state the second unique decomposition theorem:

Theorem 5.29. *(Second Uniqueness Theorem) In any MPD* $\mathfrak{a} = \cap \mathfrak{q}_j$, $\{\mathfrak{q}_j : \mathfrak{p}_j$ *is minimal$\}$ depends only upon $\mathfrak{a}$, independent of the choice of MPD. More precisely, for $\mathfrak{p}_j$ minimal, we have* $\mathfrak{q}_j = \iota^*(\iota_*(\mathfrak{a}))$, *where* $\iota : \mathcal{A} \longrightarrow \mathcal{A}_{\mathfrak{p}_j}$.

Recall that for a multiplicative set $S \subseteq \mathcal{A}$, $\iota : \mathcal{A} \longrightarrow S^{-1}\mathcal{A}$:
$\mathfrak{p}$ prime ,
$\mathfrak{p} \cap S \neq \emptyset \Longrightarrow \iota_*(\mathfrak{p}) = (1)$
$\mathfrak{p} \cap S = \emptyset \Longrightarrow \iota^*(\mathfrak{p})$ prime and $\iota^*\iota_*(\mathfrak{p}) = \mathfrak{p}$.

Lemma 5.30. $\iota^*\iota_*(\mathfrak{a}) = \cup_{s \in S}(\mathfrak{a} : s)$

Proof. $x \in \iota^*\iota_*(\mathfrak{a}) \Longrightarrow \frac{x}{1} \in \iota_*\mathfrak{a} = \{\frac{y}{s} : y \in \mathfrak{a}, s \in S\}$
    "$\subseteq$": Suppose $\frac{x}{1} = \frac{y}{s}$ for some $y \in \mathfrak{a}, s \in S$. Then $\exists t \in S$ s.t. $t(xs - y) = 0$ $\Longrightarrow stx = yt \in \mathfrak{a} \Longrightarrow x \in (\mathfrak{a} : st)$, where $st \in S$.
    "$\supseteq$": Say $x \in (\mathfrak{a} : s)$ for some $s \in S$. Thus $xs =: y \in \mathfrak{a}$. Then $\frac{x}{1} = \frac{y}{s} \in$ $\iota^*\iota_*\mathfrak{a}$ □

Lemma 5.31. $S \subseteq \mathcal{A}$ *is multiplicative set*, $\mathfrak{q} \subseteq \mathcal{A}$ *primary and* $\mathfrak{p} = rad(\mathfrak{q})$. *Then:*

(a) $\mathfrak{p} \cup S \neq \emptyset \Longrightarrow \iota_*\mathfrak{q} = (1)$

(b) $\mathfrak{p} \cap S = \emptyset \Longrightarrow \iota_*\mathfrak{q}$ *is* $\iota_*\mathfrak{p}$-*primary and* $\iota^*\iota_*\mathfrak{q} = \mathfrak{q}$.

(c) $S \cap \mathfrak{q} = \emptyset \Longleftrightarrow S \cap \mathfrak{p} = \emptyset$

Proof.   (a) Suppose $\mathfrak{p} \cap S \neq \emptyset$, say $s_0 \in \mathfrak{p} \cap S. \Longrightarrow \exists n \geq 1 : s_0^n \in \mathfrak{q} \cap S$

$$\iota_*\mathfrak{q} = \left\{ \frac{x}{s} : x \in \mathfrak{q}, s \in S \right\}$$

$\frac{1}{1} = \frac{s_0^n}{s_0^n} \in \iota_*\mathfrak{q} \Longrightarrow \iota_*\mathfrak{q} = (1)$.

(b) Suppose $\mathfrak{p} \cap S = \emptyset$. Recall that localization commutates with taking radicals 3.14, $\mathrm{rad}(\iota_*(\mathfrak{q})) = \iota_*(\mathrm{rad}(\mathfrak{q})) = \iota_*\mathfrak{p}$. Then if suffices to show that $\iota_*\mathfrak{q}$ is primary.

Let $\frac{x}{s}, \frac{y}{t} \in S^{-1}\mathcal{A}$, Suppose $(\frac{x}{s})\frac{y}{t} \in \iota_*\mathfrak{q}, \frac{y}{t} \notin \iota_*\mathfrak{q}$, <u>Want</u>: some $(\frac{x}{s})^n \in \iota_*\mathfrak{q}$.

Note : we may assume $\mathfrak{q} = (0)$, because localization is exact, hence commutes with taking quotients

$$S^{-1}(\mathcal{A}/\mathfrak{q}) \cong S^{-1}\mathcal{A}/\iota_*\mathfrak{q}.$$

Then the original statement translates to:

(i) ι is injective (i.e. $\iota^*(0)_{S^{-1}\mathcal{A}} = \iota^*\iota_*(0) \overset{?}{=} (0)$)

(ii) $\iota_*(0) = (0)_{S^{-1}\mathcal{A}}$ is primary.

These implies the remaining assertions (for $\mathfrak{q} = (0)$). In this case $\mathfrak{p}$ is the set of nilpotents in $\mathcal{A}$. Thus take $\mathfrak{q} = (0)$ and require (0) to be primary in $\mathcal{A}$. Assume $S \cap \mathfrak{p} = \emptyset$, i.e. S contains no nilpotents.

Proof of (i):
Recall Lemma 3.7 that ι injective: $(i) \Longleftrightarrow S$ contains no nonzero zerodivisors. Note that $(0) \subseteq \mathcal{A}$ is primary $\overset{def}{\Longleftrightarrow} \{$ zero-divisors in $\mathcal{A}\} \cong \{$nilpotents in $\mathcal{A}\}$.
$(i) \Longleftrightarrow S$ contains no nilpotents.
$\Longleftrightarrow S \cap \mathfrak{p} = \emptyset$.

Thus (i) holds.

Proof of (ii):

$$\left\{\begin{array}{c} \text{zero-divisors} \\ \text{in } S^{-1}\mathcal{A} \end{array}\right\} = \left\{\begin{array}{c} \dfrac{x}{s} : x \in \mathcal{A}, s \in S \\[2mm] \text{such that } \exists \dfrac{y}{t} \in S^{-1}\mathcal{A} \text{ nonzero} \\[2mm] \text{so that } \dfrac{x}{s}\dfrac{y}{t} = \dfrac{0}{1} \end{array}\right\}$$

$$= \left\{\begin{array}{c} \dfrac{x}{s} : \exists y \in \mathcal{A} \text{ with } y \cdot t \neq 0, \forall t \in S \\[2mm] \text{s.t. } \exists u \in S \text{ with } xuy = 0 \\[2mm] \text{where } uy \neq 0 \end{array}\right\}$$

$$= \left\{\begin{array}{c} \dfrac{x}{s} : s \in S \\[2mm] x \in \mathcal{A} \text{ is zerodivisor} \end{array}\right\}$$

$$= \left\{\dfrac{x}{s} : s \in S, x \in \mathcal{A} \text{ is nilpotent}\right\} \, ((0) \subseteq \mathcal{A} \text{ is primary})$$

$$= S^{-1}(\text{Nil}(\mathcal{A}))$$

$$= \text{Nil}(S^{-1}\mathcal{A}),$$

(by the fact that radical commutes with localizations)

Thus {zero-divisors in $S^{-1}\mathcal{A}$}=Nil($S^{-1}\mathcal{A}$), so $(0)_{S^{-1}\mathcal{A}}$ is primary.

(c) The "$\Longleftarrow$" direction of (c) is trivial. For the "$\Longrightarrow$" direction of (c), suppose $\exists s \in S \cap \mathfrak{p}$. Since $\mathfrak{p} = \text{rad}(\mathfrak{q})$, $\exists n \geq 1$ s.t. $s^n \in \mathfrak{q}$. S multiplicative closed $\Longrightarrow s^n \in S$. Thus $s^n \in S \cap \mathfrak{q}$. So $S \cap \mathfrak{p} \neq \emptyset \Longrightarrow S \cap \mathfrak{q} \neq \emptyset$. $\qquad\qquad\square$

Definition 5.32. *In that case call $\mathfrak{q}_j$ the $\mathfrak{p}_j$-primary component of $\mathfrak{a}$.*

Lemma 5.33. *Let $\mathfrak{a}$ be decomposable. Then $Ass'(\mathfrak{a}) =\{$minimal primes $\mathfrak{p}$ containing $\mathfrak{a}\}$, here minimal means that there is no intermediate primes between $\mathfrak{p}$ and $\mathfrak{a}$.*

Proof. It suffices to show that if any prime $\mathfrak{p} \supseteq \mathfrak{a}$, then there exists $\mathfrak{p}_j \in \text{Ass'}(\mathfrak{a})$ s.t. $\mathfrak{p}_j \subseteq \mathfrak{p}$. Indeed, $\mathfrak{p} \supseteq \mathfrak{a} \Longrightarrow \mathfrak{p} \supseteq \text{rad}(\mathfrak{a}) = \text{rad}(\cap\mathfrak{q}_j) = \cap_j\text{rad}(\mathfrak{q}_j) = \cap_j\mathfrak{p}_j$. Then $\mathfrak{p} \supseteq \mathfrak{p}_j$ for some j, because of prime avoidance 1.27. $\qquad\qquad\square$

Theorem 5.34. $\mathcal{A} \supseteq \mathfrak{a} = \cap_{j=1}^n \mathfrak{q}_j$ *MPD. If $\mathfrak{p}_j \in Ass'(\mathfrak{a})$, then*

$$\mathfrak{q}_j = \iota^* \iota_* \mathfrak{a}, \iota : \mathcal{A} \longrightarrow \mathcal{A}_{\mathfrak{p}_j}$$

As a Corollary, the isolated primary component of $\mathfrak{a}$ does not depend on MPD.

Proof.

$$\iota^*\iota_*\mathfrak{a} = \iota^*(\iota_*(\cap \mathfrak{q}_i)) = \iota^*(\cap \iota_*\mathfrak{q}_i) = \cap \iota^*\iota_*\mathfrak{q}_i$$

$$\iota^*\iota_*\mathfrak{q}_i = \begin{cases} \mathfrak{q}_i : i = j(\text{By Lemma } 5.31) \\ (1) : i \neq j \end{cases}$$

For the second identity, we must check that $\forall i \neq j,\ S \cap \mathfrak{q}_i \neq \emptyset \iff \mathfrak{q}_i \nsubseteq \mathfrak{p}_j$

If $\mathfrak{p}_i \nsubseteq \mathfrak{p}_j$ $x \in \mathfrak{p}_i, x \notin \mathfrak{p}_j$ then some $x^n \in \mathfrak{q}_i$, $\mathfrak{p}_i = \mathrm{rad}(\mathfrak{q}_i)$, $x^n \notin \mathfrak{p}_j$ because $\mathfrak{p}_j$ is prime $\implies \mathfrak{q}_i \nsubseteq \mathfrak{p}_j$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

6   Dimension Theory

6.1   Lecture 14. Artinian Rings

Definition 6.1. *An $\mathcal{A}$-module M is called **Artin** or **Artinian** is it satisfies either of the following equivalent conditions:*

(i) **DCC** *descending chain condition: if $M \supseteq M_1 \supseteq M_2 \supseteq ....$, then $\exists n_0$ s.t. $M_n = M_{n_0} \forall n \neq n_0$*

(ii) **MIN** *minimal condition: Every collection of submodules has minimal element.*

The proof of $(i) \iff (ii)$ same as the proof in definition of Noetherian ring.

Definition 6.2. *$\mathcal{A}$ is an **Artinian ring** if it satisfies the following equivalent conditions*

(i) *$\mathcal{A}$ is an Artinian $\mathcal{A}$-module*

(ii) *$\mathcal{A}$ DCC on ideals*

(iii) *$\mathcal{A}$ MIN on ideals*

Lemma 6.3. *If $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ is a short exact sequence of modules, then M Artinian $\iff M', M''$ Artinian.*

Corollary 6.4. *Any finitely generated modules over an Artinian ring is Artinian.*

Corollary 6.5. *$\mathcal{A}$ Artinian $\iff \mathcal{A}/\mathfrak{a}$: Artinian $\forall \mathfrak{a}$ ideals.*

Example 6.6.

• *A field is trivially Artinian because it has only two ideals.*

- $\mathbb{Z}$ *is NOT Artin,* $(2) \supsetneq (2^2) \supsetneq (2^3)$....

- *Any finite ring is Artinian + Noetherian e.g.* $\mathbb{Z}/n\mathbb{Z}, n \neq 0$

- *Any finite product of Artinian rings is Artinian.*

- k *is field,* $\mathfrak{m} := (X_1, ..., X_n) \subset k[X_1, ..., X_n] = \mathcal{A}$. *Then* $\mathcal{A}/\mathfrak{m}^l$ *is Artinian* $\forall l \geq 1$ *where* $\mathcal{A}/\mathfrak{m}^l$ *is finite dimensional vector space over* k.

- $k[X]/(X^l)$ *is Artinian* $\forall l \geq 1$

- $k[X^2, X^3]/(X^{10})$ *is Artin*

- $k[X]$ *is NOT Artin, for example* $(X) \supsetneq (X^2) \supsetneq (X^3) \supsetneq ...$

Lemma 6.7. *Let* $\mathcal{A}$ *Artinian. Then every prime in* $\mathcal{A}$ *is maximal and* $\mathcal{A}$ *has only finitely many primes, hence the Jacobson radical* $Jac(\mathcal{A}) = Nil(\mathcal{A})$

Proof. Let $\mathfrak{p} \subseteq \mathcal{A}$ be prime. Set $\mathcal{B} : \mathcal{A}/\mathfrak{p}$. Then $\mathcal{B}$ Artin, integral domain.
Want $\mathcal{B}$ is a field.
Let $0 \neq x \in \mathcal{B}$, Want $x \in \mathcal{B}^\times$
Consider $(x) \supseteq (x^2) \supseteq (x^3) \supseteq ....$ $\mathcal{B}$ Artinian $\implies \exists n \geq 0 : (x^n) = (x^{n+1})$, $\exists u \in \mathcal{B} : x^n = ux^{n+1} \implies 1 = ux$ because $\mathcal{B}$ is an integral domain. Then $x \in \mathcal{B}^\times$ as required.
Consider distinct maximal ideals $\mathfrak{m}_1, \mathfrak{m}_2, ... \in \mathcal{A}$. Consider $\mathfrak{m}_1 \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \mathfrak{m}_3 \supseteq ...$ Choose $n_0 : \mathfrak{m}_1 \cap ... \cap \mathfrak{m}_{n_0} = \mathfrak{m}_1 \cap .. \cap \mathfrak{m}_n \forall n \geq n_0 \implies \mathfrak{m}_1 \cap ... \cap \mathfrak{m}_{n_0} \subseteq \mathfrak{m}_n \implies \mathfrak{m}_n = \mathfrak{m}_j$ for some $j \leq n_0$. $\qquad\square$

Proposition 6.8. $\mathcal{A}$ *is Artinian* $\implies \mathcal{N} := Nil(\mathcal{A})$ *is nilpotent:* $\exists n \geq 0, \mathcal{N}^n = (0)$

Remark 6.9.
$$\mathcal{A} = \oplus_{i=1}^n k[X_i]/(X_i^i)$$
hence $\mathcal{N} = \oplus_{i=1}^n (X_i)$, *where* $(X_i) \subseteq k[X_i]/(X_i^i)$ $\mathcal{N}^n = (0), \mathcal{N}^{n-1} \neq (0)$, *If* $n < \infty, \mathcal{A}$ *is Artinian . If* $n = \infty, \mathcal{A}$ *is NOT Artin,* $\mathcal{A}$ *not Nilpotent.*

Proof. Let $\mathcal{J} := \text{Nil}(\mathcal{A}) = \text{Jac}(\mathcal{A})$ by the Lemma 6.7. Consider $\mathcal{J} \supseteq \mathcal{J}^2 \supseteq \mathcal{J}^3 \supseteq ...$ $\mathcal{A}$ is Artinian $\implies \mathcal{J}^n = \mathcal{J}^{n+1}$ for some n.
    <u>Want</u>: $\mathcal{J}^n = (0)$.
    Denote $\mathcal{I} := \mathcal{J}^n$. Note that $\mathcal{J}\mathcal{I} = \mathcal{I}$, if we know that $\mathcal{I}$ is finitely generated, suppose $\mathcal{I} \neq (0)$. Then Nakayama Lemma 2.17 $\implies \mathcal{I} = (0)$.

Let $\mathfrak{b}$ be a minimal element of {ideals $\mathfrak{b} \subseteq \mathcal{I} : \mathcal{J}^n \mathfrak{b} \neq (0)$}. Then $\exists 0 \neq x \in \mathfrak{b}$ with $\mathcal{J}^n(x) \neq (0)$. Then $(x \subseteq \mathfrak{b} \subseteq \mathcal{I}), \mathcal{J}^n(x) \neq (0)$, so by minimality, $\mathfrak{b} = (x)$. $\mathcal{J}^n(x) = \mathcal{J}^{n+1}(x) = \mathcal{J}^n \mathcal{J}(x)$.

<u>Want</u>: $\mathcal{J}(x) = (x)$

If not, then $\mathcal{J}(x)$ is a non-zero submodule in (x) and $\mathcal{J}^n \mathcal{J}(x) \neq (0)$, which contradicts the minimality of (x).

Now (x) is finitely generated, so we conclude by Nakayama.   □

6.2   Lecture 15. Krull Dimension, Artinian v.s. Noetherian

Definition 6.10. *The **Krull dimension** of a nonzero ring $\mathcal{A}$, denoted $dim(\mathcal{A})$, is the supremum of all integers $r \geq 0$ s.t. $\exists$ chain of primes in $\mathcal{A}$ of length r:* $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq ... \subsetneq \mathfrak{p}_r$.

Example 6.11.

- *k a field, $\implies (0)$ is the only prime $\implies dim(k) = 0$*

- *$dim(\mathbb{Z}) = 1$*

- *(NOT OBVIOUS) $dim(k[x_1, ..., x_n]) = n$ and $dim(\mathcal{R}[x_1, .., x_n]) = dim(\mathcal{R}) + n$.*

- *$dim(\mathcal{A}) = 0 \iff$ every prime is maximal.*

Theorem 6.12. *$\mathcal{A}$ an Artinian ring $\iff \mathcal{A}$ Noetherian and $dim(\mathcal{A}) = 0$.*

Recall last lecture, by the Proposition 6.7 says all primes in Artinian ring is maximal $\implies dim(\mathcal{A}) = 0$.

Lemma 6.13. *$\mathcal{A}$ Noetherian, $\mathfrak{a} \subseteq \mathcal{A}$ ideal $\implies \exists n \geq 0 : rad(\mathfrak{a})^n \subseteq \mathfrak{a}$*

Proof. $rad(\mathfrak{a})$ is finitely generated, suppose it is generated by a finite set $\{x_i | i = 1, ..., r\}$. Choose $N \geq 0$ large enough that $x_j^N \in \mathfrak{a}, \forall j = 1, ..., r$. Any $x \in rad(\mathfrak{a})$ may be written $x = \sum a_j x_j \implies x^n = (\sum a_j x_j)^n = \mathcal{A}$-linear combination of $x_1^{n_1}...x_r^{n_r}$ where $n_1 + ... n_r = n$. We can take n large enough $(n \geq N \times r + 1)$, then at least one of n_j is larger than N for each term $\implies x^n \in \mathfrak{a}$.   □

Corollary 6.14. *$\mathcal{A}$ Noetherian, $\mathfrak{q}$ is $\mathfrak{p}$-primary, $\exists n \geq 0 : \mathfrak{q} \supseteq \mathfrak{p}^n$. (By definition)*

Lemma 6.15. *Suppose $(0) \subseteq \mathcal{A}$ is a finite product of maximal ideals. Then under this assumption,*

$$\mathcal{A} \text{ is Artin} \iff \mathcal{A} \text{ is Noetherian}$$

Proof. Say $(0) = \mathfrak{m}_1 \cdots \mathfrak{m}_r$. Each $k_j := \mathcal{A}/\mathfrak{m}_j$ is a field. Define $M_0 := \mathcal{A}$, $M_1 := \mathfrak{m}_1$, $M_2 := \mathfrak{m}_1 \mathfrak{m}_2,...,M_r = (0)$.

Then $M_j/M_{j+1} (j = 0, 1, ..., r-1)$ is a k_{j+1}-vector space. Moreover:

$$\{\mathcal{A}\text{-submodule of } M_j/M_{j+1}\} \xleftrightarrow{bij} \{k_{j+1}\text{-vector subspace of } M_j/M_{j+1}\}$$

In general, if V is a vector space over a field k, then V is Artinian $\iff$ $dim_k(V) < \infty \iff V$ is Noetherian. Thus M_j/M_{j+1} is Artinian $\iff M_j/M_{j+1}$ is Noetherian.

To conclude, we apply the following Lemma:

Lemma 6.16. *If $M = M_0 \supseteq M_1 \supseteq ... \supseteq M_r = \{0\}$ is a chain of modules over a ring, then M is Noetherian iff each M_j/M_{j+1} is Noetherian and M is Artinian iff M_j/M_{j+1} is Artinian.*

Proof. Induction on r, check it for $r = 0$. For $r \geq 1$,

$$0 \longrightarrow M_1 \longrightarrow M_0 \longrightarrow M_0/M_1 \longrightarrow 0$$

Recall Lemma 4.3 and Lemma 6.3, we know M_0 Noetherian (Artin) $\iff$ each M_j/M_{j+1} is Noetherian (Artin) $\qquad \square$

$\qquad \square$

Now we come back to the proof of Theorem 6.12

Proof.
<u>Want</u>: Artinian $\iff$ Noetherian $+ \, dim = 0$
<u>Know</u>: Artinian $\implies dim = 0$
By Lemma 6.15, it reduces to showing

(i) Artinian $\implies (0) =$ finite product of maximal ideals.

(ii) Noetherian $+ \, dim = 0 \implies (0) =$ finite product of maximal ideals .

For the part (i). Recall $\mathcal{A}$ Artinian $\implies \{$primes $\in \mathcal{A}\} = \{\mathfrak{m}_1, ..., \mathfrak{m}_r\}$ finite set of maximal ideals.

$$(\mathfrak{m}_1 \cdots \mathfrak{m}_r)^N \subseteq (\mathfrak{m}_1 \cap ... \cap \mathfrak{m}_r)^N = \text{Jac}(\mathcal{A})^N = (0)$$

for some N by Proposition 6.8.

For part (ii), $\mathcal{A}$ Noetherian $\implies (0) = \cap_j \mathfrak{q}_j$:MPD with $\mathfrak{p}_j = \mathrm{rad}(\mathfrak{q}_j)$.

$$(dim = 0) \implies \text{Each } \mathfrak{p}_j \text{ is maximal}$$
$$\implies \text{Every } \mathfrak{p}_j \text{ is isolated/minimal}$$
$$\implies \{\text{primes in } \mathcal{A}\} = \{\mathfrak{p}_1, ..., \mathfrak{p}_r\} \text{ are all maximal.}$$

Consider $(\mathfrak{p}_1, ..., \mathfrak{p}_r)^N \subseteq (\mathfrak{p}_1 \cap ... \cap \mathfrak{p}_r)^N \subseteq (0)$, where $(\mathfrak{p}_1 \cap ... \cap \mathfrak{p}_r) = \mathrm{Nil}(\mathcal{A}) = \mathrm{rad}(0)$ and we can conclude the last inclusion by Lemma 6.13. $\square$

Definition 6.17. *A ring $\mathcal{A}$ is called **primary** iff (0) is primary.*

Proposition 6.18. *$\mathcal{A}$ is Artinian. Then $\mathcal{A}$ local $\iff$ primary.*

Proof. "$\implies$":
$(\mathcal{A} : \mathfrak{m})$ is local $\iff \mathfrak{m}$ is the unique prime ideal.
$\implies \mathfrak{m} = \mathrm{Jac}(\mathcal{A}) = \mathrm{Nil}(\mathcal{A})$
$\implies \mathfrak{m}^N = 0$ for some $N \geq 0$
$\mathcal{A} - \mathfrak{m} = \mathcal{A}^\times$ Here $\mathfrak{m} = \{\text{non-units}\}$, and by the argument above, $\mathfrak{m} = \{\text{nilpotents}\}$. (In a general ring, we have $\{\text{non-units}\} \supseteq \{\text{zero-divisors}\} \supseteq \{\text{nilpotents}\}$). In this case $\mathfrak{m} = \{\text{non-units}\} = \{\text{zero-divisors}\} = \{\text{nilpotents}\}, \implies (0)$ is primary.
    "$\impliedby$":
(0) primary $\implies \mathfrak{p} = \mathrm{rad}(0)$ is the smallest prime $\implies$ maximal.
$\implies \mathfrak{p}$ the unique prime in $\mathcal{A}$
$\implies \mathfrak{p}$: the unique maximal in $\mathcal{A}$
$\implies (\mathcal{A}, \mathfrak{m} := \mathfrak{p})$ is local.

$\square$

Question: What are the Artinian integral domains?
Answer: The fields. (0) prime $\implies (0)$ maximal $\implies \mathcal{A}$ is a field.

Proposition 6.19. *Let $(\mathcal{A}, \mathfrak{m})$ Noetherian local ring. Then either*

(i) $\mathfrak{m}^n \neq \mathfrak{m}^{n+1} \forall n \geq 0$

(ii) *Some $\mathfrak{m}^n = 0$, $\mathcal{A}$ Artinian.*

Proof. Need to show the negation of (i) leads to (ii).
That (i) is false is equivalent to $\exists n : \mathfrak{m}^n = \mathfrak{m}^{n+1} \longleftrightarrow \mathfrak{m}\mathfrak{a} = \mathfrak{a}, \mathfrak{a} : \mathfrak{m}^n$, because $\mathcal{A}$ is Noetherian we know $\mathfrak{a}$ is finitely generated. Then by Nakayama lemma we know $\mathfrak{a} = (0)$.

Let $\mathfrak{p} \subseteq \mathcal{A}$ be a prime. Then

$$\mathfrak{m}^n \subseteq \mathfrak{p} \subseteq \mathfrak{m}.$$

Take radical to get

$$\mathfrak{m} = \mathrm{rad}(\mathfrak{m}^n) \subseteq \mathrm{rad}(\mathfrak{p}) = \mathfrak{p} \subseteq \mathrm{rad}(\mathfrak{m}) = \mathfrak{m}.$$

$\mathfrak{p}$ is arbitrary, $\mathcal{A}$ is Artinian local. $\qquad\qquad\qquad\qquad\qquad\qquad\square$

Example 6.20.

- $\mathbb{Z}/(p^n)$: *Artinian local*

- $k[[x]]$: *Noetherian* $\mathfrak{m} = (x)$ *not Artinian local*

- $k[[x]]/(x^n)$: *Artinian local*

- $k[x^2, x^3]/(x^{10})$: *Artinian local* $\mathfrak{m} = (x^2, x^3)$

In the first three examples, the maximal ideal is principal while in the last example it is not.

In fact we can describe every Artinian ring in terms of Artinian local ring.

Theorem 6.21. *(Structure Theorem of Artinian Rings.) Every Artinian ring is a finite direct product of Artinian local rings, unique up to reordering/isomorphism.*

Proof. $\mathcal{A}$ Artinian $\implies \mathcal{A}$ Noetherian with $dim0 \implies \exists (0) = \cap \mathfrak{q}_j$: MPD with $\mathfrak{p}_j = \mathrm{rad}(\mathfrak{q}_j)$ being maximal.
$\exists n \geq 0$ s.t. $\mathfrak{q}_j \supseteq \mathfrak{p}_j^n \forall j$, $\mathfrak{p}_j$ maximal.
The $\mathfrak{p}_j$ are pairwise coprime
$\implies \mathfrak{p}_j^n$ are pairwise coprime by Proposition 1.26
$\implies \mathfrak{q}_j$ are pairwise coprime.
Then we know from Chinese Remainder Theorem 1.25: the map

$$\mathcal{A}/ \cap_j \mathfrak{q}_j \longrightarrow \prod_j \mathcal{A}/\mathfrak{q}_j$$

is an isomorphism, where $\mathcal{A}/\mathfrak{q}_j$ are primary by Remark 5.2, hence are local by Proposition 6.18. This means

$$\mathcal{A} \cong \prod_j \mathcal{A}/\mathfrak{q}_j$$

is a finite product of Artinian local rings.

Uniqueness: Suppose $\phi : \mathcal{A} \xrightarrow{\cong} \prod_j \mathcal{A}_j$ finite product of Artinian local ring. Let $\phi_i : \mathcal{A} \longrightarrow \mathcal{A}_i$, $\phi_j = pr_j \circ \phi$. Define $\mathfrak{q}'_i := \mathrm{Ker}(\phi_i)$. Then $\mathcal{A}/\mathfrak{q}'_i \cong \mathcal{A}_i$. By Proposition 6.18, we know Artinian local indicate primary. Then we know $\mathcal{A}/\mathfrak{q}'_i$ primary $\implies \mathfrak{q}'_i$ is primary.

$\cap \mathfrak{q}'_i = (0)$ is a MPD. But $\mathcal{A}$ is Artin, so every associated primes of (0) is minimal or isolated. $(\mathrm{Ass}'(0) = \mathrm{Ass}(0))$. Then by the Second Uniqueness Theorem of Primary Decomposition 5.29. Each primary component is uniquely determined by (0). $\qquad\qquad\square$

Remark by TeXer 6.22. *Is it true that every primary ideal in Artinian ring is the form $\mathfrak{m}_j^n$?*

6.3   Lecture 16. Krull's Intersection Theorem

Theorem 6.23. *(Krull Intersection Theorem) $\mathcal{A}$ Noetherian, $\mathfrak{a} \subseteq Jac(\mathcal{A})$, M finitely generated $\mathcal{A}$-module. Then*

$$\cap_{i \geq 0} \mathfrak{a}^i M = \{0\}$$

Corollary 6.24. *In the above setting,*

$$\cap_{i \geq 0} \mathfrak{a}^i = (0)$$

Non-example 6.25. *k is a field, $\mathcal{A} : \cup_{n \geq 1} k[[X^{1/n}]]$ "formal power series with positive rational exponents". $\mathcal{A}$ is a local ring with maximal ideal $\mathfrak{m} : \{\mathfrak{a} = \sum_{i \in \mathbb{Q}_{\geq 0}} c_i X^i | c_0 = 0\}$. $\mathcal{A}/\mathfrak{m} = k$.*
In particular, $\mathfrak{m} = Jac(\mathcal{A})$, hence it satisfies the requirement for ideals in the above theorem. But $\cap_{i \geq 0} \mathfrak{m}^i = \mathfrak{m}$. Indeed, $\mathfrak{m}$ is spanned over k by $X^\alpha, \alpha \in \mathbb{Q}_{>0}$. But $X^\alpha = (X^{\alpha/i})^i \in \mathfrak{m}^i \forall i \in \mathbb{Z}_{\geq 1}$. Thus $\mathfrak{m} \subseteq \mathfrak{m}^i \subseteq \mathfrak{m} \forall i \geq 1$. $\mathcal{A}$ forms a Non-example of Non-Noetherian ring, $\mathfrak{m}$ is not finitely generated.

Proof. (of Theorem 6.23) $\mathfrak{a} \subseteq Jac(\mathcal{A})$, which suggests us to try Nakayama's Lemma 2.17. $M' := \cap_{i \geq 0} \mathfrak{a}^i M$. M finitely generated Noetherian module $\implies M'$ is Noetherian and M' is finitely generated. Want to show $M' = 0$. By Nakayama lemma, it reduce to showing that $\mathfrak{a}M' = M'$.
Unfortunately, **ideal multiplication and intersection of modules do not in general commute**, so this is not so clear, we can at most claim $\mathfrak{a}M' \subseteq M'$.
To proceed, we need the following lemma:

Lemma 6.26. *(Artin-Rees Lemma) Let $\mathcal{A}$ be Noetherian, $\mathfrak{a}$ be any ideal in $\mathcal{A}$. M finitely generated module and $M' \subseteq M$ as a submodule. Then $\exists k \geq 0$ so that $\forall i \geq k$*

$$\mathfrak{a}^i M \cap M' = \mathfrak{a}^{i-k}(\mathfrak{a}^k M \cap M')$$

Then, by Artin-Rees Lemma 6.26, $\mathfrak{a}^i M \cap M' = \mathfrak{a}^{i-k}(\mathfrak{a}^k M \cap M')$. But $\mathfrak{a}^i M \cap M' = M' = \mathfrak{a}^k M \cap M'$. Take $i = k+1 : M' = \mathfrak{a}M'$. Then use the Nakayama Lemma 2.17, $\implies M' = 0$ done.

$\square$

The "$\supseteq$" part of Artin-Rees Lemma 6.26 is clear, because $\mathfrak{a}^{i-k}(\mathfrak{a}^k M \cap M') \subseteq \mathfrak{a}^i M \cap \mathfrak{a}^{i-k} M' \subseteq \mathfrak{a}^i \cap M'$.

Our aim next is to prove "$\subseteq$" part of Artin-Rees Lemma. We have to introduce a lot of machinery for this trickier inclusion.

Definition 6.27. *Let $\mathcal{I}$ be a **monoid** (Set with associative binary operation and with identity). An $\mathcal{I}$-**graded ring** is a ring together with a decomposition $\mathcal{A} = \oplus_{i \in \mathcal{I}} \mathcal{A}_i$ such that $\mathcal{A}_i \mathcal{A}_j \subseteq \mathcal{A}_{i+j}$. Thus $1 \in \mathcal{A}_0$.*

Example 6.28. *$\mathcal{A} = k[X_1, ..., X_n]$, $\mathcal{I} = \mathbb{Z}_{\geq 0}$, and $\mathcal{A}_i :=\{$homogeneous elements if degree $i\}$. Then $\mathcal{A} = \oplus_{i \geq 0} \mathcal{A}_i$ is a $\mathbb{Z}_{\geq 0}$ graded ring.*

Another example is still the same $\mathcal{A}$ but with $\mathcal{I} = (\mathbb{Z}_{\geq 0})^n$ and $\mathcal{A}_I = kX_1^{i_1}...X_n^{i_n}$, where $I = (i_1, ..., i_n)$

Definition 6.29. *A **graded module** M over a graded ring $\mathcal{A} = \oplus_{i \in \mathcal{I}} \mathcal{A}_i$ is a module equipped with a decomposition $M = \oplus_{i \in \mathcal{I}} M_i$ s.t. $\mathcal{A}_i \cdot M_j \subseteq M_{i+j}$. A **graded submodule** $M' \subseteq M$ is then a submodule for which $M' = \oplus_{i \in \mathcal{I}}(M' \cap M_i)$. A graded ideal $\mathfrak{a}$ is graded submodule of $\mathcal{A}$ s.t. $\mathfrak{a} = \oplus_i (\mathfrak{a} \cap \mathcal{A}_i)$. We call elements of $\mathcal{A}_i \subseteq \mathcal{A}$ or $M_i \subseteq M$ **homogeneous**. Elements of $\mathcal{A}_i$ or M_i are homogeneous of degree i. A graded submodule of $\mathcal{A}$ itself is called **graded ideal**.*

Example 6.30. *$\mathcal{A} = k[x, y]$ with its $\mathbb{Z}_{\geq 0}$-grading. Then $\mathfrak{a} = (x^2 + y)$ is NOT a graded ideal. Indeed, $\mathfrak{a} \neq \sum_{i \geq 0}(\mathfrak{a} \cap \mathcal{A}_i) \not\ni x^2 + y$.*

One way to see this is to use the $\mathbb{Z}_{\geq 0}^2$-grading and visualize.

$\mathfrak{a} \cap \mathcal{A}_1 = \mathfrak{a} \cap \mathcal{A}_{(1,0)} \oplus \mathfrak{a} \cap \mathcal{A}_{(0,1)} = 0$, and in fact $\mathfrak{a} \cap \mathcal{A}_{(i,j)} = 0$.

Lemma 6.31. *Let M be graded module over a graded ring $\mathcal{A}$.*

(i) *A submodule $M' \subseteq M$ is a graded submodule $\iff$ M' is generated by homogeneous elements.*

(ii) *Moreover, if M' is a graded submodule and finitely generated as module, then it is generated by finitely many homogeneous elements.*

Proof.   (i) $M' \subseteq M$ is graded $\iff M' = \sum_i (M' \cap M_i) \implies M'$ generated by some homogeneous elements $(x_\alpha)_\alpha$, where $x_\alpha \in M_{i(\alpha)}$

Suppose M' generated by homogeneous elements $\{x_\alpha\}$. Then

$$\sum_i (M_i \cap M') \subseteq M' \subseteq \sum_\alpha \mathcal{A}x_\alpha$$

$$= \sum_{j,\alpha} \mathcal{A}_j x_\alpha$$

$$\subseteq \sum_{j,\alpha} M_{i(\alpha)+j} \cap M' \text{(By def of graded-module)}$$

$$\subseteq \sum_i (M_i \cap M').$$

(ii) $M' \subseteq M$ graded, finitely generated.
Similar proof. But now we start with a possibly infinite generating set of homogeneous elements H of M and a possibly non-homogeneous finite generating set F of M'. And notice that each element in F can be expressed as a finite linear expansion by elements in H. Then altogether, we can select a finite homogeneous generating set of M' in H.

$\square$

Recall the setup for Artin-Rees Lemma 6.26. $\mathcal{A}$ Noetherian ring, $\mathfrak{a}$ is an ideal and M finitely generated $\mathcal{A}$-module. Consider a $\mathbb{Z}_{\geq 0}$-graded ring. We denote by

$$\tilde{\mathcal{A}} := \boxplus_{i \geq 0} \mathfrak{a}^i := \{(x_i)_{i \geq 0} : x_i \in \mathfrak{a}^i, \text{with } x_i = 0 \text{ for almost all } i\}$$

$$\tilde{\mathcal{A}}_j = \{(x_i)_{i \geq 0} \in \tilde{\mathcal{A}} : x_j \in \mathfrak{a}^j, x_i = 0, \forall i \neq j\}.$$

Multiplication on $\tilde{\mathcal{A}}$ linearly extends the maps:

$$\mathfrak{a}^i \times \mathfrak{a}^j \longrightarrow \mathfrak{a}^{i+j}$$

Definition 6.32. *There is a natural source of graded $\tilde{\mathcal{A}}$-modules. $\tilde{M} = \boxplus_{i \geq 0} M_i$ form an $\mathfrak{a}$-**filtration** (M_i):*

- M_i *is a submodule of some $\mathcal{A}$-module M.*

- $\mathfrak{a}M_i \subseteq M_{i+1} \implies \mathfrak{a}^j M_i \subseteq M_{i+j}$

- $M_{i+1} \subseteq M_i$. *Thus* $\mathfrak{a}^i \times M_j \longrightarrow M_{i+j}$ *is defined.*

$\tilde{M}$ *is a graded* $\tilde{\mathcal{A}}$*-module.*

Definition 6.33. *We call a* $\mathfrak{a}$*-filtration* **stable** *if* $\exists k \geq 0 : \forall i \geq k, \mathfrak{a} M_i = M_{i+1} \Longrightarrow$ $(\mathfrak{a}^j M_i = M_{i+j})$.

Because $\mathcal{A}$ is Noetherian, we know $\mathfrak{a}$ is finitely generated by elements $x_1, ..., x_n$. Then we know $\tilde{\mathcal{A}}$ is finitely generated as an $\mathcal{A}$-algebra by $\tilde{\mathcal{A}} = \mathcal{A}[x_1, ..., x_n]$, then by Hilbert Basis Theorem 4.5, we know $\tilde{\mathcal{A}}$ is Noetherian.

Lemma 6.34. *Suppose* $(M_i) : \mathfrak{a}$*-filtration and* $\tilde{M}$ *is graded* $\tilde{\mathcal{A}}$*-module. Then* $\tilde{M}$ *is finitely generated* $\tilde{\mathcal{A}}$*-module iff the* $\mathfrak{a}$*-filtration* (M_i) *is stable.*

Proof. "$\Longleftarrow$": By definition, (M_i) stable ($\exists k \geq 0, \forall i \geq k, \mathfrak{a} M_i = M_{i+1}$) $\Longrightarrow$ $\tilde{M} = \tilde{\mathcal{A}} \boxplus_{i \leq k} M_k$, where we claim that each M_k is finitely generated $\mathcal{A}$-module. This is true because M is finitely generated module over a Noetherian ring $\mathcal{A}$, thus it is Noetherian by 4.4. And submodule of a Noetherian module is Noetherian. Then $\tilde{M}$ is finitely generated $\tilde{\mathcal{A}}$-module.

"$\Longrightarrow$". Assume $\tilde{M}$ is finitely generated $\tilde{\mathcal{A}}$-module, then we can choose k large enough such that

$$\tilde{M} = \tilde{\mathcal{A}} \boxplus_{i \leq k} M_k.$$

If we pick j-th component for $j \geq k$, we have

$$\begin{aligned} M_j &= \tilde{\mathcal{A}}_j \cdot M_0 + \tilde{\mathcal{A}}_{j-1} M_1 + ... + \tilde{\mathcal{A}}_{j-k} M_k \\ &= \mathfrak{a}^j M_0 + ... + \mathfrak{a}^{j-k} M_k \\ &\subseteq \mathfrak{a}^{j-k} M_k \end{aligned}$$

Then together with the definition of $\mathfrak{a}$-filtration, we know $\mathfrak{a}^{j-k} M_k = M_j$, thus the filtration is stable. $\qquad\square$

Now we come back to the proof of Artin-Ress Lemma 6.26 thus the Krull-intersection theorem 6.23. $\tilde{\mathcal{A}}$: Noetherian $\Longleftarrow \mathcal{A}$ Noetherian $\mathfrak{a}$: finitely generated as an $\mathcal{A}$ module . Suppose $\mathfrak{a}$ is generated as $(x_1, ..., x_r)$. By the Hilbert basis theorem, $\tilde{\mathcal{A}}$: Noetherian can be derived form $\tilde{\mathcal{A}}$ being finitely generated as an $\mathcal{A}$-module by $x_1, .., x_r \in \mathfrak{a}^1 = (\tilde{\mathcal{A}})_1$.

Proof. of Artin-Rees Lemma 6.26.
Assume its hypothesis, choose $\forall i \geq 0, M_i := \mathfrak{a}^i M$: then it is a stable $\mathfrak{a}$-filtration (i.e. $\mathfrak{a} M_i = \mathfrak{a} \cdot \mathfrak{a}^i M = \mathfrak{a}^{i+1} M = M_{i+1}$):

Because M is finitely generated over $\mathcal{A}$, we know $\tilde{M}$ is finitely generated over $\tilde{\mathcal{A}}$. Then we conclude by Lemma 6.34 that (M_i) is stable filtration.

Consider $M_i' = \mathfrak{a}^i M \cap M'$: an $\mathfrak{a}$-filtration. $\tilde{M}' := \boxplus_{i \geq 0} M_i'$. $\tilde{M}'$ is naturally a $\tilde{\mathcal{A}}$-submodule of $\tilde{M}$. <u>Want</u>: M_i' is a stable $\mathfrak{a}$-filtration.

<u>Know</u>: $\tilde{M}$ is finitely generated $\tilde{\mathcal{A}}$-module, and $\tilde{\mathcal{A}}$ is Noetherian
$\implies \tilde{M}$ is Noetherian.
$\implies \tilde{M}'$ is finitely generated $\tilde{\mathcal{A}}$-module hence also Noetherian.
$\implies (M_i')$ is stable $\mathfrak{a}$-filtration by Lemma 6.34.

Choose n large enough that the module $\tilde{M}'$ is generated by $\boxplus_{0 \leq i \leq n} M_i'$

$$\tilde{M}' = \tilde{\mathcal{A}} \boxplus_{0 \leq i \leq n} M_i'$$

$$\implies \mathfrak{a}^{n+1} M \cap \tilde{M}' = M_{n+1}' = \sum_{0 \leq i \leq n} \tilde{\mathcal{A}}_{n+1-i} M_i' = \sum_{0 \leq i \leq n} \mathfrak{a}^{n+1-i}(\mathfrak{a}^i M \cap M')$$

$$\subseteq \sum_{0 \leq i \leq n} \mathfrak{a}(\mathfrak{a}^n M \cap \mathfrak{a}^{n-i} M') \subseteq \mathfrak{a}(\mathfrak{a}^n M \cap M'),$$

which give the trickier inclusion of Artin-Rees. $\square$

We have proved the Artin-Rees Lemma and thus Krull's intersection theorem. <u>Recall</u> The theorem of Krull intersection says that if $\mathcal{A}$ is Noetherian, $\mathfrak{a} \subseteq \mathrm{Jac}(\mathcal{A})$, M is a finitely generated $\mathcal{A}$-module, then $\cap_i \mathfrak{a}^i M = 0$. Then we have the following corollaries

Corollary 6.35. *Suppose $\mathcal{A}$ Noetherian, $\mathfrak{a} \subseteq \mathrm{Jac}(\mathcal{A})$, then*

$$\cap_i \mathfrak{a}^i = 0$$

Corollary 6.36. *Suppose $(\mathcal{A}, \mathfrak{m})$ Noetherian, local, $\mathfrak{m} = \mathrm{Jac}(\mathcal{A})$, then*

$$\cap_i \mathfrak{m}^i = 0$$

Exercise 6.37. *Deduce Krull intersection theorem form Corollary 6.36.*

Proof. <u>Claim</u>: $(\mathcal{B}, \mathfrak{n})$ is Noetherian local, N is a finite $\mathcal{B}$-module: $\cap_i \mathfrak{n}^i = 0 \implies \cap_i \mathfrak{n}^i N = 0$. Suppose N is finitely generated by $\{x_\alpha\}$.

$$N' = \cap_i \mathfrak{n}^i N \subseteq \cap_i (\mathfrak{n}^i \oplus_\alpha \mathcal{B} x_\alpha) = \oplus_\alpha (\cap_i \mathfrak{n}^i) x_\alpha = 0,$$

the last equality from Corollary 6.36.

Then we start from the hypothesis of Krull's intersection theorem: $\mathcal{A}$ Noetherian, $\mathfrak{a} \subseteq \mathrm{Jac}(\mathcal{A})$, M is a finitely generated $\mathcal{A}$-module $M' = \cap \mathfrak{a}^i M$.

Pick an arbitrary maximal $\mathfrak{m}$ in $\mathcal{A}$. $\mathfrak{a} \subseteq \mathfrak{m}$. Then localize $\mathcal{A}$ and M at $\mathfrak{m}$. We get $\mathcal{A}_{\mathfrak{m}}$ and $M'_{\mathfrak{m}} = \cap(\mathfrak{a}_{\mathfrak{m}})^i M_{\mathfrak{m}} \subseteq \cap(\mathfrak{m}_{\mathfrak{m}})^i M_{\mathfrak{m}} = 0$, where $(\mathcal{A}_{\mathfrak{m}}, \mathfrak{m}_{\mathfrak{m}})$ is Noetherian local. The last equality by the claim above.

Then we know $M'_{\mathfrak{m}}$ vanish at every $\mathfrak{m}$, and we conclude by "being zero is a local property" 3.35.

$\square$

Question: Let $\mathfrak{p} \in Spec(\mathcal{A})$. What is $Ker(\mathcal{A} \longrightarrow \mathcal{A}_{\mathfrak{p}})$?

Definition 6.38. *The **nth symbolic power** $\mathfrak{p}^{(n)}$ of $\mathfrak{p}$ is defined by $\mathfrak{p}^{(n)} := \iota^*((\iota_*\mathfrak{p})^n) = \iota^*(\iota_*(\mathfrak{p}^n))$ for $\iota : \mathcal{A} \longrightarrow \mathcal{A}_{\mathfrak{p}}$.*

Proposition 6.39. *Let $\mathfrak{p}$ be a prime ideal in a ring $\mathcal{A}$. The n-th symbolic power of $\mathfrak{p}$ has the following properties:*

(a) $\mathfrak{p}^{(n)} = \{a \in \mathcal{A} : \exists s \in S := \mathcal{A} - \mathfrak{p}, \; s.t. \; as \in \mathfrak{p}^n\}$.

(b) $\mathfrak{p}^{(n)}$ is the $\mathfrak{p}$-primary component of $\mathfrak{p}^n$.

(c) $\mathfrak{p}^{(n)} = \mathfrak{p}^n$ iff $\mathfrak{p}^n$ is $\mathfrak{p}$-primary.

Here, we will give an application of Krull's intersection theorem.

Theorem 6.40. *$\mathcal{A}$-Noetherian, then $Ker(\mathcal{A} \longrightarrow \mathcal{A}_{\mathfrak{p}}) = \cap_{i \geq 0}\mathfrak{p}^{(i)}$.*

Proof. We know $Ker(\mathcal{A} \longrightarrow \mathcal{A}_{\mathfrak{p}}) = \iota^*((0)) \overset{?}{=} \cap_{i \geq 0}\iota^*(\iota_*(\mathfrak{p})^i)$. The last equality is guaranteed by the Corollary 6.36 because $(0) = \cap_{i \geq 0}\iota_*(\mathfrak{p})^i$, where $\iota_*(\mathfrak{p})$ is the maximal in the local Noetherian ring $\mathcal{A}_{\mathfrak{p}}$. $\square$

6.4 Lecture 17. Krull's Principal Ideal Theorem

We start from a special case of Krull's principal ideal theorem and will eventually reduce the theorem to the special case.

Lemma 6.41. *$\mathcal{A}$ Noetherian local integral domain: (0) prime $\subseteq \mathfrak{m}$ maximal $\subseteq \mathcal{A}$. Then the following are equivalent:*

(i) $\exists$ prime $\mathfrak{p}$ with $(0) \subsetneq \mathfrak{p} \subsetneq \mathfrak{m}$

(ii) $\forall f \in \mathfrak{m}, \exists$ prime $\mathfrak{p} \ni f \; s.t. \; , \; (0) \subsetneq \mathfrak{p} \subsetneq \mathfrak{m}$

In other words, this means $\mathfrak{m}$ is the minimal prime that contains some (f) iff $Spec(\mathcal{A}) = \{(0), \mathfrak{m}\}$.

N.b. $(ii) \Longrightarrow (i)$ is clear: take $f = 0$.

Example 6.42. $\mathcal{A} = k[[X, Y]] \supseteq \mathfrak{m} = (X, Y) \supseteq (0)$. There exists $(0) \subsetneq \mathfrak{p} \subsetneq \mathfrak{m}$, e.g., $\mathfrak{p} = (X)$. The conclusion says that $\forall f \in \mathfrak{m} \exists$ prime $\mathfrak{p} \ni f$ with $(0) \subsetneq \mathfrak{p} \subsetneq \mathfrak{m}$, e.g. $f = Y \in \mathfrak{m}$

Definition 6.43. $dim(\mathcal{A}) = \sup\{t \geq 0 : \exists$ chain of primes $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq ... \subsetneq \mathfrak{p}_t \subseteq \mathcal{A}\}$

*For prime $\mathfrak{p} \subseteq \mathcal{A}$: **height** $ht(\mathfrak{p}) := \sup\{t \geq 0 | \exists chain \; \mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_t = \mathfrak{p}\}$*

$$ht(\mathfrak{p}) = dim(\mathcal{A}_\mathfrak{p})$$

Coheight: $coht(\mathfrak{p}) := \sup\{t \geq 0 | \exists \mathfrak{p} = \mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_t \subsetneq \mathcal{A}\}$

$$coht(\mathfrak{p}) = dim(\mathcal{A}/\mathfrak{p})$$

Another version:

Lemma 6.44. $0 \neq f($ non-unit $) \in \mathcal{A}$: Noetherian integral domain. Then any minimal prime $\mathfrak{m}_0$ of (f) satisfies $ht(\mathfrak{m}_0) = 1$, where $\mathfrak{m}_0 \supseteq (f)$ minimal for this property, in other words, "$\mathfrak{m}_0 \in Ass'((f))$", see 5.33.

Reduce Lemma 6.44 to Lemma 6.41, we may assume that $\mathcal{A}$ is local with $\mathfrak{m}$ the maximal ideal:

- replace $\mathcal{A}$ by $\mathcal{A}_\mathfrak{m}$, $\iota : \mathcal{A} \longrightarrow \mathcal{A}_\mathfrak{m}$

- replace $\mathfrak{m}$ by $\iota_*(\mathfrak{m})$

- replace f by $f/1 = \iota(f)$

Then there are bijections

$$\{\text{primes } \mathfrak{p} \subseteq \mathfrak{m}\} \longleftrightarrow \{\text{primes of } \mathcal{A}_\mathfrak{m}\}$$

and

$$\{\text{primes } \mathfrak{p} \ni f\} \longleftrightarrow \{ \text{ primes of } \mathcal{A}_\mathfrak{m} \text{ that contains } f/1\}$$

So $(\mathcal{A}_\mathfrak{m}, \iota_*\mathfrak{m})$ is Noetherian local domain and $ht(\iota_*(\mathfrak{m})) = ht(\mathfrak{m})$. (We will reload it as $(\mathcal{A}, \mathfrak{m})$)

<u>Know</u>: $\mathfrak{m} \in Ass'((f))$, i.e., $\nexists$ prime $\mathfrak{p} \ni f$ s.t. $(0) \subsetneq \mathfrak{p} \subsetneq \mathfrak{m}$ (We know $\mathfrak{p} \ni f \neq 0$, if $f \in \mathfrak{p} \subsetneq \mathfrak{m}$, then $\mathfrak{m}$ would not be a minimal prime of (f)).

<u>Want</u>: $ht(\mathfrak{m}) = 1$, i.e., $1 = \sup T$ where $T := \{t \geq 0, \exists chain \mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_t = \mathfrak{m}\}$. which is equivalent to

- $(0) \subsetneq \mathfrak{m}, (\Longleftarrow \mathfrak{m} \ni f \neq 0), \quad T \geq 1$

- $\nexists$ prime $\mathfrak{p} : (0) \subsetneq \mathfrak{p} \subsetneq \mathfrak{m}, \quad T < 2,$

Which is true if we assume Lemma 6.41.

Now we come back to the proof of the special case of Noetherian local domain.

Proof. "$(i) \Longrightarrow (ii)$" in Lemma 6.41

$(ii) \Longleftrightarrow \dim(\mathcal{A}/(f)) \geq 1, \forall f \in \mathfrak{m}$, there are two bijections:

$$\mathfrak{m} \longleftrightarrow \text{ a maximal ideal in } \mathcal{A}/(f),$$

$$\mathfrak{m} \supsetneq \mathfrak{p} \supseteq (f) \longleftrightarrow \text{ a prime ideal in } \mathcal{A}/(f).$$

Consider the canonical projection $\pi : \mathcal{A} \longrightarrow \mathcal{A}/(f)$. Let $\mathfrak{p}$: prime s.t. $\mathfrak{m} \supsetneq \mathfrak{p} \not\ni f$.

Assume the negation of $(ii) \Longleftrightarrow \dim(\mathcal{A}/(f)) = 0$. Then by Theorem 6.12, $\frac{\mathcal{A}}{(f)}$ is Artinian. $\Longrightarrow \exists k$ s.t., $\forall i \geq k$, $\mathfrak{p}^{(k)} + (f) = \mathfrak{p}^{(i)} + (f)$, where $\mathfrak{p}^{(k)}$ is the k-th symbolic power defined in 6.38.

Indeed, $\frac{\mathfrak{p}^{(k)} + (f)}{(f)}$ is a descending chain in $\frac{\mathcal{A}}{(f)}$.

The negation of (ii) : $\exists f \in \mathfrak{m}$ s.t. $\forall \mathfrak{p}$ prime , either

(a). NOT $(0 \subsetneq \mathfrak{p} \subsetneq \mathfrak{m})$

or

(b). $\mathfrak{p} \not\ni f$

Case (a). OK $\Longrightarrow$ NOT (i) for this $\mathfrak{p}$

Case (b). We focus on this now.

<u>Know</u>: $f \notin \mathfrak{p} \subsetneq \mathfrak{m}$.

<u>Want</u>: $\mathfrak{p} = (0)$

As above, $\exists k, \forall i \geq k$:

$$\mathfrak{p}^{(k)} \subseteq \mathfrak{p}^{(i)} + (f) \tag{*}$$

Claim:

$$\mathfrak{p}^{(k)} = \mathfrak{p}^{(i)} + (f)\mathfrak{p}^{(k)} : \tag{**}$$

Proof. of Claim:

"$\supseteq$" ✓

"$\subseteq$". Let $x \in \mathfrak{p}^{(k)}$. By (*) $\exists y \in \mathfrak{p}^{(i)}, z \in \mathcal{A}$ s.t. $x = y + fz$

$x - y = fz \in \mathfrak{p}^{(k)}$

$\Longrightarrow z \in (\mathfrak{p}^{(k)} : f) = \mathfrak{p}^{(k)}$ ($\mathfrak{p}^{(k)}$ is $\mathfrak{p}$-primary and $\mathfrak{p} \not\ni f$, we conclude the equality $(\mathfrak{p}^{(k):f}) = \mathfrak{p}^{(k)}$ by 5.20)

Taking $i \geq k$, $\mathfrak{p}^{(k)} \subseteq \mathfrak{p}^{(i)} + (f)\mathfrak{p}^{(k)}$, hence we have prove the claim. □

Then we take $i = k+1$ and consider the module $M := \mathfrak{p}^{(k)}/\mathfrak{p}^{(k+1)}$. (Claim:$\mathfrak{p}^{(k)} = \mathfrak{p}^{(k+1)} + f\mathfrak{p}^{(k)})\Longrightarrow$

$$\mathfrak{p}^{(k)}/\mathfrak{p}^{(k+1)} = (\mathfrak{p}^{(k+1)} + (f)\mathfrak{p}^{(k)})/\mathfrak{p}^{(k+1)} = (f)\mathfrak{p}^{(k)}/\mathfrak{p}^{(k+1)}$$

$\mathcal{A}$ is local Noetherian, then $(f) \subseteq \mathrm{Jac}(\mathcal{A}) = \mathfrak{m}$.

$$(f)M = M \Longrightarrow M = \mathfrak{p}^{(k)}/\mathfrak{p}^{(i)} = 0 \text{ by Nakayama 2.17.}$$

$\Longrightarrow \mathfrak{p}^{(i)} = \mathfrak{p}^{(k)},\ \forall i \geq k$
$\Longrightarrow \mathfrak{p}^{(k)} = \cap_i \mathfrak{p}^{(i)} = \mathrm{Ker}(\mathcal{A} \longrightarrow \mathcal{A}_\mathfrak{p})$, by Theorem 6.40. But $\mathrm{Ker}(\mathcal{A} \longrightarrow \mathcal{A}_\mathfrak{p}) = 0$
because $\mathcal{A}$ is a domain.
$\Longrightarrow \mathfrak{p}^k \subseteq \mathfrak{p}^{(k)} = (0)$
Because $\mathcal{A}$ is domain, $\mathfrak{p}^{(k)} = 0 \Longrightarrow \mathfrak{p} = (0)$ as desired. $\square$

Theorem 6.45. *(Krull's Principal Ideal Theorem) $\mathcal{A}$ a Noetherian ring and $a \in \mathcal{A}$ is non-unit and non-zerodivisor. $\mathfrak{p} \in Ass'((a))$, i.e. $\mathfrak{p} \supseteq (a)$ is minimal. Then $ht(\mathfrak{p}) = 1$.*

Recall: $\dim(\mathcal{A}) = \sup\{t \geq 0 | \exists \text{chain } \mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_t \subseteq \mathcal{A}\}$
$\mathfrak{p}$ prime: $ht(\mathfrak{p}) = \sup\{t \geq 0 | \exists \text{chain } \mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_t = \mathfrak{p}\}$

Definition 6.46. *$\mathfrak{a}$ is any ideal in $\mathcal{A}$. The **height** of $\mathfrak{a}$, $ht(\mathfrak{a}) = \inf\{ht(\mathfrak{p})|\mathfrak{p} \supseteq \mathfrak{a}\}$ and **coheight** $coht(\mathfrak{a}) = \sup\{coht(\mathfrak{p})|\mathfrak{p} \supseteq \mathfrak{a}\}$*

Then the Theorem 6.45 is equivalent to "if a is non-unit and non-zerodivisor, then $ht((a)) = 1$ "

Proof. $\mathcal{A}$ Noetherian, $\Longrightarrow (0)$ decomposable, where $(0) = \cap_i \mathfrak{q}_i$, minimal priamry decomposition, $\mathfrak{p}_i = \mathrm{rad}(\mathfrak{q}_i)$
    Recall:
$$\{\text{zero-divisors in } \mathcal{A}\} = \cup_i \mathfrak{p}_i,$$

thus $a \notin \mathfrak{p}_i \forall i$. Let i s.t. $\mathfrak{p} \supseteq \mathfrak{p}_i$ (exists because $\{\mathfrak{p}_i\} \supseteq \{\text{minimal primes of } \mathcal{A}\}$)
    $a \in \mathfrak{p}, a \notin \mathfrak{p}_i, \Longrightarrow \mathfrak{p}_i \subsetneq \mathfrak{p} \Longrightarrow ht(\mathfrak{p}) \geq 1$
    <u>Want</u>: $ht(\mathfrak{p}) = 1$. If not, we can find a longer chain $\mathfrak{p}'' \subsetneq \mathfrak{p}' \subsetneq \mathfrak{p}$, we assume $\mathfrak{p}''$ minimal, and then after changing the index (if necessary), set $\mathfrak{p}'' = \mathfrak{p}_i$.
    Now replace $\mathcal{A}$ by $\mathcal{A}/\mathfrak{p}_i$, $\mathfrak{p}'$ by $\mathfrak{p}'/\mathfrak{p}_i$, $\mathfrak{p}$ by $\mathfrak{p}/\mathfrak{p}_i$, a by its image.
    Then $\mathcal{A}$ Noetherian integral domain, $0 \neq a \in \mathcal{A}, a \in \mathfrak{p}, \mathfrak{p} \supset (a)$, minimal. Then by Lemma 6.44$\Longrightarrow \nexists \mathfrak{p}' : (0) \subsetneq \mathfrak{p}' \subsetneq \mathfrak{p} \Longrightarrow \dim(\mathfrak{p}) = 1$. $\square$

Remark 6.47. *If $0 \neq f \in \mathbb{C}[X_1, .., X_N]$, $Z(f)$ being the zero loci of f. Then every irreducible component X of $Z(f)$ has dimension $N-1$.*

$Z(f) \longleftrightarrow$ *prime* $\mathfrak{p} \ni f$
$X \longleftrightarrow$ *minimal primes* $\mathfrak{p} \supseteq (f)$
$codim_{\mathbb{C}^N}(X) = 1 \Longleftrightarrow ht(\mathfrak{p}) = 1$

Recall from linear algebra: if V is finite dimensional vector space over field k, and l is a nonzero linear functional on V, then

$$\dim(ker(V)) = \dim(V) - 1$$

Krull dimension theorem is a variant for polynomials.

6.5   Lecture 18. Krull Dimension Theorem

Geometric Interpretation: suppose $k = \bar{k}$, Suppose $\mathcal{A} = k[x_1, .., x_n]/\mathfrak{q}$ (some prime $\mathfrak{q}$) $\longleftrightarrow X = V(\mathfrak{q})$ irreducible variety in k^n, where $V(\mathfrak{q}) = \{z | f(z) = 0 \forall f \in \mathfrak{q}\}$.

Then $\dim(\mathcal{A}) \longleftrightarrow \dim(X) := \sup\{t \geq 0 : \exists$ chain of irreducible subvarieties $X = X_0 \supsetneq X_1 \supsetneq ... \supsetneq X_t\}$

$\{$primes in $\mathcal{A}\} \longleftrightarrow \{$primes $\mathfrak{p}$ in $k[x_1, .., x_n] \mid \mathfrak{p} \supsetneq \mathfrak{q}\}$ one to one corresponds to $Y \subseteq X$ irreducible subvarieties. (this correspondence is inclusion reversing)

$ht(\mathfrak{p}) \longleftrightarrow codim_X(Y) := \sup\{t \geq 0 | \exists$chain of irreducible subvarieties such that $X = X_0 \supsetneq X_1 \supsetneq ... \supsetneq X_t = Y\}$

$\mathfrak{a} \subseteq \mathcal{A}$ any ideal with $\text{rad}(\mathfrak{a}) = \mathfrak{a} \longleftrightarrow Z \subseteq X$ closed subvariety

$\mathfrak{p}_i \in \text{Ass}'(\mathfrak{a}) i.e. \mathfrak{p}_i \supseteq \mathfrak{a}$ minimal $\longleftrightarrow$ irreducible components $Y_i \subseteq Z$

$codim_X(Z) = \inf_{Y_i}\{codim_X(Y_i) | Y_i$ is irreducible component of $Z\}$

$\text{coht}(\mathfrak{p}) = \dim(\mathcal{A}/\mathfrak{p}) \longleftrightarrow \dim(Y)$

$\text{coht}(\mathfrak{a}) = \dim(\mathcal{A}/\mathfrak{a}) = \sup_i\{\text{coht}(\mathfrak{p}_i)\}$

$\dim(Z) = \sup\{\dim(Y_i) | Y_i$ is irreducible component of $Z\}$

Krull principal intersection theorem says :"Every irreducible component of a hypersurface in X has codimension 1"

$ht(\mathfrak{a}) = 1 : codim_X(Z) = 1$, $X, \emptyset \neq Z \longleftrightarrow \mathfrak{a} = (a)$, where $Z = \{p \in X : a(\mathfrak{p}) = 0\}$ (subset cut out by one equation) and $a \neq 0$ non-unit

$\mathfrak{p}_i \supseteq \mathfrak{a}$ minimal $ht(\mathfrak{p}) = 1 \longleftrightarrow codim_X(Y_i) = 1 \longleftrightarrow Y_i \subseteq Z$ irreducible component.

Theorem 6.48. *(Krull Dimension Theorem) Let $\mathcal{A}$ Noetherian, $r \geq 1$, $a_1, .., a_r \in \mathcal{A}$, $\mathfrak{a} = (a_1, ..., a_r)$, $\mathfrak{p} \in Ass'(\mathfrak{a})$. Then $ht(\mathfrak{p}) \leq r$.*

Geometrically:"every subvariety cut out by $\leq r$ equations has codimension $\leq r$"

Proof. Induct on $r \geq 1$. $r = 1$ case is just the Krull's intersection theorem. Suppose $\exists$ chain $\mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_t = \mathfrak{p}$

<u>Want</u>: $t \leq r$. Replace $\mathcal{A}$ by $\mathcal{A}_\mathfrak{p}$, which does not change the height or the minimality assumption. Reduce to the case $(\mathcal{A}, \mathfrak{p})$ $\mathcal{A}$ is Noetherian local ring and $\mathfrak{p}$ is the maximal ideal in $\mathcal{A}$. We know $\mathfrak{p}$ is the minimal among those primes containing $\mathfrak{a}$ $\Longrightarrow \mathfrak{p}$ is the only prime that contain $\mathfrak{a}$.

So $\mathfrak{p}_t = \mathfrak{p}$ containing $\mathfrak{a}$ being minimal $\mathfrak{p}_{t-1} \not\supseteq \mathfrak{a}$ $\exists$ generator of $\mathfrak{a}$ not in $\mathfrak{p}_{t-1}$. Suppose $a_r \notin \mathfrak{p}_{t-1}$.

We may assume, enlarging the chain as necessary, that there are no primes between $\mathfrak{p}_{t-1}$ and $\mathfrak{p}_t$. (If $\exists$ prime between $\mathfrak{p}_{t-1}, \mathfrak{p}_t$, then $\exists$ a prime $\mathfrak{q}$ s.t. maximal with the property $\mathfrak{p}_{t-1} \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}_t$, then add $\mathfrak{q}$ to our chain. We can always attain the maximal one because $\mathcal{A}$ is Noetherian)

$\mathfrak{p}_{t-1} \subsetneq \mathfrak{p}_{t-1} + (a_r) \subseteq \mathfrak{p}_t \Longrightarrow$ "$\mathfrak{p} = \mathfrak{p}_t$ is the only prime containing $\mathfrak{p}_{t-1} + (a_r)$"
$\Longrightarrow \mathrm{rad}(\mathfrak{p}_{t-1} + (a_r)) = \mathfrak{p} \supseteq \mathfrak{a} \ni a_i$
$\Longrightarrow \exists N \geq 1 : a_i^N = a_i' + a_r y_i \in \mathfrak{p}_{t-1} + (a_r)$
Define $\mathfrak{a}' := (a_1', ..., a_{r-1}') \subseteq \mathfrak{p}_{t-1}$.

<u>Want</u>:$\mathfrak{p}_{t-1} \in \mathrm{Ass}'(\mathfrak{a}')$. If we can show this, then our inductive hypothesis gives $t - 1 \leq r - 1 \Longrightarrow t \leq r$. Let $\mathfrak{p}' \in \mathrm{Ass}'(\mathfrak{a}')$ s.t. $\mathfrak{p}' \subseteq \mathfrak{p}_{t-1} \subsetneq \mathfrak{p}_t = \mathfrak{p}$ (Such a $\mathfrak{p}'$ exists.)

To show that $\mathfrak{p}' = \mathfrak{p}_{t-1}$, it suffices to show $\mathrm{ht}(\mathfrak{p}/\mathfrak{p}') \leq 1$ in $\mathcal{A}/\mathfrak{p}'$. Let $\bar{a}_r :=$ images of a_r in $\mathcal{A}/\mathfrak{p}'$. By the Krull's principal ideal theorem 6.45, it will suffice to show that $\mathfrak{p}/\mathfrak{p}' \in \mathrm{Ass}'((\bar{a}_r)) \Longleftarrow \mathfrak{p} = \mathrm{rad}(\mathfrak{p}' + (a_r))$.
To see this:
$\mathfrak{p} = \mathrm{rad}(\mathfrak{a}) = \mathrm{rad}(\mathfrak{a}' + (a_r)) \subseteq \mathrm{rad}(\mathfrak{p}' + (a_r)) \subseteq \mathrm{rad}(\mathfrak{p}) = \mathfrak{p}$. $\qquad\qquad\square$

Corollary 6.49. *$\mathcal{A}$ Noetherian, $\mathfrak{a}$ is an ideal in $\mathcal{A}$*
$\Longrightarrow ht(\mathfrak{a}) < \infty$.

Proof. $\mathfrak{a} = (a_1, ..., a_r) \Longrightarrow \mathrm{ht}(\mathfrak{a}) \leq r$ by the above theorem. $\qquad\qquad\square$

Remark by TeXer 6.50. *This means each Noetherian semi-local ring is finite dimensional. But still a general Noetherian ring can be infinite dimensional. A counter example is given by Nagata, which solved Hilbert's 14th problem.*

Corollary 6.51. *$(\mathcal{A}, \mathfrak{m})$: Noetherian local ring with the maximal ideal. $k := \mathcal{A}/\mathfrak{m}$ field. Then $dim(\mathcal{A}) \leq dim_k(\mathfrak{m}/\mathfrak{m}^2)$. $\mathfrak{m}/\mathfrak{m}^2$ is called **Zariski cotangent space** and $\mathcal{A}$ is called **regular** if the equality holds.*

N.b.: $\forall$ $\mathcal{A}$-module M, the quotient $M/\mathfrak{m}M$ is a k-vector space.

Proof. Suppose, $r = dim_k(\mathfrak{m}/\mathfrak{m}^2)$, $\pi(f_1), ... \pi(f_r)$ is a basis of $\mathfrak{m}/\mathfrak{m}^2$. Let $f_1, ..., f_r \in \mathfrak{m}$ be lifts of the f_i.

Set $M = \mathfrak{m}$, $N := M/(f_1, ..., f_r)$.

Claim: $\mathfrak{m}N = N$. $N = \frac{M}{\mathfrak{m}M}$, Want: $\mathfrak{m}N \supseteq N \iff \forall y \in M, \exists z \in M, m \in \mathfrak{m} s.t. y = m \cdot z + \sum_i \alpha_i f_i$. And in fact, we know $\pi(y) = \sum_i \alpha_i \pi(f_i) \implies \pi(y - \sum_i \alpha_i f_i) = 0 \implies \exists mz \in \mathfrak{m}M$ s.t. $mz + \sum_i \alpha_i f_i = y$. done.

Then by Nakayama lemma 2.17, $N = 0 \implies \mathfrak{m} = (\tilde{a}_1, ... \tilde{a}_r) \implies ht(\mathfrak{m}) = \dim(\mathcal{A}) \leq r$ $\qquad\square$

Corollary 6.52. $\mathcal{A}$ *Noetherian,* $\mathfrak{a}$ *is an ideal in* $\mathcal{A}$ *with* $ht(\mathfrak{a}) = r$. *Then exists* $a_1, ..., a_r \in \mathfrak{a} : ht(\mathfrak{a}) = ht((a_1, ..., a_r))$.

Proof. It suffice by induction to show: For $s \leq r$, if we can find $a_1, ..., a_{s-1} \in \mathfrak{a}$ with $ht((a_1, ..., a_{s-1})) = s - 1$, then there exists an $a_s \in \mathfrak{a}$ s.t. $ht((a_1, ..., a_s)) = s$.
Consider a MPD $\mathfrak{b} = (a_1, .., a_{s-1}) = \cap \mathfrak{q}_i$ with $\mathfrak{p}_i = rad(\mathfrak{q}_i)$

$ht(\mathfrak{b}) = s - 1$

It will suffice to show that $\mathfrak{a} \not\subseteq \cup \mathfrak{p}_i$ then any $a_s \in \cup \mathfrak{p}_i - \mathfrak{a}$ will give

$ht(a_1, ... a_s) \leq s$ by Krull dimension theorem 6.48

$ht(a_1, ..., a_s) \geq s$ by considering MPD.

For a complete proof, see the Theorem 6.53 $\qquad\square$

6.6 Lecture 19. System of Parameters

<u>Know</u>: $\mathcal{A}$ Noetherian, $r \geq 1$, $\mathfrak{a} = (a_1, ..., a_r), a_i \in \mathcal{A}$, $\mathfrak{p} \supset \mathfrak{a}$ minimal, then

$$ht(\mathfrak{p}) \leq r.$$

If $r = 1$, and a_1 : not a zero divisor, then $ht(\mathfrak{p}) = 1$.

What about the reverse direction?

Theorem 6.53. *(Converse to Krull)*
$\mathfrak{a} \subset \mathcal{A}$, *Noetherian, set* $r = ht(\mathfrak{a}) : \inf\{ht(\mathfrak{p}) | \mathfrak{p} \supset \mathfrak{a}, \mathfrak{p} prime\}$ *Then*

(i) $\forall s = 1, ..., r \; \exists x_1, ..., x_s \in \mathfrak{a}$ *such that* $ht(x_1, .., x_s) = s$

(ii) *Let* $\mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_r$ *be a chain that realize the height of* $\mathfrak{a}$, *then we can find* $x_1, ..., x_r \in \mathfrak{a}$ *s.t.* $\mathfrak{p}_i \supset (x_1, .., x_i)$ *is minimal.*

(iii) *Any prime* $\mathfrak{p}$ *of* $ht(\mathfrak{p}) = r$ *is a minimal prime of some ideal* $(a_1, ..., a_r)$

<u>Note:</u> (i) $\implies$ (iii) take $\mathfrak{a} = \mathfrak{p}, s = r : ht(x_1, ..., x_r) = r = ht(\mathfrak{p})$, $\mathfrak{p} \supset (x_1, ..., x_r)$ is minimal.

Proof. (i): $\text{ht}(\mathfrak{a}) = r$, then we can find some chain $\mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_r$ s.t. there is no intermediate primes between each $\mathfrak{p}_i, \mathfrak{p}_j, i, j \leq r$. We pick up the first s primes in this chain, $\mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_s$.

We induct on s, . Assume we have found $x_1, ..., x_s$ s.t. $\mathfrak{p}_i \supset (x_1, ..., x_i)$ minimal $\forall i \leq s$, then $\text{ht}(\mathfrak{p}_i) \leq i$ by Theorem 6.48. On the other hand, $\text{ht}(\mathfrak{p}_i) \geq i$ by the existence of $\mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_i \implies \text{ht}(\mathfrak{p}_i) = i, \forall i \leq s$.

Consider the minimal primes $\{\mathfrak{q}_j\} = \text{Ass}'((x_1, ..., x_s))$, then $\mathfrak{p}_s$ is one of $\mathfrak{q}_j$.

Claim: $\mathfrak{p}_{s+1} \not\subset \cup_j \mathfrak{q}_j$.

Indeed, if not, since $\mathfrak{q}_j$ prime $\mathfrak{p}_{i+1} \subseteq \mathfrak{q}_j$ for some j, by the "avoidance of primes" 1.27. Then $\text{ht}(\mathfrak{q}_j) \leq s$, by Krull dimension 6.48, but $\text{ht}(\mathfrak{p}_{s+1}) \geq s + 1$. Contradiction, thus the claim holds.

Choose $x_{s+1} \in \mathfrak{p}_{s+1} - \cup_j \mathfrak{q}_j$. Then $\mathfrak{p}_{s+1} \supseteq (x_1, .., x_{s+1})$. Except for the $s+1 = r$ case, x_{s+1} is automatically in $\mathfrak{a}$. If $s+1 = r$, we can choose $x_r \in \mathfrak{a} - \cup_j \mathfrak{q}_j$ because $\mathfrak{a} \not\subset \cup_j \mathfrak{q}_j$, otherwise contradicts the height of $\mathfrak{a}$.

<u>Want:</u>$\mathfrak{p}_{s+1} \in \text{Ass}'((x_1, ..., x_{s+1}))$, so $\mathfrak{p}_{s+1} \supsetneq$ some $\mathfrak{q}_j$ as above, in particular $\mathfrak{p}_{s+1} \supsetneq \mathfrak{p}_s$.

Take $\mathfrak{p}' \in \text{Ass}'((x_1, .., x_{s+1}))$ s.t. $\mathfrak{p}_{s+1} \supseteq \mathfrak{p}'$. Then claim: $\text{ht}(\mathfrak{p}') = s + 1$,

for the proof of the claim: $\text{ht}(\mathfrak{p}') \leq s + 1$ by Krull, and $\text{ht}(\mathfrak{p}') \geq s + 1$ because $\mathfrak{p}'$ is not a minimal prime $\mathfrak{q}_j$ of $\mathfrak{p}_s$ because $\mathfrak{p}' \supsetneq \mathfrak{p}_s$

If $(\mathfrak{p}' \subsetneq \mathfrak{p}_{s+1})$ we can get a contradiction on our initial choice of chain that realize the height of $\mathfrak{a}$.

We have finished the proof of induction steps. For the case $s = 1$, the claim of (i) reduce to Krull's principal ideal theorem 6.45. The choice of $(x_1, ..., x_s)$ above also implies (ii). $\square$

Corollary 6.54. *: $(\mathcal{A}, \mathfrak{m})$ Noetherian Local, Thus $dim(\mathcal{A}) = ht(\mathfrak{m}) \leq \infty$.*

Then $\exists x_1, ..., x_n \in \mathfrak{m}$ s.t. $\mathfrak{m}$ is minimal over $(x_1, ..., x_n)$. Then $\mathfrak{m}$ is the only prime containing $(x_1, .., x_n)$, so $\mathfrak{m} = \text{rad}((x_1, ..., x_n))$ and $(x_1, ..., x_n)$ is $\mathfrak{m}$-primary. (Recall that any ideal whose radical is maximal is primary 5.12)

Definition 6.55. *$(\mathcal{A}, \mathfrak{m})$ Noetherian Local, we say when $n = dim(\mathcal{A}) = ht(\mathfrak{m})$ that $x_1, ..., x_n$ are **parameters** for $\mathfrak{m}$ (or form a **system of parameters**). Equivalently, any of the following holds:*

(i) $\mathfrak{m} \supseteq (x_1, ..., x_n)$ *is minimal*

(ii) $\mathfrak{m} = rad(x_1, ..., x_n)$

(iii) $(x_1, ..., x_n)$ *is $\mathfrak{m}$-primary.*

Theorem 6.56. $(\mathcal{A}, \mathfrak{m})$ *is Noetherian Local,* $dim(\mathcal{A}) = ht(\mathfrak{m}) = min\{n \geq 1 : \exists x_1, ..., x_n \ s.t. \ \mathfrak{m} \subseteq (x_1, .., x_n) \ minimal.\}$

Proof. $\geq$ converse of Krull

$\leq$ Krull $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ □

Theorem 6.57. $(\mathcal{A}, \mathfrak{m})$ *Noetherian local. Let* $x_1, .., x_r \in \mathfrak{m}$. *Consider the following assertions:*

(i) *We can extend* $x_1, .., x_r$ *to a system of parameters for* $\mathfrak{m}$.

(ii) $dim(\mathcal{A}/(x_1, .., x_r)) = dim(\mathcal{A}) - r$.

(iii) $ht((x_1, ..., x_r)) = r$

Then $(i) \Longleftrightarrow (ii) \Longleftarrow (iii)$

Proof. $(iii) \Longrightarrow (i)$: If $x_1, ..., x_r$ are not already a system of parameters, then $\mathfrak{m} \supseteq (x_1, .., x_r)$ is not minimal. So we can find $\mathfrak{m} =: \mathfrak{p}_{r+1} \supsetneq \mathfrak{p}_r \supsetneq ... \supsetneq \mathfrak{p}_0$ and apply the converse of Krull 6.53 to obtain $x_{r+1} \in \mathfrak{p}_{r+1} = \mathfrak{m}$ s.t. $ht(x_1, .., x_{r+1}) = r + 1$. Continue finitely many times to set the required system of parameters.

It remains to show $(i) \Longleftrightarrow (ii)$.

"$(i) \Longrightarrow (ii)$": Consider $y_1, .., y_s \in \mathfrak{m}$. Let $\overline{\mathcal{A}} := \mathcal{A}/(x_1, .., x_r)$. $\overline{\mathcal{A}} \supseteq \overline{\mathfrak{m}} :=$ Image of $\mathfrak{m}$. Then $(\overline{\mathcal{A}}, \overline{\mathfrak{m}})$ is Noetherian local. Write $\overline{y}_1, ..., \overline{y}_s \in \overline{\mathcal{A}}$ the image of $y_1, .., y_s$

$\{x_1, ..., x_r, y_1, ..., y_s\}$ system of parameters, by definition, is equivalent to $r + s = dim(\mathcal{A})$ and $(x_1, ..., x_r, y_1, ..., y_s)$ is $\mathfrak{m}$-primary.

Note:$(x_1, ..., x_r, y_1, ..., y_s)$ $\mathfrak{m}$-primary

$\Longleftrightarrow \mathfrak{m}$ is the only prime containing $(x_1, .., y_s)$

$\Longleftrightarrow \overline{\mathfrak{m}}$ is the only prime containing $(\overline{y}_1, ..., \overline{y}_s)$

$\Longleftrightarrow (\overline{y}_1, ..., \overline{y}_s)$: $\overline{\mathfrak{m}}$-primary

$\{\overline{y}_1, ..., \overline{y}_s\}$ system of parameters for $(\overline{\mathcal{A}}, \overline{\mathfrak{m}}) \Longleftrightarrow s = dim(\overline{\mathcal{A}})$ and $(\overline{y}_1, ..., \overline{y}_s)$ is $\overline{\mathfrak{m}}$-primary.

FACT1:$[\exists y_1, ..., y_s \ s.t. \ (x_1, ..., x_r, y_1, ..., y_s)$ is $\mathfrak{m}$- primary$] \Longrightarrow dim(\mathcal{A}) \leq r + s$, by Krull's dimension theorem 6.48.

And in fact, if we start we a system of parameters $(\overline{z}_1, ..., \overline{z}_t)$ of $\overline{\mathcal{A}}$, z_i are their preimages in $\mathcal{A}$, we have proved that $(x_1, ..., x_r, z_1, ..., z_t)$ is $\mathfrak{m}$ primary, then $dim(\mathcal{A}) \leq t + r = dim(\overline{\mathcal{A}}) + r$

$(i) \Longrightarrow \exists y_1, .., y_s \ s.t., \ \{x_1, ...x_r, y_1, ..., y_s\}$ is system of parameters. $\Longrightarrow r + s = dim(\mathcal{A})$ and $(x_1, ..., x_r, y_1, ..., y_s)$ is $\mathfrak{m}$-primary. Then, as prove before, $(\overline{y}_1, ..., \overline{y}_s)$: $\overline{\mathfrak{m}}$-primary, we have $dim(\overline{\mathcal{A}}) \leq s = dim(\mathcal{A}) - r$, which indicates (ii).

Now check that (ii) implies (i).

If (ii) holds, with $s := \dim(\mathcal{A}) - r = \dim(\overline{\mathcal{A}})$, then $\exists y_1, ..., y_s \in \mathcal{A}$ s.t. $\{\overline{y}_1, ..., \overline{y}_s\}$ is a system of parameters of $\overline{\mathcal{A}}$. $\implies (\overline{y}_1, ..., \overline{y}_s)$ is $\overline{\mathfrak{m}}$-primary $\implies$ $(x_1, .., x_r, y_1, ..., y_s)$ is $\mathfrak{m}$-primary. Also, we know $\dim(\mathcal{A}) = r + s$, then by definition $(x_1, ..., x_r, y_1, ..., y_s)$ is a system of parameters of $\mathcal{A}$. □

Corollary 6.58. $(\mathcal{A}, \mathfrak{m})$, *Noetherian local,* $a \in \mathcal{A}$ *non-zerodivisor. Then:*

$$dim(\mathcal{A}/(a)) = dim(\mathcal{A}) - 1$$

Proof. Recall: $\text{ht}((a)) = 1$ by Krull principal ideal theorem 6.45.

By the above (6.57 (iii)implies (i) and (ii)), we may extend $\{a\}$ to a system of parameters $\{a_0, ..., a_n\}$, $a_0 = a$, with $\dim(\mathcal{A}) - 1 = \dim(\mathcal{A}/(a))$ □

6.7   Lecture 20-1. Dimension of Polynomial Rings, Regularity

Theorem 6.59. $\mathcal{A}$ *Noetherian* $\implies dim(\mathcal{A}[X_1, .., X_n]) = dim(\mathcal{A}) + n$

Proof. We may assume $n = 1$ (then iterate with $\mathcal{A}$ replaced by $\mathcal{A}[X_1], etc$)

Easy direction: $\dim(\mathcal{A}[X]) \geq \dim(\mathcal{A}) + 1$. Indeed, consider a chain $\mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_n$ in $\mathcal{A}$. Consider $\mathfrak{p}_0 \mathcal{A}[X] \subsetneq ... \subsetneq \mathfrak{p}_n \mathcal{A}[X] \subsetneq \mathfrak{p}_n \mathcal{A}[X] + X \mathcal{A}[X]$.

N.b. If $\mathfrak{p} \subsetneq \mathcal{A}$ is prime, then $\mathcal{A}[X]/\mathfrak{p}\mathcal{A}[X] \cong (\mathcal{A}/\mathfrak{p})[X]$ is a domain. so $\mathfrak{p}\mathcal{A}[X]$ is prime. And $\mathfrak{p}_n \mathcal{A}[X] + X \mathcal{A}[X]$ is prime because $\mathcal{A}[X]/(\mathfrak{p}_n \mathcal{A}[X] + X \mathcal{A}[X]) \cong \mathcal{A}/\mathfrak{p}_n$

Hard direction $\dim(\mathcal{A}[X]) \leq \dim(\mathcal{A}) - 1$. Consider $\mathfrak{p}_0 \subseteq ...$

Because $\dim(\mathcal{A}[X]) = \sup\{\text{ht}(\mathfrak{m}) : \mathfrak{m} \subseteq \mathcal{A}[X] \text{ maximal }\}$

So it suffices to show $\forall \mathfrak{m} \subseteq \mathcal{A}[X]$ that $\text{ht}(\mathfrak{m}) \leq r + 1$, where $r := \dim(\mathcal{A})$. May assume $r \leq \infty$.

Consider $\mathfrak{p} := \mathfrak{m} \cap \mathcal{A}$, it is a prime in $\mathcal{A}$ because $\mathfrak{p} := \mathfrak{m} \cap \mathcal{A} = \mathfrak{m}/(X)$ and also maximal. It suffices to show $\text{ht}(\mathfrak{m}) \leq \text{ht}(\mathfrak{p}) + 1$.

We localize at $\mathfrak{p}$. $S := S_\mathfrak{p} = \mathcal{A} - \mathfrak{p}$. $S^{-1}\mathcal{A} = \mathcal{A}_\mathfrak{p}$ is local with maximal ideal $\mathfrak{p}_\mathfrak{p}$. $S^{-1}(\mathcal{A}[X]) = (S^{-1}\mathcal{A})[X] = \mathcal{A}_\mathfrak{p}[X]$. $S^{-1}\mathfrak{m} \subseteq S^{-1}\mathcal{A}[X]$ remains a maximal ideal, and $\text{ht}(S^{-1}\mathfrak{m}) = \text{ht}(\mathfrak{m})$, because the localization with respect to S, preserves the primes and their inclusions for those ideals not intersecting S. And the problem reduce to the case of Noetherian local ring.

We now assume that $(\mathcal{A}, \mathfrak{p})$: Noetherian local ring, $\mathfrak{m} \subseteq \mathcal{A}[X]$ maximal, $\mathfrak{m} \cap \mathcal{A} = \mathfrak{p}$. $r = dim\mathcal{A} < \infty$.

<u>Want</u>: $\text{ht}(\mathfrak{m}) \leq r + 1$

It suffices by theorem 6.56 to construct $r + 1$ elements of $\mathcal{A}[X]$ that generate an ideal with radical $\mathfrak{m}$.

Know: $r = \dim(\mathcal{A}) = \operatorname{ht}(\mathfrak{p})$, so we can find $x_1, ..., x_r \in \mathcal{A}$ s.t. $\mathfrak{p}$ is the only prime of $\mathcal{A}$ containing $(x_1, ..., x_r)$ i.e., $\operatorname{rad}((x_1, ..., x_r)) = \mathfrak{p}$.

Consider

$$\mathcal{A}[X] \longrightarrow \mathcal{A}[X]/\mathfrak{p}\mathcal{A}[X] = (\mathcal{A}/\mathfrak{p})[X]$$

$$\mathfrak{m} \longmapsto \overline{\mathfrak{m}} \text{ maximal}$$

where $\mathfrak{m} \supseteq \mathfrak{p}\mathcal{A}[X]$ and $\mathcal{A}/\mathfrak{p}$ is a field, thus $\mathcal{A}/\mathfrak{p}[X]$ is a PID.

$\overline{\mathfrak{m}} = (\overline{f})$ for some $\overline{f} \in (\mathcal{A}/\mathfrak{p})[X]$. Say $\overline{f}$ is the image of $f \in \mathfrak{m}$.

Claim: $\mathfrak{m}$ is the only prime that contains $x_1, .., x_r, f$.

Indeed, assume $\mathfrak{q}$ a prime in $\mathcal{A}$ that contains $x_1, .., x_r, f \implies \mathfrak{q} \cap \mathcal{A}$ is a prime of $\mathcal{A}$ containing $x_1, .., x_r$, hence $\mathfrak{q} \cap \mathcal{A} = \mathfrak{p}$, so $\mathfrak{q} \supseteq \mathfrak{p}\mathcal{A}[X]$, so $\mathfrak{q}$ identifies with a prime ideal $\overline{\mathfrak{q}} \subseteq \mathcal{A}[X]/\mathfrak{p}\mathcal{A}[X]$ which contains $\overline{f}$, hence $\overline{\mathfrak{q}} = \overline{\mathfrak{m}}$, hence $\mathfrak{q} = \mathfrak{m}$. $\mathfrak{m} = \operatorname{rad}((x_1, ..., x_r, f))$.

$\square$

Example 6.60. *(All the bad examples in algebraic geometry is more or less related to this example) One other example: k is a field, $k[[X, Y]] := \{$formal power series over k in $X, Y\} = \{\sum_{ij} c_{ij} X^i Y^j\}$, $k[[X, Y]]$ is Noetherian, local ring with maximal ideal (X, Y)*

Assume $\mathcal{A} := k[[X, Y]]/(X^2, XY)$. what is $\dim(\mathcal{A})$?

$\mathcal{A}/(x) \cong k[[y]]$, $\mathcal{A}/(x, y) \cong k$ are integral domains $\implies (X) \subsetneq (X, Y)$ is a chain of prime, notice that $\mathcal{A}$ is not a integral domain $\implies \dim(\mathcal{A}) \geq 1$

$\mathcal{A} \supseteq \mathfrak{m} = (x, y)$ (x and y here means the image of x and y in the quotient ring.)

Claim $\operatorname{rad}((y)) = \mathfrak{m}$

Proof. $x^2 = 0 \in (y), y^1 \in (y) \to \mathfrak{m} \subseteq \operatorname{rad}((y))$, and by the fact that $\mathfrak{m}$ is maximal $\mathfrak{m} = \operatorname{rad}((y))$ $\square$

By the theorem on parameters, deduce that $\dim(\mathcal{A}) \leq 1$. hence $\dim(\mathcal{A}) = 1$.

Lemma 6.61. *$k = \overline{k}$ say $k = \mathbb{C}$. $\mathcal{A} = k[X_1, ..., X_n]$. Let $\mathfrak{m} \subseteq \mathcal{A}$ be a maximal ideal, then $\mathfrak{m} = (X_1 - x_1, ..., X_n - x_n)$ for some $(x_1, .., x_n) \in k^n$. Then $\operatorname{ht}(\mathfrak{m}) = n$, and $\mathcal{A}_\mathfrak{m}$ a local ring of dimension n whose maximal ideal $\mathfrak{m}\mathcal{A}_\mathfrak{m}$ has n generators.*

Proof. $\dim(\mathcal{A}_\mathfrak{m}) = \operatorname{ht}(\mathfrak{m}\mathcal{A}_\mathfrak{m}) = \operatorname{ht}(\mathfrak{m}) \leq \dim(\mathcal{A}) = n$. $\operatorname{ht}(\mathfrak{m}) \geq n$ because $\mathfrak{m} = \mathfrak{p}_n \supsetneq ... \supsetneq \mathfrak{p}_0$, $\mathfrak{p}_i = (X_1 - x_1, ..., X_i - x_i)$ $\square$

Lemma 6.62. *Now let $(\mathcal{A}, \mathfrak{m})$: Noetherian local of $d := \dim(\mathcal{A}) = \operatorname{ht}(\mathfrak{m})$ and we set $k = \mathcal{A}/\mathfrak{m}$.*

(a) *In general , $d \leq dim_k(\mathfrak{m}/\mathfrak{m}^2)$ (The later is a k-vector space because M and A-module $\implies M/\mathfrak{m}M$ is a k-vector space.)*

(b) *The following are equivalent:*

  (i) *$\mathfrak{m}$ admits a set of d generator: $\mathfrak{m} = (x_1, .., x_d)$*

  (ii) *$d = dim_k(\mathfrak{m}/\mathfrak{m}^2)$*

  *And if these hold, we call $(\mathcal{A}, \mathfrak{m})$ is **regular***

Example 6.63. *$(k[x_1, .., x_n], \mathfrak{m})$ is regular.*

Proof.

(a) Set $n := dim_k(\mathfrak{m}/\mathfrak{m}^2)$. Choose $x_1, .., x_n \in \mathfrak{m}$ s.t. $\bar{x}_1, ..., \bar{x}_n \in \mathfrak{m}/\mathfrak{m}^2$ form a basis.

 By Nakayama Lemma $\implies \mathfrak{m} = (x_1, ..., x_n) \implies d \leq n$ by Krull dimension theorem.

(b) $(i) \implies (ii)$
 $\mathfrak{m} = (x_1, ..., x_d) \implies \mathfrak{m}/\mathfrak{m}^2$ is spannd by $\bar{x}_1, ..., \bar{x}_d$, so $dim_k(\mathfrak{m}/\mathfrak{m}^2) \leq d$. Combine with (a) to get (ii).

 $(ii) \implies (i)$ Same proof as (a)

$\square$

7   Integral Extension of Rings

We will cover the contents of §5 of A-M and §3 pf Bosch
   Motivation: to show that $\dim(\mathcal{A}) = tr.deg_k(Frac(\mathcal{A}))$, $\forall \mathcal{A}$ integral domain that is finitely generated as an algebra over some field $k \subseteq \mathcal{A}$.
   For example: $\mathcal{A} = k[x_1, .., x_n]$
   <u>Want</u>: Machinery for comparing a general ring $\mathcal{A}$ as above to this example.

7.1   Lecture 20-2. Integral Element

Consider a monic polynomial equation with coefficients in $\mathcal{A}$:

$$x^n + a_1 x^{n-1} + ... + a_n = 0 \tag{*}$$

Definition 7.1. *Let $\mathcal{A} \subseteq \mathcal{B}$ be rings. Say that $x \in \mathcal{B}$ is **integral over** $\mathcal{A}$ if $\exists n \geq 1, a_1, .., a_n \in \mathcal{A}$ s.t. the above Equation(*) holds.*

*And we say that $\mathcal{B}$ is **integral over** $\mathcal{A}$ if each $x \in \mathcal{B}$ is integral over $\mathcal{A}$.*

A non-obvious fact: $x, y \in \mathcal{B}$ integral over $\mathcal{A}$, then $x \pm y, xy$ are integral over $\mathcal{A}$ (The elements in $\mathcal{B}$ integral over $\mathcal{A}$ form a ring)

Lemma 7.2. *$\mathcal{A} \subseteq \mathcal{B}$ are rings. The followings are equivalent for $x \in \mathcal{B}$.*

i). *x is integral over $\mathcal{A}$*

ii). *$\mathcal{A}[x]$ is finite over $\mathcal{A}$, i.e., $\mathcal{A}[x]$ is a finitely generated $\mathcal{A}$-module: $\exists e_1, .., e_n \in \mathcal{A}[x], s.t. \mathcal{A}[x] = \sum_i \mathcal{A} e_i$*

iii). *$\exists$ subring $\mathcal{A}[x] \subseteq \mathcal{C} \subseteq \mathcal{B}$ s.t. $\mathcal{C}$ finitely generated $\mathcal{A}$-module.*

iv). *$\exists$ faithful $\mathcal{A}[x]$-module M which is finitely generated as an $\mathcal{A}$-module. (Here by faithful, we mean the only element $y \in \mathcal{A}[x], y \cdot m = 0, \forall m \in M \implies y = 0$)*

Example 7.3. *$\frac{1}{2} \in \mathbb{Q}$ is not integral over $\mathbb{Z}$, $\mathbb{Z}[\frac{1}{2}]$ not a finitely generated $\mathbb{Z}$-module. It equals to $\sum_{n=0}^{\infty} 2^{-n} \mathbb{Z}$.*

Proof. $(i) \implies (ii)$ If x satisfies $x^n + a_1 x^{n-1} + ... + a_n = 0$, then $\mathcal{A}[x] = \sum_{i=0}^{n-1} \mathcal{A} x^i \ni x^n = -(a_1 x^{n-1} + ... + a_n) \implies x^{n+1} = -a_1 x^n - (a_2 x^{n-1} + ... + a_n x)$. By induction, we know $\mathcal{A}[x]$ is a finitely generated $\mathcal{A}$-module.

$(ii) \implies (iii)$ $\mathcal{C} := \mathcal{A}[x]$,

$(iii) \implies (iv)$ $M := \mathcal{C}$

$(iv) \implies (i)$ Suppose a finitely generated $\mathcal{A}$-module M which is simultaneously a faithful $\mathcal{A}[x]$-module. $M = \sum_i^n \mathcal{A} e_i, e_i \in M$. Because M is a $\mathcal{A}[x]$-module, we can apply the action of x on each e_i and get a system of linear equations:

$$x \cdot e_1 = a_{11} e_1 + ... + a_{1n} e_n$$
$$\vdots$$
$$x \cdot e_n = a_{n1} e_1 + ... + a_{nn} e_n$$

with coefficients $a_{ij} \in \mathcal{A}$. In terms of matrices, we can write

$$\Delta \cdot \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = 0,$$

where $\Delta = (\delta_{ij}x - a_{ij}) \in (\mathcal{A}[x])^{n \times n}$. Now consider the Cramer's rule in linear algebra:

$$\Delta^{ad} \cdot \Delta = (det\Delta) \cdot Id,$$

we have the following equality

$$\det \Delta \cdot \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = 0,$$

hence $\det \Delta m = 0$, $\forall m \in M$, by the assumption in (iv), M is a faithful $\mathcal{A}[x]$-module $\implies \det \Delta = 0$. Therefore x satisfies the following monic polynomial equation

$$\det(\delta_{ij}X - a_{ij}) = 0$$

as desired.

$\square$

7.2 Lecture 21. Normal Domain

Last time we proved Lemma 7.2, many corollary can be derived form it.

Lemma 7.4. $\mathcal{A} \subseteq \mathcal{B} \subseteq \mathcal{C}$, $x \in \mathcal{C}$. Then:

$$[x \text{ integral over } \mathcal{A}] \implies [x \text{ integral over } \mathcal{B}]$$

Lemma 7.5. $\mathcal{A} \subseteq \mathcal{B} \subseteq \mathcal{C}$ are rings. If $\mathcal{C}$ finite over $\mathcal{B}$ and $\mathcal{B}$ finite over $\mathcal{A}$, then $\mathcal{C}$ is finite over $\mathcal{A}$. This can proved trivially by flattening the definition.

Proof. $\mathcal{C} = \sum_{i=1,..,m} \mathcal{B}y_i$ and $\mathcal{B} = \sum_{j=1,..,n} \mathcal{A}x_j \implies$

$$\mathcal{C} = \sum_{i,j} \mathcal{A}x_jy_i, \quad x_j \in \mathcal{B}, y_i \in \mathcal{C} \implies x_jy_i \in \mathcal{C}.$$

$\square$

Lemma 7.6. *Suppose* $\mathcal{A} \subseteq \mathcal{B}$ *rings,* $x_1,..,x_n \in \mathcal{B}$ *integral over* $\mathcal{A}$. *Then*

(i) $\mathcal{A}[x_1,..,x_n]$ *is finite over* $\mathcal{A}$

(ii) $\mathcal{A}[x_1,..,x_n]$ *is integral over* $\mathcal{A}$

Notice here $\mathcal{A}[x_1,...,x_2]$ does not mean the polynomial ring but some ring generated by replacing the indeterminates X_i by the corresponding element x_i in $\mathcal{B}$

Proof. In fact, (i) implies (ii). By Lemma 7.2 part iii). because $\forall x \in \mathcal{A}[x_1, ..., x_n]$, $\mathcal{A}[x] \subseteq \mathcal{C} \subseteq \mathcal{A}[x_1, ..., x_n]$ where $\mathcal{C} = \mathcal{A}[x_1, ..., x_n]$ and $\mathcal{C}$ is finite over $\mathcal{A}$.

Now we prove (i). Induct on n. $n = 1$ apply Lemma 7.2 part ii)., done. For $n \geq 2$, consider the inclusion $\mathcal{A}[x_1, ..., x_{n-1}] \subseteq \mathcal{A}[x_1, ..., x_{n-1}][x_n] \subset \mathcal{A}[x_1, ..., x_n]$, where $\mathcal{A}[x_1, ..., x_{n-1}][x_n]$ is finite over $\mathcal{A}[x_1, .., x_{n-1}]$ and then apply Lemma 7.5, done. $\qquad\square$

Lemma 7.7. $\mathcal{A} \subseteq \mathcal{B}$. *The following are equivalent:*

(i) $\mathcal{B}$ *is integral over* $\mathcal{A}$ *and finitely generated as an* $\mathcal{A}$*-algebra.*

(ii) $\mathcal{B}$ *is finite over* $\mathcal{A}$ *(i.e., finitely generated as an* $\mathcal{A}$*-module).*

Proof. "$(i) \Longrightarrow (ii)$":$\mathcal{B}$ is finitely generated $\mathcal{A}$-algebra, then $\mathcal{B} = \mathcal{A}[x_1, .., x_n]$, $\Longrightarrow($ each x_j is integral over $\mathcal{A}$, and $\mathcal{B} = \mathcal{A}[x_1, ..., x_n]$ is finite over $\mathcal{A}$ by Lemma 7.6

"$(ii) \Longrightarrow (i)$": $\mathcal{B}$ is finite over $\mathcal{A}$ automatically means $\mathcal{B}$ is finitely generated $\mathcal{A}$-algebra. By Lemma 7.2, part iii). $\Longrightarrow i$)., $\forall x \in \mathcal{B}, \mathcal{A}[x] \subseteq \mathcal{B} \subseteq \mathcal{B}$, where $\mathcal{B}$ is itself finitely generated $\mathcal{A}$-module, then we know x is integral over $\mathcal{A}$. $\qquad\square$

Lemma 7.8. $\mathcal{A} \subseteq \mathcal{B}$ *are rings. Then* $\overline{\mathcal{A}} := \{x \in \mathcal{B} | x \text{ integral over } \mathcal{A}\}$ *is an* $\mathcal{A}$*-subalgebra of* $\mathcal{B}$.

Proof. If $x, y \in \mathcal{B}$ are integral over $\mathcal{A}$. then by Lemma 7.6, $\mathcal{A}[x, y]$ is finite over $\mathcal{A}$ $\Longrightarrow \mathcal{A}[x, y]$ is integral over $\mathcal{A}$. so $xy, a_1 x + a_2 y \in \mathcal{A}[x, y], \forall a_1, a_2 \in \mathcal{A}$ are integral over $\mathcal{A}$. $\qquad\square$

Lemma 7.9. $\mathcal{A} \subseteq \mathcal{B} \subseteq \mathcal{C}$ *where* $\mathcal{B}$ *is integral over* $\mathcal{A}$, *and* $\mathcal{C}$ *is integral over* $\mathcal{B}$, $\Longrightarrow \mathcal{C}$ *is integral over* $\mathcal{A}$.

Proof. Let $x \in \mathcal{C}$. Write

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

Set $\mathcal{B}_0 := \mathcal{A}[b_1, ..., b_n]$. Then by some Lemma 7.6 above, we know $\mathcal{B}_0$ is finite and integral over $\mathcal{A}$, and "x integral over $\mathcal{B}_0$" $\Longrightarrow$ "$\mathcal{B}_0[x]$ finite over $\mathcal{B}_0$".

Then we know "$\mathcal{B}_0$ is finite over $\mathcal{A}$", and "$\mathcal{B}_0[x]$ is finite over $\mathcal{B}_0$", then by Lemma 7.4 above, we know $\mathcal{B}_0[x]$ is finite over $\mathcal{A}$. Then by Lemma 7.2 part iii), $\mathcal{A}[x] \subseteq \mathcal{B}_0[x] \subseteq \mathcal{C}$ and $\mathcal{B}_0[x]$ is finite over $\mathcal{A} \Longrightarrow x$ is integral over $\mathcal{A}$. $\qquad\square$

Definition 7.10. $\mathcal{A} \subseteq \mathcal{B}$ *rings,* $\overline{\mathcal{A}} := \{x \in \mathcal{B} | x \text{ integral over } \mathcal{A}\} =:$ *" the **integral closure of** $\mathcal{A}$ **in** $\mathcal{B}$". We call $\mathcal{A}$ is **integrally closed in** $\mathcal{B}$ if $\overline{\mathcal{A}} = \mathcal{A}$.*

Corollary 7.11. $\overline{\mathcal{A}}$ *is integrally closed in* $\mathcal{B}$: $\overline{\overline{\mathcal{A}}} = \overline{\mathcal{A}}$, *"integral closures are integrally closed"*

Proof. Suppose $x \in \mathcal{B}$ is integral over $\overline{\mathcal{A}}$. Since by definition, $\overline{\mathcal{A}}$ is integral over $\mathcal{A}$. Then by Lemma 7.9, x is integral over $\mathcal{A} \Longrightarrow x \in \overline{\mathcal{A}} \Longrightarrow \overline{\overline{\mathcal{A}}} = \overline{\mathcal{A}}$. $\qquad\square$

Lemma 7.12. *(Lemma 9)*
$\mathcal{A} \subseteq \mathcal{B}$ *rings,* $\mathfrak{b} \subseteq \mathcal{B}$ *an ideal, and set* $\mathfrak{a} := \mathcal{A} \cap \mathfrak{b}$. *If* $\mathcal{B}$ *is integral over* $\mathcal{A}$, *then* $\mathcal{B}/\mathfrak{b}$ *is integral over* $\mathcal{A}/\mathfrak{a}$.

Proof. Let $x + \mathfrak{b} \in \mathcal{B}/\mathfrak{b}$. Write $x^n + ... = 0$ with coefficients in $\mathcal{A}$, and then reduce to the conclusion by $\mod \mathfrak{b}$. $\qquad\square$

Lemma 7.13. *(Lemma 10) Let* $\mathcal{A} \subseteq \mathcal{B}$ *are rings, and multiplicative set* $S \subseteq \mathcal{A}$. *Then* $\mathcal{A}$, *then* $S^{-1}\mathcal{B}$ *is integral over* $S^{-1}\mathcal{A}$.

Proof. Let $\frac{x}{s} \in S^{-1}\mathcal{B}$, $x \in \mathcal{B}, s \in S$. Indeed

$$x^n + a_1 x^{n-1} + ... + a_n = 0$$

implies

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

which means $\frac{x}{s}$ is integral over $S^{-1}\mathcal{A}$. $\qquad\square$

Definition 7.14. *Let* $\mathcal{A}$ *a domain (:= integral domain). set* $K := Frac(\mathcal{A})$ *field of fractions. Call* $\mathcal{A}$ **normal** *if* $\mathcal{A}$ *is integrally closed in* K, *i.e.,* $x \in K$, *integral over* $\mathcal{A} \Longrightarrow x \in \mathcal{A}$. *Note in some references e.g., Atiyah-Macdonald "normal" is equivalent to "integrally closed"*

Lemma 7.15. *(Lemma 11)* $\mathbb{Z}$ *is normal.*

Proof. Let $x \in \mathbb{Q}^{\times}$, say $x = r/s$, $gcd(x, s) = 1$, $r, s \in \mathbb{Z}, s \neq 0$. Suppose $\exists a_1, .., a_n \in \mathbb{Z}$ s.t.,
$$x^n + a_1 x^{n-1} + ... + a_n = 0.$$
Then after multiplying it by s^n, set

$$r^n = -(a_1 r^{n-1} s + a_2 r^{n-2} s^2 + ... + a_n s^n)$$

$\Longrightarrow s | r^n$, $gcd(r^n, s) = 1, \Longrightarrow s \in \mathbb{Z}^{\times} \Longrightarrow x \in \mathbb{Z}$. $\qquad\square$

Lemma 7.16. *(Lemma11') Any UFD (unique factorization domain) is normal (via the same proof): e.g.* $\mathbb{Z}, k[x_1, ..., x_n]$

Consider an example of ring which is not normal:

Example 7.17. $\mathcal{A} = k[x^2, x^3] \subset K = Frac(\mathcal{A}) = k(x), (because\ x^3/x^2)$ *is not normal.*

The element $x \in K$ *is integral over* $\mathcal{A}$, *but not in* $\mathcal{A}$.

Similarly, $k[x(x-1), x^2(x-1)]$ *is not normal.*

Proposition 7.18. $\mathcal{A}$ *is a domain.* $K := Frac(\mathcal{A})$. L/K *is an algebraic field extension. Suppose* $\mathcal{B} :=$*integral closure of* $\mathcal{A}$ *in* L. *Then* $\mathcal{B}$ *is normal.*

Proof. Integral closure $\mathcal{B}$ is a subring of a field L, thus it is a integral domain.

Check that $Frac(\mathcal{B}) = L$: By definition, $\mathcal{B}$ is a the set of integral element of L over $\mathcal{A}$, then $Frac(\mathcal{B}) \subseteq L$. For the converse inclusion, $x \in L$, L is an algebraic field extension of K, then x satisfies some polynomial equation with coefficients in K.

$$x^n + k_1 x^{n-1} + ... + k_n = 0$$

each k_i can be written as a_i/s_i where $s_i \in \mathcal{A}^{\times}$, multiply the above equation by s^n, where $s := \prod_i s_i \in \mathcal{A} \in \mathcal{B}$, then we get

$$(sx)^n + (a_1 s_2 ... s_n)(sx)^{n-1} + ... = 0,$$

which means $sx \in \overline{\mathcal{A}} = \mathcal{B} \implies x \in Frac(\mathcal{B})$. This proof in fact says each element $x \in L$ can be written as $\frac{b}{a}$, $b \in \mathcal{B}, a \in \mathcal{A}^{\times}$. $\square$

Example 7.19. $\mathcal{A} = \mathbb{Z}, K = \mathbb{Q}$, L/K *is finite extension (*L *is a number field.)* $\mathcal{B}$ *is the integral closure of* $\mathcal{A}$ *in* L.

$\mathcal{B} =: \mathcal{O}_L$ *"ring of integers in* L*".*

Example 7.20. $\mathcal{A} = \mathbb{Z}[\sqrt{3}], L = \mathbb{Q}(\sqrt{3})$, *FACT:* $\mathcal{O}_L = [(1 + \sqrt{3})/2] \supsetneq \mathbb{Z}[\sqrt{3}]$

$\mathbb{Z}[\sqrt{3}]$ *is not normal.*

Definition 7.21. $\mathcal{A}$ *is a domain,* $\mathcal{A}^{norm} :=$ *"integral closure of* $\mathcal{A}$ *in the faction field* $K = Frac(\mathcal{A})$*" is called the* **normalization** *of* $\mathcal{A}$. *It is normal by Prop 7.18. Examples include*

$$k[X^2, X^3]^{norm} = k[X]$$

$$\mathbb{Z}[\sqrt{3}]^{norm} = \mathbb{Z}\left[\frac{1 + \sqrt{3}}{2}\right]$$

Lemma 7.22. *(Lemma 12)* $\mathcal{A} \subseteq \mathcal{B}$, *integral extension of rings.*

    (i) ($\mathcal{A}$ is a field $\iff$ $\mathcal{B}$ is a field) provided that $\mathcal{A}$ and $\mathcal{B}$ are domains

    (ii) Let $\mathfrak{q} \subseteq \mathcal{B}$ prime, and $\mathfrak{p} := \mathfrak{q}^c = \mathfrak{q} \cap \mathcal{A}$. prime (in $\mathcal{A}$). Then $\mathfrak{q}$ maximal $\iff$ $\mathfrak{p}$ maximal.

Proof. (i) "$\implies$", Let $x \in \mathcal{B} - \{0\}$. Write $x^n + a_1 x^{n-1} + ... + a_n = 0$ with $a_i \in \mathcal{A}$ and n minimal. Then $a_n \neq 0$, because otherwise we could cancel a factor of $x \neq 0$ to reduce n.

    Then $x^{n-1} + a_1 x^{n-2} + ... + a_n/x = 0$ in $Frac(\mathcal{B})$. Then $\frac{1}{x} = -(x^{n-1} + a_1 x^{n-2} + ...)/a_n \in \mathcal{B}$ (because $\mathcal{A}$ is a field $a_n \in \mathcal{A}^\times$).

    "$\impliedby$", $\mathcal{B}$ is field, $x \in \mathcal{A} - \{0\} \subseteq \mathcal{B} - \{0\}$, $1/x \in \mathcal{B}$ is integral over $\mathcal{A}$

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

with $a_i \in \mathcal{A}$ and n minimal. Multiply by x^{n-1},

$$\frac{1}{x} = -(a_1 + ... + a_n x^{n-1}) \in \mathcal{A}$$

$\implies \mathcal{A}$ is a field.

    (ii): $\mathcal{B}/\mathfrak{q}$ is integral over $\mathcal{A}/\mathfrak{p}$ by Lemma 7.12 and then apply part (i).

$\square$

7.3   Lecture 22. Going-Up

Corollary 7.23. *If $(\mathcal{A}, \mathfrak{m})$: local ring and $\mathcal{A} \subseteq \mathcal{B}$: integral extension, then*

$$\{primes \ \mathfrak{q} \ of \ \mathcal{B} \ with \ \mathfrak{q} \cap \mathcal{A} = \mathfrak{m}\} = \{maximal \ ideals \ in \ \mathcal{B}\}$$

Proof. $\subseteq$: $\mathfrak{q} \cap \mathcal{A}$: maximal $\implies \mathfrak{q}$ maximal by Lemma 7.22.

    $\supseteq$: $\mathfrak{q}$ maximal implies by Lemma 7.22. $\mathfrak{q} \cap \mathcal{A}$ maximal, $\mathfrak{q} \cap \mathcal{A} = \mathfrak{m}$. $\square$

Definition 7.24. $\mathcal{A} \subseteq \mathcal{B}$, *integral extensions*, $\mathfrak{q} \in Spec(\mathcal{B})$ ***lies over*** $\mathfrak{p} \in Spec(\mathcal{A})$ *iff $\mathfrak{q} \cap \mathcal{A} = \mathfrak{p}$.*

Theorem 7.25. *Let $\mathcal{A} \subseteq \mathcal{B}$ integral extensions:*

    (i) (Maximality) Let $\mathfrak{q} \subseteq \mathcal{B}$ prime, and $\mathfrak{p} := \mathfrak{q}^c = \mathfrak{q} \cap \mathcal{A}$. prime (in $\mathcal{A}$). Then $\mathfrak{q}$ maximal $\iff$ $\mathfrak{p}$ maximal. This has been proved in Lemma 7.22, but we put it here for consistency.

(ii) *(Lying-Over): Every prime* $\mathfrak{p} \subset \mathcal{A}$ *has some prime* $\mathfrak{q} \subseteq \mathcal{B}$ *lying over it.*
   (equivalently, then map $Spec(\mathcal{B}) \longrightarrow Spec(\mathcal{A})$: $\mathfrak{q} \mapsto \mathfrak{q} \cap \mathcal{A}$ is surjective.)

(iii) *(Incomparablity) The primes lying over a given prime satisfy no inclusion relations, i.e.,*

$$\left.\begin{array}{l} \mathfrak{q}, \mathfrak{q}' \in Spec(\mathcal{B}) \\ \mathfrak{q} \supseteq \mathfrak{q}', \mathfrak{q} \cap \mathcal{A} = \mathfrak{q}' \cap \mathcal{A} \end{array}\right\} \Longrightarrow \mathfrak{q} = \mathfrak{q}'.$$

Equivalently, if $\mathfrak{q} \supsetneq \mathfrak{q}'$ *(primes in $\mathcal{B}$), then* $\mathfrak{q} \cap \mathcal{A} \supsetneq \mathfrak{q}' \cap \mathcal{A}$*. The direction* $\mathfrak{q} \cap \mathcal{A} \supsetneq \mathfrak{q}' \cap \mathcal{A} \Longrightarrow \mathfrak{q} \supsetneq \mathfrak{q}'$ *holds automatically, we have* $\mathfrak{q} \cap \mathcal{A} \supsetneq \mathfrak{q}' \cap \mathcal{A} \Longleftrightarrow \mathfrak{q} \supsetneq \mathfrak{q}'$.

(iv) *(Going-Up) For all* $\mathfrak{p}, \mathfrak{p}' \in Spec(\mathcal{A}), \mathfrak{q} \in Spec(\mathcal{B})$ *s.t.* $\mathfrak{p} \subseteq \mathfrak{p}', \mathfrak{q} \cap \mathcal{A} = \mathfrak{p}$,
   $\exists \mathfrak{q}' \in Spec(\mathcal{B})$ *s.t.* $\mathfrak{q}' \supseteq \mathfrak{q}, \mathfrak{q}' \cap \mathcal{A} = \mathfrak{p}'$ *Equivalently, if we start with a chain* $\mathfrak{p} = \mathfrak{p}_1 \subseteq .... \subseteq \mathfrak{p}_n \in Spec(\mathcal{A})$ *and a prime* $\mathfrak{q}$ *lying over* $\mathfrak{p}$*, then there exists a chain* $\mathfrak{q} = \mathfrak{q}_1 \subseteq ... \subseteq \mathfrak{q}_n \in Spec(\mathcal{B})$*, s.t.,* $\mathfrak{q}_i \cap \mathcal{A} = \mathfrak{p}_i$*. Moreover, by "Incomparablity", if* $\mathfrak{p} \subsetneq \mathfrak{p}'$*, then* $\mathfrak{q} \subsetneq \mathfrak{q}'$.

Equivalently,

Corollary 7.26. $\mathcal{A} \subseteq \mathcal{B}$ *integral extension,* $\mathfrak{b} \subseteq \mathcal{B}$ *ideal,* $\mathfrak{a} := \mathfrak{b} \cap \mathcal{A}$

(i) $dim(\mathcal{A}) = dim(\mathcal{B})$

(ii) $dim(\mathcal{A}/\mathfrak{a}) = dim(\mathcal{B}/\mathfrak{b})$, *i.e.* $coht(\mathfrak{a}) = coht(\mathfrak{b})$.

(iii) $ht(\mathfrak{b}) \leq ht(\mathfrak{a})$.

Proof.
$(i)\checkmark$. In general ring morphism, for each (strictly inclusion) chain in $\mathcal{B}$, there exists a (possibly not strictly inclusion) chain in $\mathcal{A}$. In the case of integral extension, the incomparability alone guarantees the strict inclusion of the chain in $\mathcal{A}$. We know $\dim(\mathcal{A}) \geq \dim(\mathcal{B})$. In return, the Going-Up+Incomparability guarantee $\dim(\mathcal{A}) \leq \dim(\mathcal{B})$
$(ii)\checkmark$. By Lemma 7.12, $\mathcal{B}/\mathfrak{b}$ is integral over $\mathcal{B}/\mathfrak{b}$ and (ii) reduce to (i).
(iii). For primes $\mathfrak{q} \subsetneq \mathcal{B}$ $\mathfrak{p} \subseteq \mathcal{A}$ s.t. $\mathfrak{q}$ lies over $\mathfrak{q}$, we have $ht(\mathfrak{p}) \geq ht(\mathfrak{q})$ because for each proper including chain of primes that ends with$\mathfrak{q} \subseteq \mathcal{B}$, there exists a proper including chain of primes ending with $\mathfrak{q} \subseteq \mathcal{A}$, where the proper inclusion is guaranteed by Incomparability. (We can not use Going-Up to argue $ht(\mathfrak{p}) \leq ht(\mathfrak{q})$).
   $ht(\mathfrak{b}) \leq ht(\mathfrak{a}) := \inf_{\mathfrak{p} \supseteq \mathfrak{a}} ht(\mathfrak{p})$ and $ht(\mathfrak{p}) := \sup\{t | \exists \mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_t = \mathfrak{p}\}$.

<u>Want</u>: if $\mathfrak{p} \supseteq \mathfrak{a}$, then $\mathrm{ht}(\mathfrak{p}) \geq \mathrm{ht}(\mathfrak{b})$.

Given a prime $\mathfrak{p} \supseteq \mathfrak{a}$, then by Lying-Over, $\exists$ prime $\mathfrak{q} \in \mathcal{B}$ s.t. $\mathfrak{q} \cap \mathcal{A} = \mathfrak{p}$. We may assume that $\mathfrak{p} \supseteq \mathfrak{a}$ is minimal, then by Incomparability $\mathfrak{q} \supseteq \mathfrak{b}$ is minimal.

$$\mathrm{ht}(\mathfrak{p}) \geq \mathrm{ht}(\mathfrak{q}) \geq \mathrm{ht}(\mathfrak{b})$$

$\square$

Proof. (of Theorem 7.25) the initial proof of Lying-Over in lecture used the term :"Let $\mathfrak{p} \in \mathrm{Spec}(\mathcal{A})$. $\mathcal{A}_\mathfrak{p} \subseteq \mathcal{B}_\mathfrak{p}$ integral extension". Here the $\mathfrak{p}$ is not necessarily prime in $\mathcal{B}$, hence the notion $\mathcal{B}_\mathfrak{p}$ should be replaced by $\varphi(S)^{-1}\mathcal{B}$ where $S := \mathcal{A} - \mathfrak{p}$ and φ is the inclusion map: $\mathcal{A} \hookrightarrow \mathcal{B}$.

Lying-Over:

$$
\begin{array}{ccccccc}
\mathfrak{n} \cap \mathcal{B} =: \mathfrak{q} & \subseteq & \mathcal{B} & \longhookrightarrow & \varphi(S)^{-1}\mathcal{B} & \supseteq & \exists \mathfrak{n} \text{ maximal} \\
\big\uparrow & & \big\uparrow & & \big\uparrow & & \big\uparrow \\
\mathfrak{m} \cap \mathcal{A} =: \mathfrak{p} & \subseteq & \mathcal{A} & \longhookrightarrow & S^{-1}\mathcal{A} & \supseteq & \mathfrak{m} \text{ maximal}
\end{array}
$$

$\mathfrak{q} := \mathfrak{n} \cap \mathcal{B}$ lies over $\mathfrak{p}$ because

$$(\mathfrak{n} \cap \mathcal{B}) \cap \mathcal{A} = (\mathfrak{n} \cap \varphi(S)^{-1}\mathcal{B}) \cap \mathcal{A} = \mathfrak{m} \cap \mathcal{A} = \mathfrak{p}$$

Incomparability: The construction above gives a bijection between

$$\{\text{primes of } \mathcal{B} \text{ lying over } \mathfrak{p}\} \longleftrightarrow \{\text{primes of } \varphi(S)^{-1}\mathcal{B} \text{ lying over } \mathfrak{m} = S^{-1}\mathfrak{p}\}$$

and by Lemma 7.22, the later can be identified as

$$\{ \text{ maximal ideals in } \varphi(S)^{-1}\mathcal{B} \text{ that lies over } \mathfrak{m}\},$$

which is always incomparable.

Going up:

$$
\begin{array}{ccccc}
\mathfrak{q} & \subseteq & \exists?\mathfrak{q}' & \subseteq & \mathcal{B} \\
\big| & & \big| & & \big\uparrow \\
\mathfrak{p} & \subseteq & \mathfrak{p}' & \subseteq & \mathcal{A}
\end{array}
$$

Consider the prime $\mathfrak{p}'/\mathfrak{p} \subset \mathcal{A}/\mathfrak{p} \subseteq \mathcal{B}/\mathfrak{q}$, where the second inclusion is integral extension. By lying over, we can find a prime $Q \subseteq \mathcal{B}/\mathfrak{q}$ lying over $\mathfrak{p}'/\mathfrak{p}$. Then $Q = \mathfrak{q}'/\mathfrak{q}$ for some $\mathfrak{q}' \in \mathrm{Spec}(\mathcal{B})$

$$\mathfrak{p}'/\mathfrak{p} = (\mathfrak{q}'/\mathfrak{q}) \cap (\mathcal{A}/\mathfrak{p}) = \frac{\mathfrak{q}' \cap \mathcal{A}}{\mathfrak{q} \cap \mathcal{A}} = \frac{\mathfrak{q}' \cap \mathcal{A}}{\mathfrak{q}} \implies \mathfrak{p}' = \mathfrak{q}' \cap \mathcal{A}$$

Then $\mathfrak{q}'$ lies over $\mathfrak{p}'$. $\square$

7.4   Lecture 23. Galois Transitivity and Going-Down

In order to prove the Going-Down theorem, we digress for a while to discuss some facts in field theory.

Definition 7.27. *A **normal** extension L/K of fields, is an extension s.t., each irreducible $f \in K[X]$ that has ≥ 1 root in L splits completely in L. (In other words, L/K is a union of "splitting fields")*

Definition 7.28. *L/K is **Galois** if it is normal and separable*

Definition 7.29. *L/K is **separable** if each $\alpha \in L$ is separable over K. i.e.,*

$$\#Hom_K(K(\alpha), \overline{K}) = dim_K K(\alpha),$$

("$\leq$" holds in general)

   $\alpha \in L$ separable over K is equivalent to "the minimal polynomial $f \in K[X]$ for α $(f(\alpha) = 0, deg(f)$minimal) has no repeated roots."
   N.b. $char(K) = 0 \implies$ every extension is separable.

Example 7.30. *$K = \mathbb{F}_p(t)$, $L := K(t^{1/p^n})$ is not separable. In fact, it is purely inseparable:*
$$\#Hom_K(K(\alpha), \overline{K}) = 1 \ \forall \alpha \in L$$

<u>*FACT*</u>: *let L/K be a normal extension. Let $G := Aut(L/K), L^G := \{\alpha \in L : g(\alpha) = \alpha \forall g \in G\}$*

$$\overbrace{K \subseteq \underbrace{L^G \subseteq L}_{Galois}}^{purely\ insep}.$$

See GTM 211 for details.

Theorem 7.31. *Let $\mathcal{A}$: normal domain, $K := Frac(\mathcal{A})$. Let L/K: normal extension of fields. Let $\mathcal{B} :=$ integral closure of $\mathcal{A}$ in L. Then $G := Aut(L/K)$ acts transitively on the primes of $\mathcal{B}$ lying over a given prime of $\mathcal{A}$:*

   (i) *For each $g \in G$, the restriction of g to $\mathcal{B}$ induces a ring automorphism $g : \mathcal{B} \xrightarrow{\sim} \mathcal{B}$*

  (ii) *$\forall g \in G, \mathfrak{q} \in Spec(\mathcal{B}) \implies g(\mathfrak{q}) \in Spec(\mathcal{B})$ and $\mathfrak{q} \cap \mathcal{A} = g(\mathfrak{q}) \cap \mathcal{A}$.*

 (iii) *$\forall \mathfrak{q}, \mathfrak{q}' \in Spec(\mathcal{B})$ with $\mathfrak{q} \cap \mathcal{A} = \mathfrak{q}' \cap \mathcal{A}$, $\exists g \in G$, s.t. $g(\mathfrak{q}) = \mathfrak{q}'$:*

Proof.

(i) Let $x \in \mathcal{B}$, $g \in G$
   Want: $g(x) \in \mathcal{B}$:
   Indeed, write
   $$x^n + a_1 x^{n-1} + ... + a_n = 0, \ a_i \in \mathcal{A},$$
   then
   $$\begin{aligned}
   0 &= g(x^n + a_1 x^{n-1} + ... + a_n) \\
   &= g(x)^n + g(a_1)g(x)^{n-1} + .. + g(a_n) \\
   &= g(x)^n + a_1 g(x)^{n-1} + ... + a_n \quad (g \text{ fixes } K \supseteq \mathcal{A})
   \end{aligned}$$
   $\implies g(x) \in \mathcal{B}.$

   We have shown that $g \in Aut(L/K)$ satisfies $g(\mathcal{B}) \subset \mathcal{B} \forall g \in\in G$. True also for g^{-1}. Then we know after restricting to $\mathcal{B}$ $g \circ g^{-1}$ and $g^{-1} \circ g$ are also identities. $Aut(L/K)$ restricts to a group of ring automorphism.

(ii) Let $g \in G$, $\mathfrak{q} \in \text{Spec}(\mathcal{B})$. g restrict to a ring morphism then $g(\mathfrak{q}) = (g^{-1})^{-1}(\mathfrak{q})$ always prime $g(\mathfrak{q}) \in \mathcal{B}$. Also $\mathfrak{q} \cap \mathcal{A} = g(\mathfrak{q} \cap \mathcal{A}) = g(\mathfrak{q}) \cap g(\mathcal{A}) = g(\mathfrak{q}) \cap \mathcal{A}$ because g fixes $\mathcal{A}$.

(iii) (a) Assume first that L/K finite, then $\#G < \infty$. Let $\mathfrak{q}, \mathfrak{q}' \in \text{Spec}(\mathcal{B})$ with $\mathfrak{q} \cap \mathcal{A} = \mathfrak{p} = \mathfrak{q}' \cap \mathcal{A}$.

   Claim:
   $$\mathfrak{q}' \subseteq \cup_{g \in G} g(\mathfrak{q}).$$

   By prime avoidance 1.27, the claim $\implies \exists g \in G, \mathfrak{q} \subseteq g(\mathfrak{q})$ both lying over $\mathfrak{q}$ (by part (ii)), then by incomparability 7.25 we know $\mathfrak{q}' = g(\mathfrak{q})$, as desired.

   Proof of the claim: Let $x \in \mathfrak{q}'$. Set $y := \prod_{g \in G} g(x) \in L^G$. By Galois theory, $\exists n \geq 1$ s.t. $y^n \in K$. Moreover, since each $g(x) \in \mathcal{B}$, and $\mathcal{B}$: integral over $\mathcal{A}$, we see that y^n is integral over $\mathcal{A}$ and belongs to K. (It is an integral element in $\text{Frac}(\mathcal{A})$). Since $\mathcal{A}$ is normal, we get that $y^n \in \mathcal{A} \cap \mathfrak{q}' = \mathfrak{q} \cap \mathcal{A}$.

   Since $\mathfrak{q}$ is prime, and $y^n = \prod_{g \in G} g(x)^n$, deduce that $g(x) \in \mathfrak{q}$ for some $g \in G$. **Notice that this step relies on the finiteness of $\#G$**
   Hence, we know $x \in g^{-1}(\mathfrak{q})$. Thus $\mathfrak{q}' \subseteq \cup_{g \in G} g^{-1}(\mathfrak{q}) = \cup_{g \in G} g(\mathfrak{q})$ as claimed.

   This completes the proof of (iii) in the case that L/K is finite.

   (b) For the infinite case.

Recall the **Zorn's Lemma**: In a nonempty partially ordered set $(A, \leq)$ in which each chain $C \subseteq A$ has an upper bound in A, then there is a maximal element.

We will use this to deduce the infinite case from the finite case. Consider a subextension $L/E/K$, with E/K normal. Then $R_E := \mathcal{B} \cap E$ is the integral closure of A in E. $\mathfrak{q}_1 \cap R_E = \mathfrak{q}_1 \cap E$ and $\mathfrak{q}_2 \cap R_E = \mathfrak{q}_2 \cap E$ are primes of R_E that lies over $\mathfrak{p}$

$$
A := \left\{
\begin{array}{l}
(E, g) : E \text{ as above} \\
\qquad g \in Aut(E/K) \\
\quad \text{s.t. } g(\mathfrak{q} \cap E) = \mathfrak{q}_2 \cap E
\end{array}
\right\}
$$

define an order on A:

$(E, q) \leq (E', g')$ iff $E \subseteq E', g'|_E = g$

<u>Want</u>: $\exists g \in Aut(L/K)$ s.t. $(L, g) \in A$

$A \neq \emptyset \Longleftarrow (K, id) \in A$. Let $C = \{(E_i, g_i)\}_{i \in I} \subseteq A$ be a chain, where $i \leq j \Longrightarrow (E_i, g_i) \leq (E_j, g_j)$.
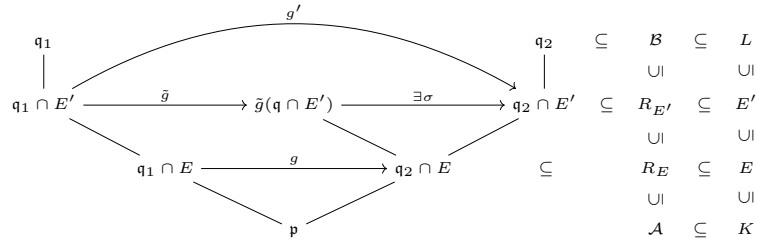
Then C has an upper bound $(E, g) \in A$

$$
\left\{
\begin{array}{l}
E := \cup_i E_i \\
\exists! g \in Aut(E/K) \\
\quad \text{s.t. } g|_{E_j} = g_j
\end{array}
\right.
$$

Thus by Zorn's lemma, $\exists$ maximal $(E, g) \in A$.

<u>Claim</u>: $E = L$.

If not. then $\exists$ finite normal extension E'/E with $E' \subseteq L$ and $E' \supsetneq E$. (Take any $\alpha \in L$, $\alpha \notin E$. Let $f \in E[X]$ be the minimal polynomial of α over E. Take $E' :=$ field obtained by adjoining to E all roots of f in L.)

Let $\tilde{g} \in Aut(E'/K)$ be any extension of g (such $\tilde{g}$ exists).
Then $\tilde{g}(\mathfrak{q}_1 \cap E')$ lies over $\mathfrak{q}_2 \cap E$.

Since theorem holds for E'/E (finite normal extension), $\exists \sigma \in Aut(E'/E)$ s.t. $\sigma(\tilde{g}(\mathfrak{q}_1 \cap E')) = \mathfrak{q}_2 \cap E'$.

Set $g' := \sigma \circ \tilde{g} \in Aut(E'/K)$. Clearly, $g'(\mathfrak{q}_1 \cap E') = \mathfrak{q}_2 \cap E'$, so $(E', g') \in A$. Also, $E \subsetneq E'$ and $g'|E = g$, which contradict the maximality of (E, g)

$\square$

Then let's talk about the so called going-down property.

Definition 7.32. *Let $\mathcal{A} \subseteq \mathcal{B}$ are rings. We say that $\mathcal{A} \subseteq \mathcal{B}$ has property **Going-Down** (GD) if*

$$\forall \ primes, \ \mathfrak{p}' \subsetneq \mathfrak{p} \subset \mathcal{A}, \mathfrak{q} \subset \mathcal{B}$$

with $\mathfrak{q} \cap \mathcal{A} = \mathfrak{p}$, $\exists$ prime $\mathfrak{q}' \subsetneq \mathfrak{q}$ with $\mathfrak{q}' \cap \mathcal{A} = \mathfrak{p}'$

$$
\begin{array}{ccccc}
\exists \mathfrak{q}' & \subsetneq & \mathfrak{q} & \subsetneq & \mathcal{B} \\
| & & | & & \cup| \\
\mathfrak{p}' & \subsetneq & \mathfrak{p} & \subsetneq & \mathcal{A}
\end{array}
$$

See P239 of Eisenbud or 32-33 of Matsumura for a non-example.

Theorem 7.33. *(Going-Down for integral extension over normal ring) Let $\mathcal{A} \subseteq \mathcal{B}$ be domains with $\mathcal{A}$ normal, $\mathcal{B}$ integral over $\mathcal{A}$. Then $\mathcal{A} \subseteq \mathcal{B}$ has Going-Down property.*

Proof. Let $K := Frac(\mathcal{A})$, $L_1 := Frac(\mathcal{B})$. $\implies L_1$ is integral over K as rings by Lemma 7.22, equivalently L/K is algebraic field extension.

Let L be any normal algebraic extension of K, that contains L_1 (e.g., $L = \overline{K} \supseteq L_1$) (e.g., $L :=$ "normal closure of L_1 in $\overline{K} \supseteq L_1$")

Hence x, y belong to a finite extension of $K \iff x, y$ algebraic over K, $\implies x/y$ algebraic over K.

Let $\mathcal{C} := ($ integral closure of $\mathcal{A}$ in L)=(integral closure of $\mathcal{B}$ in L)

Let $Q' \subseteq \mathcal{C}$ lies over $\mathfrak{p}'$, it exists by Lying-Over.

Let $Q_1 \subseteq \mathcal{C}$ lies over $\mathfrak{p}$, with $Q_1 \supseteq Q'$. It exists by Going-Up.

Let $Q \subseteq \mathcal{C}$ lies over $\mathfrak{q}$, it exists by Lying over.

Notice that both Q and Q_1 lies over $\mathfrak{p}$, by Theorem 7.31, $\exists g \in \mathrm{Aut}(L/K)$ s.t. $g(Q_1) = Q$.

$Q' \subsetneq Q_1 \implies g(Q') \subsetneq Q_1$

$\implies \mathfrak{q}' = g(Q') \cap \mathcal{B} \subsetneq g(Q_1) \cap \mathcal{B} = \mathfrak{q}$ by Incomparability.

Note that g fixes $\mathcal{A}$ so $\mathfrak{q}' \cap \mathcal{A} = (g(Q') \cap \mathcal{B}) \cap \mathcal{A} = g(Q') \cap \mathcal{A} = g(Q' \cap \mathcal{A}) = g(\mathfrak{p}') = \mathfrak{p}'$. $\qquad\square$

As an application of Going-Down. Recall $\forall \mathcal{A} \subseteq \mathcal{B}$ integral, $\forall \mathfrak{b} \subseteq \mathcal{B}, \mathfrak{a} \subseteq \mathcal{A} \cap \mathfrak{b}$

(i) $\dim(\mathcal{A}) = \dim(\mathcal{B})$

(ii) $\dim(\mathcal{A}/\mathfrak{a}) = \dim(\mathcal{B}/\mathfrak{b})$, i.e., $\mathrm{coht}(\mathfrak{a}) = \mathrm{coht}(\mathfrak{b})$

(iii) $\mathrm{ht}(\mathfrak{b}) \leq \mathrm{ht}(\mathfrak{a})$.

Corollary 7.34. *Suppose $\mathcal{A} \subseteq \mathcal{B}$ are domains, with $\mathcal{A}$ noraml, $\mathcal{B}$ integral over $\mathcal{A}$. Let $\mathfrak{b} \subseteq \mathcal{B}$, $\mathfrak{a} = \mathcal{A} \cap \mathfrak{b}$. Then $ht(\mathfrak{a}) = ht(\mathfrak{b})$.*

Proof. Want: $\mathrm{ht}(\mathfrak{b}) \overset{?}{\geq} \mathrm{ht}(\mathfrak{a})$, where $\mathrm{ht}(\mathfrak{b}) = \inf_{\mathfrak{q} \supseteq \mathfrak{b}} \mathrm{ht}(\mathfrak{q})$ and $\mathrm{ht}(\mathfrak{a}) = \inf_{\mathfrak{p} \supseteq \mathfrak{a}} \mathrm{ht}(\mathfrak{p})$.

It suffices to show for each prime $\mathfrak{q} \subset \mathfrak{b}$ that $\mathfrak{p} := \mathfrak{q} \cap \mathcal{A} \supseteq \mathfrak{a}$ satisfies $\mathrm{ht}(\mathfrak{q}) \geq \mathrm{ht}(\mathfrak{p})$. Let $\mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_r = \mathfrak{p}$ be a chain of primes. By the going-down property, there exists a chain of primes $\mathfrak{q}_0 \subsetneq ... \subsetneq \mathfrak{q}_r = \mathfrak{q}$ in $\mathcal{B}$ such that $\mathfrak{q}_i$ lies over $\mathfrak{p}_i$

$\implies \mathrm{ht}(\mathfrak{q}) \geq r$. Since $\mathrm{ht}(\mathfrak{p}) = \sup\{r \text{ as above}\}$, we then conclude that $\mathrm{ht}(\mathfrak{q}) \geq \mathrm{ht}(\mathfrak{p})$. $\qquad\square$

7.5 Lecture 24. Noether Normalization Theorem

Definition 7.35. *"k-domain $\mathcal{A}$" (k is a field and $\mathcal{A}$ is a k-algebra as well as a domain)*

finitely generated k-domain means a k-domain which is a finitely generated as k-algebra $\iff \mathcal{A} \cong k[X_1, ..., X_n]/\mathfrak{a}$ for some $\mathfrak{a}$, $n \implies \dim(\mathcal{A}) \leq n$

Theorem 7.36. *(Noether Normalization) Let $\mathcal{A}$ finitely generated k-algebra. Set $d := \dim(\mathcal{A}) \in \mathbb{Z}_{\geq 0}$. Then there exists an injective morphism of k-algebras*

$$k[X] := k[X_1, .., X_d] \overset{\kappa}{\hookrightarrow} \mathcal{A}$$

which is integral: $\mathcal{A}$ is integral over $\kappa(k[X])$.

N.b. κ is determined by $x_1 := \kappa(X_1), ..., x_n := \kappa(X_d) \in \mathcal{A}$. κ is injective $\iff x_1, ..., x_d \in \mathcal{A}$ are algebraically independent over k. So the theorem says : $\exists$ algebraically independent $x_1, .., x_d \in \mathcal{A}$ s.t., $\mathcal{A}$ is integral over the k-algebra $\mathcal{A}_0 := k[x_1, ..., x_d] \subseteq \mathcal{A}$.

Corollary 7.37. *Let $\mathcal{A}$ finitely generated k-domains, then $K := Frac(\mathcal{A})$. Then $dim(\mathcal{A}) = tr.deg_k(K)$*

Proof. of Corollary 7.37. Let $d := \dim(\mathcal{A})$ $\mathcal{A}_0 = k[x_1, .., x_d]$ as above. $K_0 = Frac(\mathcal{A}_0) \cong k(x_1, ..., x_d)$

$\mathcal{A}$: integral over $\mathcal{A}_0 \implies K$ algebraic over K_0 (Confer the proof of Theorem 2 today).

$$\implies tr.deg_k(K) = tr.deg_k(K_0) = d = \dim(\mathcal{A}). \qquad \square$$

N.b., If $\kappa : k[X_1, ..., X_n] \longrightarrow \mathcal{A}$ is injective and integral, then automatically $n = \dim(\mathcal{A})$, because we have seen that integral extension preserves dimension.

First, we give a key lemma for Noether Normalization (NN).

Lemma 7.38. *Let $\mathcal{A}$ be a k-algebra, with $x_1, .., x_n \in \mathcal{A}$, $0 \neq f \in k[X_1, .., X_n]$ where $k[X_1, .., X_n]$ is the free polynomial ring. $w := f(x_1, .., x_n) \in k[x_1, ..., x_n] \subseteq \mathcal{A}$. Then $\exists z_1, .., z_{n-1} \in k[x_1, .., x_n]$ s.t. $k[x_1, ..., x_n]$ is integral over $k[z_1, .., z_{n-1}, w]$.*

And we have to give some motivation for this key lemma in that the lemma indicates the NN:

Proof. (Lemma 7.38$\implies$ NN 7.36) $\mathcal{A}$ is finitely generated k-algebra, say $\mathcal{A}$ generated by $x_1, ..., x_n$. If $x_1, ..., x_n$ are algebraic independent, then done: $\mathcal{A} = k[x_1, .., x_n]$.

Else $\exists 0 \neq f \in k[X_1, .., X_n]$ s.t. $0 = f(x_1, .., x_n)$, then by the key lemma (here $w = 0$), $\exists z_1, .., z_{n-1}$ s.t. $k[x_1, ..., x_n]$ integral over $k[z_1, .., z_{n-1}]$. Iterate finitely many times: $\mathcal{A}$ is integral over $k[u_1, ..., u_d]$, where $u_1, .., u_d$ are algebraic independent, $d \leq n - 1$. $\qquad \square$

For pedagogical reason, we start with a Baby case (Baby case, $n = 2, w = 0$) $\mathcal{A} = k[X, Y]/(f)$ for some $0 \neq f \in k[X, Y]$. x, y are images of X, Y, thus $0 = f(x, y)$.

<u>Want</u> $\exists z \in \mathcal{A}$ s.t. $\mathcal{A}$ is integral over $k[z]$.

Example 7.39. *For example, we can choose $f = XY - 1$ ($\implies xy = 1, y = 1/x$). Then $\mathcal{A}$ <u>Not</u> integral over $k[x]$. Thus the choice $z = x$ doesn't work.*

$$k[X] \cong k[x] \subsetneq \mathcal{A} = \frac{k[X, Y]}{XY - 1} \cong k\left[x, \frac{1}{x}\right] \cong k(x) \cong k(X).$$

$k[X]$ is normal because it is UFD, hence it is integrally closed in $k(X) \implies \mathcal{A}$ is <u>NOT</u> integral over $k(x)$. (y is algebraic over $k[x]$ but not integral over $k[x]$.)
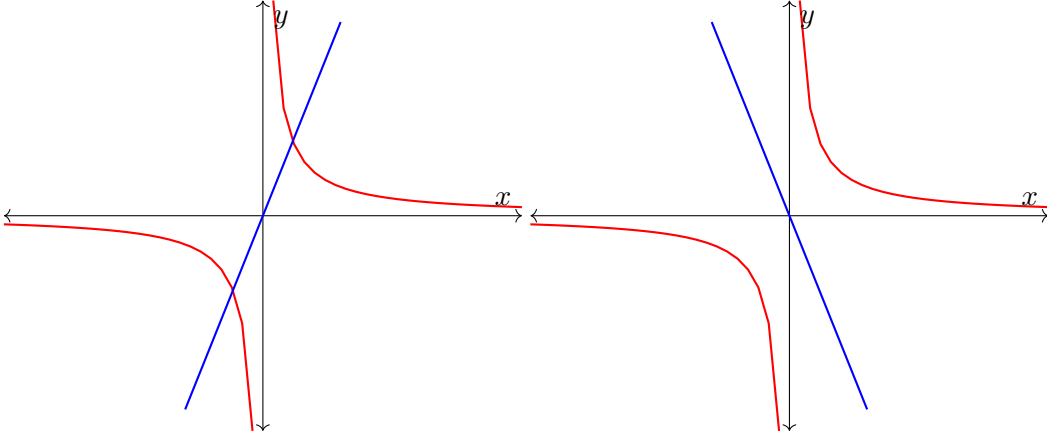
Similarly, $\mathcal{A}$ is not integral over $k[y]$.

But if we choose $z = y - ax$, then

$$zx = -ax^2 + xy = -ax^2 + 1$$

$$-ax^2 - zx + 1 = 0$$

$\implies \mathcal{A} = k[x, z]$ is integral over $k[z], \forall a \in k, a \neq 0$.

We have also a geometric interpretion of the above example: $Spec(\mathcal{A}) = \{(x, y) : xy = 1\}$, by the lying-over properties of integral extensions in Theorem 7.25, we know there should be a surjective map from $Spec(\mathcal{A})$ to $Spec(k[z])$

The general surjective map looks like $(x - c_0, y - d_0) \longmapsto (x - c_0, y - d_0) \cap k[z] = (z - d_0 + ac_0)$, it should be interpreted as the projection along blue line to y-axis. However when we choose $a < 0$, although $k[x, z]$ is still integral over $k[z]$, this geometric interpretation fails because the correspondence between maximals and points relies on the Hilbert Nullstellensatz which requires the the field to be algebraically closed.

The above simple example gives us implication for the proof of the baby case:

Lemma 7.40. *In the context of Baby case, $\mathcal{A} = k[X, Y]/(f)$ write $f = f_n + ... + f_0$. where f_i homogeneous of degree i and $f_n \neq 0$. If $Y - aX \nmid f_n$, $a \in k$. Then $\mathcal{A}$ is integral over $k[y - ax]$*

Proof. By substituting $X' := X$, $Y' := Y - aX$, reduce to the case $a = 0$.

If $Y \nmid f_n$, then $f_n = X^n +$ (lower powers in X with coefficients in Y). Then $f(x, y) = 0 \implies x^n +$ (lower powers in x with coefficients in y). Then we know $\mathcal{A} = k[X, Y]/(f) = k[x, y]$ is integral over $k[y]$. $\square$

Corollary 7.41. *If k is infinite, then Baby case holds.*

Proof. By the above lemma, it suffices to find $a \in k$ s.t. $Y - aX \nmid f_n$. Over $\bar{k}$, $f_n = \prod_{i=1\ldots,n}(\alpha_i X - \beta_i Y)$ $\alpha_i, \beta_i \in \bar{k}$ not both zero.

Just need that $a \neq \alpha_i/\beta_i \forall i$. This is always possible because k is infinite. $\square$

How about finite k?

Example 7.42. $k = \mathbb{F}_2$, $f = Y(Y - X) - 1$, *denote* $f_2 = Y(Y - X)$ *Then* $Y - aX | f_2$ $\forall a \in k$ *so previous strategy fails. (in fact $\mathcal{A}$ is not integral over $k[y - ax]$ for all a)*

Try $z : y - x^s$, $s \in \mathbb{Z}_{\geq 0}$. Say $s \geq 2$.

$0 = f(x, y) = f(x, x^s + z) = (x^s + z)(x^s + z - x) - 1$

$\implies 0 = x^{2s} + (....)$ *the* $(...)$ *are of lower order in x with coefficients in z*

$\implies x$ *integral over $k[z] \implies \mathcal{A} = k[x, z]$ is integral over $k[z]$. This choice works for any $f \neq 0$ if s is large enough in terms of f.*

Proof. (of key lemma [7.38](#) due to Nagata) Write $f = \sum_{\alpha \in I} c_\alpha X^\alpha$, where $c_\alpha \in k^\times$ and $X^\alpha := X_1^{\alpha_1} \cdots X_n^{\alpha_n}$. For some finite $I \subseteq \mathbb{Z}_{\geq}^n$. Choose $z_j := x_j - x_n^{s_j}$ for $j = 1, ..., n-1$, where $s_j \in \mathbb{Z}_{\geq 0}$ to be chosen later.

Then $x_j = x_n^{s_j} + z_j$, so

$$w = f(x_1, ..., x_n) = f(x_n^{s_1} + z_1, ..., x_n^{s_{n-1}} + z_{n-1}, x_n)$$
$$= \sum_{\alpha \in I} c_\alpha (x_n^{s_1} + z_1)^{\alpha_1} \cdots (x_n^{s_{n-1}} + z_{n-1})^{\alpha_{n-1}} x_n^{\alpha_n}$$

where each power equals $x_n^{s_j \alpha_j} + (...)$ lower powers with coefficients in z_j

$$= \sum_{\alpha \in I} c_\alpha x_n^{l(\alpha)} + (...), \quad l(\alpha) := s_1 \alpha_1 + ... + s_{n-1} \alpha_{n-1} + \alpha_n,$$

where $(...)$ are of lower powers in x_n with coefficients in $k[z_1, .., z_{n-1}]$

To make sure the leading term does not cancel out, we need <u>Sublemma:</u> $\exists (s_1, ..., s_{n-1})$ s.t., $\forall, \alpha, \beta \in I$

$$\alpha \neq \beta \implies l(\alpha) \neq l(\beta) \tag{*}$$

<u>Proof1</u>: Take $s_j = s^j$, where $s := \max\{|\alpha_j| + 1 | \alpha \in I, j = 1, ..., n\}$.

<u>Proof2</u>: ($*$) basically says that $(s_1, ..., s_{n-1})$ have to avoid finitely many proper subspaces of $\mathbb{Q}^{n-1}$, which is always possible, because finite union of proper subspaces can not be the vector space it self.

Choose s as in sublemma. Choose $\alpha \in I$ s.t. $l(\alpha)$ maximal. Then $w = c_\alpha x_n^{l(\alpha)} + (...)$

$\Longrightarrow x_n$ is integral over $k[z_1, ..., z_{n-1}, w]$

$\Longrightarrow$ each $x_j = x_n^{s_j} + z_j$ is integral over $k[z_1, ..., z_{n-1}, w]$

$\Longrightarrow k[x_1, ..., x_n]$ is integral over $k[z_1, ..., z_{n-1}, w]$. $\qquad\square$

The above proved the key Lemma 7.38 thus the Noether Normalization 7.36.

Theorem 7.43. *Let $\mathcal{A}$ be finitely generated k-domain, $\mathfrak{p} \in Spec(\mathcal{A})$. Then $ht(\mathfrak{p}) + coht(\mathfrak{p}) = ht(\mathfrak{p}) + dim(\mathcal{A}/\mathfrak{p}) = dim(\mathcal{A})$*

Proof. Set $n := \dim(\mathcal{A})$. NN 7.36$\Longrightarrow \exists x_1, .., x_n \in \mathcal{A}$ algebraic independent s.t. $\mathcal{A}$ is integral over $\mathcal{A}_0 := k[x_1, .., x_n] \cong k[X_1, .., X_n]$.

$\mathcal{A}_0$ is UFD $\Longrightarrow \mathcal{A}_0$ is normal.

Both $\mathcal{A}_0$ $\mathcal{A}$ are domains and $\mathcal{A}_0 \subseteq \mathcal{A}$ is an integral extension. So by the Going-Down properties 7.33 , we have

$$\mathfrak{p}_0 := \mathcal{A}_0 \cap \mathfrak{p} \in \mathrm{Spec}(\mathcal{A}_0)$$

that $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{p}_0)$, $\mathrm{coht}(\mathfrak{p}) = \mathrm{coht}(\mathfrak{p}_0)$, $\dim(\mathcal{A}) = \dim(\mathcal{A}_0)$. Thus by replacing $\mathcal{A}$ by $\mathcal{A}_0$, we may assume $\mathcal{A} = k[X_1, ..., X_n]$. (And now our problem reduces to understanding $\mathrm{Spec}(k[X_1, ..., X_n])$)

If $\mathfrak{p} = (0)$, then we are done: $\mathrm{ht}(\mathfrak{p}) = 0$, $\mathrm{coht}(\mathfrak{p}) = \dim(\mathcal{A})$.

So we may assume $\mathfrak{p} \neq (0)$. Suppose a special case where $\mathfrak{p} \ni X_n$. Then $\mathfrak{p} \supseteq (X_n)$.

Set $\overline{\mathcal{A}} := \mathcal{A}/(X_n) \cong k[X_1, ..., X_{n-1}]$, $\overline{\mathfrak{p}} := \mathfrak{p}/(X_n)$.

Then $0 \subsetneq (X_n) \subseteq \mathfrak{p}$, so $\mathrm{ht}(\mathfrak{p}) \geq \mathrm{ht}(\overline{\mathfrak{p}}) + 1$. (Given $(0) = \overline{\mathfrak{q}_0} \subsetneq ... \subsetneq \overline{\mathfrak{q}_r} = \overline{\mathfrak{p}}$, get $(0) \subsetneq (X_n) = \mathfrak{q}_0 \subsetneq ... \subsetneq \mathfrak{q}_r = \mathfrak{p}$)

Also $\mathrm{coht}(\overline{\mathfrak{p}}) = \dim(\overline{\mathcal{A}}) = \mathrm{coht}(\overline{\mathfrak{p}})$,

$\dim(\overline{\mathcal{A}}) = n - 1 = \dim(\mathcal{A}) - 1$.

In general $\mathrm{ht}(\mathfrak{p}) + \mathrm{coht}(\mathfrak{p}) \leq \dim(\mathcal{A})$ holds trivially. so we just need to show

$$\mathrm{ht}(\mathfrak{p}) + \mathrm{coht}(\mathfrak{p}) \geq \dim(\mathcal{A}),$$

where $\mathrm{ht}(\mathfrak{p}) \geq \mathrm{ht}(\overline{\mathfrak{p}}) + 1$, $\mathrm{coht}(\mathfrak{p}) = \mathrm{coht}(\overline{\mathfrak{p}})$ and $\dim(\mathcal{A}) = \dim(\overline{\mathcal{A}}) + 1$. (If we are able to show $\mathrm{ht}(\overline{\mathfrak{p}}) + \mathrm{coht}(\overline{\mathfrak{p}}) \geq \dim(\overline{\mathcal{A}})$, we are done)

So we can argue by induction on n in the special case $X_n \in \mathfrak{p}$.

We now reduce the general case to this one. Choose any $0 \neq f \in \mathfrak{p}$. By the key lemma 7.38 for NN, $\exists z_1, ..., z_{n-1} \in \mathcal{A} = k[x_1, ..., x_n]$, s.t. $\mathcal{A}$ integral over $\mathcal{A}_0 := k[z_1, ..., z_{n-1}, z_n]$, where $z_n := f(x_1, ..., x_n)$. Then $\mathrm{tr.deg}_k(\mathrm{Frac}(\mathcal{A}_0)) = \mathrm{tr.deg}_k(\mathrm{Frac}(\mathcal{A})) = n$, so $\{z_j\}$ are algebraically independent. Thus $\mathcal{A}_0$ is again a polynomial ring, hence $\mathcal{A}_0$ is normal.

By arguing as in the beginning of the proof, we have with $\mathfrak{p}_0 := \mathfrak{p} \cap \mathcal{A}_0$ that $\dim(\mathcal{A}_0) = \dim(\mathcal{A})$, $\mathrm{coht}(\mathfrak{p}_0) = \mathrm{coht}(\mathfrak{p})$, $\mathrm{ht}(\mathfrak{p}_0) = \mathrm{ht}(\mathfrak{p})$. So it suffices to show that $\mathrm{coht}(\mathfrak{p}_0) + \mathrm{ht}(\mathfrak{p}_0) \geq \dim(\mathcal{A}_0)$.

But now $f \in \mathfrak{p} \implies z_n \in \mathfrak{p}_0$, so we reduce to the special case $x_n \in \mathfrak{p}$. Argued as above. $\square$

Lemma 7.44. *$\mathcal{A}$ is finitely generated k-domain. Let $\mathfrak{p} \subsetneq \mathfrak{p}'$ be "adjacent primes" i.e., no primes contained in between. Then*

$$ht(\mathfrak{p}') = ht(\mathfrak{p}) + 1$$

Proof. Apply previous theorem to $(\mathcal{A}, \mathfrak{p})$, $(\mathcal{A}, \mathfrak{p}')$ and $(\overline{\mathcal{A}}, \overline{\mathfrak{p}'})$, where $\overline{\mathcal{A}} = \mathcal{A}/\mathfrak{p}$ and $\overline{\mathfrak{p}'} = \mathfrak{p}'/\mathfrak{p}$. Hypothesis that $\mathfrak{p}$, $\mathfrak{p}'$ "adjacent" $\implies \mathrm{ht}(\overline{\mathfrak{p}'}) = 1$. Then by Theorem 7.43

$$\mathrm{ht}(\mathfrak{p}) + \mathrm{coht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{p}) + \dim(\overline{\mathcal{A}}) = \dim(\mathcal{A})$$

$$\mathrm{ht}(\mathfrak{p}') + \mathrm{coht}(\mathfrak{p}') = \mathrm{ht}(\mathfrak{p}') + \mathrm{coht}(\overline{\mathfrak{p}'}) = \dim(\mathcal{A})$$

$$\mathrm{ht}(\overline{\mathfrak{p}'}) + \mathrm{coht}(\overline{\mathfrak{p}'}) = \dim(\overline{\mathcal{A}})$$

Then

$$\mathrm{ht}(\mathfrak{p}') - 1 = \mathrm{ht}(\mathfrak{p}') - \mathrm{ht}(\overline{\mathfrak{p}'}) = \dim(\mathcal{A}) - \dim(\overline{\mathcal{A}}) = \mathrm{ht}(\mathfrak{p})$$

. $\square$

Recall what we have know about the dimension theory of finitely generated k-domain. $\forall k$ field, $\mathcal{A}$ a finitely generated k-domain, then

(i) $\dim(\mathcal{A}) = tr.deg_k(K)$, where $K := Frac(\mathcal{A})$

(ii) $\mathrm{ht}(\mathfrak{p}) + \mathrm{coht}(\mathfrak{p}) = \dim(\mathcal{A}), \forall \mathfrak{p} \in \mathrm{Spec}(\mathcal{A})$

(iii) $\mathrm{ht}(\mathfrak{m}) = \dim(\mathcal{A}), \forall \mathfrak{m}$ maximal

(iv) If $\mathfrak{p} \subsetneq \mathfrak{p}'$ are adjacent,,i.e., $\mathrm{ht}(\mathfrak{p}'/\mathfrak{p}) = 1$, then $\mathrm{ht}(\mathfrak{p}') = \mathrm{ht}(\mathfrak{p}) + 1$

Corollary 7.45. *If $\mathcal{A}$ is finitely generated k-domain. Every maximal chain of primes in $\mathcal{A}$ has length $dim(\mathcal{A})$. That is to say: if $\mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_r \subset \mathcal{A}$ is a chain of primes that cannot be enlarged, then $r = dim(\mathcal{A})$.*

The above corollary is false for general rings $\mathcal{A}$. See the exercises, Matsumura, the keyword is **"Catenary"**

Proof. Maximality of the chain implies: $\mathfrak{p}_0 = (0) \implies \mathrm{ht}(\mathfrak{p}_0) = 0$ and $\mathfrak{p}_r$ maximal $\implies \mathrm{ht}(\mathfrak{p}_r) = \dim(\mathcal{A})$. Also $\forall \mathrm{ht}(\mathfrak{p}_i/\mathfrak{p}_{i-1}) = 1 \implies \mathrm{ht}(\mathfrak{p}_i) = \mathrm{ht}(\mathfrak{p}_{i-1}) + 1 \implies \dim(\mathcal{A}) = \mathrm{ht}(\mathfrak{p}_r) - \mathrm{ht}(\mathfrak{p}_0)$.

Note that this Corollary implies $(ii), (iii), (iv)$ $\square$

Corollary 7.46. *(Another proof of Zariski's Lemma 4.23 thus the Nullstellensatz 4.30) Let K/k be field extension s.t. K is finitely generated k-algebra, then K/k is finite.*

Proof. It suffices to show that K/k is algebraic (i.e.,integral) because by 7.7 integral +finitely generated $\iff$ finite. That is, we want $tr.deg_k(K) = 0$. But $tr.deg_k(K) = \dim(K) = 0$. $\square$

8   Valuation Rings and Normality

8.1   Lecture 25. Valuation

Recall the proof that the ring $\mathcal{A} := k[X,Y]/(XY-1)$ is not integral over $k[x]$. We denote by x, y the image of X, Y in $\mathcal{A}$.

We embed

$$\mathcal{A} \hookrightarrow k(X)$$

$$x, y \longmapsto X, 1/X$$

We then argued that $k[X]$ is normal, hence that $\mathcal{A} \cong k[X, 1/X]$ is Not integral over $k[X]$.

Here, we will give another proof.

Definition 8.1. *Any $0 \neq f \in \mathcal{A}$ may be written in the form*

$$a_{-n}X^{-n} + ... + a_m X^m,$$

where $a_j \in k, a_{-n} \neq 0$.
    Set $v(f) := -n \in \mathbb{Z}$. Note:

1. $v(f_1 f_2) = v(f_1) + v(f_2)$

2. $v(f_1 + f_2) \geq min(v(f_1), v(f_2))$, *if* $v(f_1) \neq v(f_2)$, *then* $v(f_1 + f_2) = \min(v(f_1), v(f_2))$

Now suppose that $f \in k[X, 1/X]$, and $f \notin k[X]$. Then $v(f) \leq -1$, but

$$f^n + a_1 f^{n-1} + ...a_0 = 0$$

with $a_j \in k[X]$. Note $v(a_j) \geq 0$
$\implies v(a_j f^{n-j}) \geq v(f^{n-j}) = (n-j)v(f) \leq -1$
$\implies v(f^n) = nv(f) < v(a_1 f^{n-1} + ... + a_n)$, *contradicting to* $f^n + a_1 f^{n-1} + .. + a_n = 0$.

Definition 8.2. *Let K be a field, $(G, 0, +, \leq)$ totally ordered abelian group e.g. $(G = \mathbb{Z})$. A map $v : K^\times \longrightarrow G$ is called a **valuation** if it satisfies the property*

1. $v(f_1 f_2) = v(f_1) + v(f_2)$

2. $v(f_1 + f_2) \geq min(v(f_1), v(f_2))$,
   if $v(f_1) \neq v(f_2)$, then $v(f_1 + f_2) = \min(v(f_1), v(f_2))$

In that case, the set $\mathcal{A} := \{x \in K^\times : v(x) \geq 0\} \cup \{0\}$ is a subring of K, called the **valuation ring of** v.

Lemma 8.3. *The set $\mathfrak{m} := \{x \in K^\times : v(x) > 0\} \cup \{0\}$ is a maximal ideal of $\mathcal{A}$ and $(\mathcal{A}, \mathfrak{m})$ is a local ring with $\mathcal{A}^\times = \{x \in K^\times : v(x) = 0\}$*

Proof. $x \in K^\times \cap \mathcal{A}$, $v(x) = 0$, $\implies v(1/x) + v(x) = v(1) = 0 \implies v(1/x) = 0$.
   $\implies 1/x \in \mathcal{A}$, so $x \in \mathcal{A}^\times$. $\implies (\mathcal{A}, \mathfrak{m})$ is local ($\impliedby \mathcal{A} - \mathfrak{m} \subseteq \mathcal{A}^\times$ 1.20) $\qquad \square$

Definition 8.4. *(K: field), We say that a subring $\mathcal{A} \subseteq K$ is a **valuation ring** if $\exists$ valuation $v : K^\times \longrightarrow G$ s.t. $\mathcal{A}$ is the valuation ring of v. We call G the* **valuation group of** v.

Lemma 8.5. *Valuation ring $\mathcal{A} \subseteq K$ are normal.*

Proof. Valuation ring $\mathcal{A}$ is a subring of a field, thus always an integral domain, and $\text{Frac}(\mathcal{A}) \subseteq K$. Suppose $f \in K - \mathcal{A}$ is integral over $\mathcal{A}$:

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

Each $v(a_i) \geq 0$ because $a_i \in \mathcal{A}$ but $v(f) \leq 0$ get a contradiction as before. $\qquad \square$

Custom: one extends $v : K^\times \longrightarrow G$ to $v : K \longrightarrow G \cup \{\infty\}$ by $v(0) := \infty$. Then $\mathcal{A} := \{x \in K : v(x) \geq 0\}$, $\mathfrak{m} := \{x \in K : v(x) > 0\}$.

Example 8.6. $K = k(X) = Frac(k[X])$. *Each* $f \in K^\times$ *may be written* $f = X^n \frac{P}{Q}$, *where* $P, Q \in k[X]$ *and* $X \nmid P \cdot Q$ *in* $k[X]$, $v(f) := n$. *This defines a valuation with the corresponding ring* $\mathcal{A} = k[X]_{\mathfrak{p}}, \mathfrak{p} = (X)$.

for example $v(X + X^2) = v(X(X + 1)) = 1$

Example 8.7. $\mathcal{A} = k[[X]], K = k((X)), v(\sum a_i X^i) := min\{i : a_i \neq 0\}$ *is a valuation ring.*

Example 8.8. $k[X^2, X^3]$ *is not normal thus not a valuation ring.*

Example 8.9. $k[X(X - 1), X^2(X - 1)]$ *is not normal thus not a valuation ring.*

Lemma 8.10. *Let* $\mathcal{A} \subseteq K$ *be a subring in a field. Then the following are equivalent:*

(i) $\mathcal{A}$ *is a valuation ring (VR) of some* v

(ii) $x \in K - \mathcal{A} \implies 1/x \in \mathcal{A}$ *(i.e.,* $\forall x \in K$, *either* $x \in \mathcal{A}$ *or* $1/x \in \mathcal{A}$ *or both.)*

Proof. $(i) \implies (ii)$, Say $\mathcal{A}$ is a VR corresponding to $v : K^\times \longrightarrow G$, if $x \in K - \mathcal{A}$, then $v(x) < 0$, so $v(1/x) > 0$, so $1/x \in \mathcal{A}$.

$(ii) \implies (i)$:

Set $G := K^\times / \mathcal{A}^\times$ (quotient of multiplication group), $\sigma : K^\times \longrightarrow G$

Define "$\leq$ on G" : $x\mathcal{A}^\times \leq y\mathcal{A}^\times \iff y \in x\mathcal{A}$ or equivalently $(yx^{-1} \in \mathcal{A})$.

Claim: Then "$\leq$" is total order.

Indeed, let $x\mathcal{A}^\times, y\mathcal{A}^\times \in G$. Take representatives $x, y \in K^\times$. Then $x/y \in K^\times$. If $x/y \in \mathcal{A}$, then $x \in y\mathcal{A}^\times$, so $y\mathcal{A}^\times \leq x\mathcal{A}^\times$.

If $x/y \in \mathcal{A}$. Then $x \in y\mathcal{A}$, $y\mathcal{A}^\times \leq x\mathcal{A}^\times$.

Else, $x/y \in K - \mathcal{A}$, so $y/x \in \mathcal{A}$ by (ii) hence $x\mathcal{A}^\times \leq y\mathcal{A}^\times$.

We also have the equality, $x\mathcal{A}^\times = y\mathcal{A}^\times \iff$ both x/y and y/x are in $\mathcal{A}$.

Claim: σ satisfies the valuation criteria and $\mathcal{A}$ is induced by σ.

$\sigma(f_1 f_2) = \sigma(f_1)\sigma(f_2)$: because σ is a group morphism.

$\sigma(f_1 + f_2) \geq min\{\sigma(f_1), \sigma(f_2)\}$ and $\sigma(f_1 + f_2) = min\{\sigma(f_1), \sigma(f_2)\}$ if $\sigma(f_1) \neq \sigma(f_2)$:

Suppose $\sigma(f_1) \geq \sigma(f_2) \implies f_1 f_2^{-1} \in \mathcal{A}$: $(f_1 + f_2)f_2^{-1} = f_1 f_2^{-1} + 1 \in \mathcal{A}$, then $\sigma(f_1 + f_2) \geq min\{\sigma(f_1), \sigma(f_2)\}$.

If $\sigma(f_1) \neq \sigma(f_2) \iff$ either f_1/f_2 or $f_2/f_1 \in K - \mathcal{A}$ but not both. Assume $f_1/f_2 \in \mathcal{A}, f_2/f_1 \in K - \mathcal{A}, \implies min\{\sigma(f_1), \sigma(f_2)\} = \sigma(f_2)$. $(f_1 + f_2)f_2^{-1} \in \mathcal{A}$ always holds, it remains to check whether $f_2(f_1 + f_2)^{-1} \in \mathcal{A}$. Indeed

$$\frac{f_2}{f_1} \in K - \mathcal{A} \implies \frac{f_1 + f_2}{f_1} = 1 + f_2/f_1 \in K - \mathcal{A} \implies \frac{f_1}{f_1 + f_2} \in \mathcal{A}$$

$$f_2(f_1 + f_2)^{-1} = \frac{(f_1 + f_2) - f_1}{f_1 + f_2} = 1 - \frac{f_1}{f_1 + f_2} \in \mathcal{A}$$

Set $\mathcal{A}' = \{x \in K^\times : \sigma(x) \geq 0_G\} \cup \{0_K\}$, where 0_G is multiplicative identity $1 \cdot \mathcal{A}^\times$ in $K^\times / \mathcal{A}^\times$.

<u>Claim</u>: $\mathcal{A} = \mathcal{A}'$.

$x \in \mathcal{A}' \implies \sigma(x) \geq 0_G = 1 \cdot \mathcal{A}^\times \implies x \in 1 \cdot \mathcal{A} = \mathcal{A} \; \mathcal{A}' \subseteq \mathcal{A}$.

$x \in \mathcal{A}, x \in 1 \cdot \mathcal{A} \implies \sigma(x) \geq 0 \implies x \in \mathcal{A}'$.

$\square$

Theorem 8.11. *Let $\mathcal{A} \subseteq K$ K is a field. $\overline{\mathcal{A}} :=$ integral closure of $\mathcal{A}$ in K. Then*

$$\overline{\mathcal{A}} = \cap_{\substack{\mathcal{B}: VR, \; in \; K \\ , with \; \mathcal{A} \subseteq \mathcal{B} \subseteq K}} \mathcal{B}$$

Proof. "$\subseteq$": if $x \in K$ is integral over $\mathcal{A}$, then x is also integral over each $\mathcal{B} \supseteq \mathcal{A}$, but $\mathcal{B}:$ VR $\implies \mathcal{B}$ normal 8.5, hence $x \in \mathcal{B}$. Thus $\overline{\mathcal{A}} \subseteq \cap_{...} \mathcal{B}$

"$\supseteq$": Need to show that if $f \in K$ is not integral over $\mathcal{A}$.

<u>Want</u>: $\exists$ VR $\mathcal{B} \supseteq \mathcal{A}$ with $f \notin \mathcal{B}$.

f not integral over $\mathcal{A} \implies f \notin \mathcal{A}[1/f] \implies 1/f \notin \mathcal{A}[1/f]^\times$:

$\exists \mathfrak{p} \subset \mathcal{A}[1/f]$ primes so that $1/f \in \mathfrak{p}$.

Then quote the Lemma bellow

Lemma 8.12. $\mathcal{R} \subseteq K$ *, a subring in a field, given $\mathfrak{p} \in Spec(\mathcal{R})$, then there exists a valuation ring $\mathcal{B}$ s.t., $\mathcal{R}_{\mathfrak{p}} \subseteq \mathcal{B} \subseteq K$ s.t. the maximal $\mathfrak{m}$ of $\mathcal{B}$ s.t. $\mathfrak{m} \cap \mathcal{R} = \mathfrak{p}$.*

With Lemma 8.12, we can proceed on. Set $\mathcal{R} = \mathcal{A}[1/f]$ and $\mathfrak{p}$ to be a prime in $\mathcal{A}[1/f]$ that contains $1/f$. Then $1/f \in \mathfrak{p} \implies f \notin \mathcal{B}$. $\square$

Proof. (of Lemma 8.12 due to Matsumura)

Set $\Sigma := \{\text{rings } \mathcal{C}: \mathcal{R}_{\mathfrak{p}} \subseteq \mathcal{C} \subseteq K, \mathfrak{p}\mathcal{C} \subsetneq \mathcal{C}\}$, partially ordered by inclusion. We have $\mathcal{R} \in \Sigma$, so $\Sigma \neq \emptyset$. Moreover a union of a chain is again an element in Σ, so by Zorn's Lemma, there is a maximal element. We assume $\mathcal{B}$ is the maximal element of Σ. Since $\mathfrak{p}\mathcal{B} \subsetneq \mathcal{B}$, there exists a maximal ideal $\mathfrak{m}$ of $\mathcal{B}$ containing $\mathfrak{p}\mathcal{B}$. Since $\mathcal{B} \subseteq \mathcal{B}_{\mathfrak{m}}$ and $\mathfrak{p}\mathcal{B}_{\mathfrak{m}} \subsetneq \mathcal{B}_{\mathfrak{m}} \implies \mathcal{B}_{\mathfrak{m}} \in \Sigma$, by maximality of $\mathcal{B}$, we have $\mathcal{B} = \mathcal{B}_{\mathfrak{m}}$. So $(\mathcal{B}, \mathfrak{m})$ is a local ring. Also $\text{rad}(\mathfrak{p}\mathcal{B}) = \mathfrak{m}$. Indeed, we have that for any prime that contains $\mathfrak{p}\mathcal{B}$, the ring $\mathcal{B}$ is local with maximal ideal $\mathfrak{m}$. Thus there is only one such prime.

<u>Claim</u>: $\mathfrak{m} \cap \mathcal{R} = \mathfrak{p}$:

$\mathfrak{p} \subseteq \mathfrak{p}\mathcal{B} \cap \mathcal{R} \subseteq \mathfrak{m} \cap \mathcal{R}$ (This is guaranteed by $\mathfrak{p}\mathcal{B}$ being a proper ideal)

$\mathfrak{m} \cap \mathcal{R} = \mathfrak{m} \cap \mathcal{R}_{\mathfrak{p}} \cap \mathcal{R}$ (This is guaranteed by $\mathcal{R} \subseteq \mathcal{R}_{\mathfrak{p}} \subseteq K$, and $\mathcal{R} \subseteq \mathcal{B} \subseteq K$, where we regard it as intersection of subsets in K)

$\mathfrak{m} \cap \mathcal{R}_{\mathfrak{p}}$ is an ideal of $\mathcal{R}_{\mathfrak{p}}$ (This is gauranteed by $\mathcal{R}_{\mathfrak{p}} \subseteq \mathcal{B}) \Longrightarrow \mathfrak{m} \cap \mathcal{R}_{\mathfrak{p}} \subseteq \mathfrak{p}\mathcal{R}_{\mathfrak{p}}$
$\mathfrak{m} \cap \mathcal{R} \subseteq \mathfrak{p}\mathcal{R}_{\mathfrak{p}} \cap \mathcal{R} = \mathfrak{p}$.

Altogether, we have $\mathfrak{p} = \mathfrak{m} \cap \mathcal{R}$.

Claim: $(\mathcal{B}, \mathfrak{m})$ is a valuation ring of K.

Want: For $x, 1/x \in K^{\times}$, at least one of $x, 1/x$ lies in $\mathcal{B}$.

Assume x is not contained in $\mathcal{B}$. Then $\mathcal{B}[x]$ properly contains $\mathcal{B}$. So by maximality of $\mathcal{B}$, we know $\mathfrak{p}\mathcal{B}[x] = \mathcal{B}[x]$

$$1 = b_0 + ...b_{n-1}x + b_n x^n, \text{ where } b_i \in \mathfrak{p}\mathcal{B}$$

Write: $(1 - b_0) = \sum_{i=1,...,n} b_i x^i \equiv 1 \mod \mathfrak{p}\mathcal{B}$. Hence $(1 - b_0) \equiv 1 \mod \mathfrak{m}$, hence $(1 - b_0) \in \mathcal{B}^{\times}$. If we multiply both side by x^{-n}:

$$(1 - b_0)x^{-n} = \sum_{i=1,...,n} b_i x^{i-n}.$$

Thus $\frac{1}{x}$: integral over $\mathcal{B}$. Thus $\mathcal{B}[\frac{1}{x}]$ integral over $\mathcal{B}$.

Want: $1/x \in \mathcal{B}$.

By "Lying-Over" 7.25, $\exists \mathfrak{n} \in \mathrm{Spec}(\mathcal{B}[\frac{1}{x}])$ with $\mathfrak{n} \cap \mathcal{B} = \mathfrak{m}$.

Then $\mathfrak{p}\mathcal{B}[\frac{1}{x}] \subseteq \mathfrak{m}\mathcal{B}[\frac{1}{x}] \subseteq \mathfrak{n} \subsetneq \mathcal{B}[\frac{1}{x}]$.

So maximality of $\mathcal{B} \Longrightarrow \mathcal{B}[\frac{1}{x}] = \mathcal{B} \Longrightarrow \frac{1}{x} \in \mathcal{B}$. $\square$

8.2   Lecture 26. Discrete Valuation Ring and Normality

Definition 8.13. *A valuation $v : K^{\times} \longrightarrow G$ is **discrete** if $G \cong \mathbb{Z}, v \neq 0$. It is **normalized** if v is surjective: $v(G) = \mathbb{Z}$. In general, $v(K^{\times}) = n\mathbb{Z}$ for some $n \in \mathbb{Z}_{\geq 1}$, so $\frac{1}{n}v$ is normalized. A **discrete valuation ring** (DVR) is a VR attached to a normalized discrete valuation.*

Example 8.14. $\mathcal{A} = k[x]_{(x)}$, $v(x^n \frac{u}{v}) := n$ *for* $x \nmid uv$, $u, v \in k[x]$
   or $\mathcal{A} = k[[x]]$ *as before.*
   $\mathbb{Z}_{(p)} : \{x = p^n \frac{a}{b} \in \mathbb{Q} | a, b, n \in \mathbb{Z}, b \neq 0, p \nmid ab\}$, $v(x) := n\}$.

Non-example 8.15. $\mathcal{A} = \cup_{n \geq 1} k[[X^{1/n}]] \ni f = \sum_{i \in \mathbb{Q}} a_i X^i$. $v(f) := \min\{i : a_i \neq 0\}$, $v : K^{\times} \longrightarrow \mathbb{Q}$.

Definition 8.16. *Let $\mathcal{A} \subset K$ be a DVR with normalized valuation*

$$v : K \longrightarrow \mathbb{Z} \cup \{\infty\}$$

$$\mathfrak{p} = \{x \in K | v(x) \geq 1\}$$

*A **uniformizer** is an element ϖ with $v(\varpi) = 1$.*

Lemma 8.17. *Each $x \in K^\times$ is uniquely of the form*

$$x = u\varpi^n$$

for some $u \in \mathcal{A}^\times, n \in \mathbb{Z}$. One has $v(x) = n$, hence $n \geq 0 \Longleftrightarrow x \in \mathcal{A}$, $n \geq 1 \Longleftrightarrow x \in \mathfrak{p}$.

Proof. Let $n := v(x), u := x\varpi^{-n}$, then $v(u) = v(x) - nv(\varpi) = n - n = 0$, so $u \in \mathcal{A}^\times$. This proof is independent on the choice of uniformizer ϖ. □

Lemma 8.18. *The ideals in $\mathcal{A}$ are (0) and (ϖ^n). Moreover: $(\varpi^n) = \mathfrak{p}^n \, \forall n \in \mathbb{Z}_{\geq 0}$. Any two uniformizer differ by a unit: $\varpi' = u\varpi, u \in \mathcal{A}^\times$. Moreover,*

$$\{uniformizer\} = \mathfrak{p} - \mathfrak{p}^2.$$

Proof. If $x = u\varpi^n \in \mathcal{A}(n \geq 0)$, then $(x) = (\varpi^n)$. If $\mathfrak{a} \subseteq \mathcal{A}$ is any nonzero ideal, let $n := \min\{v(x) : 0 \neq x \in \mathfrak{a}\}$.

Then $\forall y \in \mathfrak{a}$, we have $v(y) \geq n = v(\varpi^n)$. So $v(y\varpi^{-n}) \geq 0$, so $y\varpi^{-n} \in \mathcal{A}$. Hence, any $y \in (\varpi^n)$. Thus $\mathfrak{a} \subseteq (\varpi^n)$. Conversely, $\exists x \in \mathfrak{a}$ with $v(x) = n$. Then $v(\varpi^n/x) = 0$. So $\frac{\varpi^n}{x} \in \mathcal{A}^\times$, so $(\varpi^n) \subseteq (x) \subseteq \mathfrak{a}$. Thus $\mathfrak{a} = (\varpi^n)$

Thus, $\mathfrak{p}$ maximal $\Longrightarrow \mathfrak{p} = (\varpi) \Longrightarrow \mathfrak{p}^n = (\varpi^n)$.

The same argument works for any other ϖ'. Gives $(\varpi') = \mathfrak{p} = (\varpi) \Longrightarrow \varpi' \in \mathcal{A}^\times\varpi$.

Also $\varpi \notin \mathfrak{p}^2$, alse $(\varpi) = (\varpi^2) \Longrightarrow v(\varpi) = 0$ contradiction.

See form the proof that $\forall 0 \neq x \in \mathcal{A}$, $v(x) = \min\{n \geq 0 | x \in \mathfrak{p}^n\}$. Thus the last statement holds. □

Corollary 8.19. *($\mathcal{A}$ DVR) then $\mathcal{A}$ is Noetherian.*

Proof. Indeed, every ideal is principal hence finitely generated. □

Corollary 8.20. *$Spec(\mathcal{A}) = \{(0), \mathfrak{p}\}$, $\mathfrak{p} \neq (0)$.*

Corollary 8.21. *$dim(\mathcal{A}) = 1$.*

Corollary 8.22. *$\mathcal{A}$ regular:*

Proof. i.e., $dim_k(\mathfrak{p}/\mathfrak{p}^2) = \dim(\mathcal{A}) = 1$.

$$dim_k(\mathfrak{p}/\mathfrak{p}^2) = \{\text{minimal number of generators of } \mathfrak{p}\}$$

by a corollary of Nakayama lemma 2.19: And it equals to 1 because $\mathfrak{p} = (\varpi)$ □

Corollary 8.23. *$\mathcal{A}$ DVR $\implies$ $\mathcal{A}$ VR $\implies$ $\mathcal{A}$ normal.*

Corollary 8.24. *The set $\{$nonzero $\mathcal{A}$-submodule of $K\}$ forms a group $\cong \mathbb{Z}$. They are of the form $\mathcal{A}\varpi^n, n \in \mathbb{Z}$. $\mathcal{A}\varpi^m \cdot \mathcal{A}\varpi^n = \mathcal{A}\varpi^{m+n}$*

Now, Let $\mathcal{A}$: Noetherian local domain of dimension $\dim(\mathcal{A}) = 1$. DVR gives examples of such $\mathcal{A}$. But there are also Non-DVR examples

$$\mathcal{A} = k[[x^2, x^3]] = \left\{ f = \sum_{i=0}^{\infty} a_i x^i | a_i \in k, a_1 = 0 \right\},$$

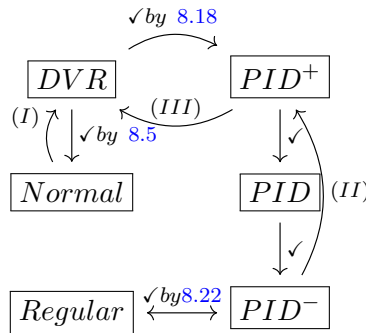$$\mathfrak{m} = (x^2, x^3).$$

because it is not normal, nor regular.

Theorem 8.25. *$(\mathcal{A}, \mathfrak{p})$ is Noetherian local domain with $\dim(\mathcal{A}) = 1$. The following are equivalent.*

- *$\mathcal{A}$ DVR*

- *$\mathcal{A}$ normal*

- *$\mathcal{A}$ PID*

- *$\mathcal{A}$ regular*

We also introduce the some other notions:

- *PID^- : $\mathfrak{p}$ is principal $\exists \varpi \in \mathcal{A}$ s.t $\mathfrak{p} = (\varpi)$.*

- *PID^+ : $\exists \varpi \in \mathcal{A}$ s.t. every nonzero ideal in $\mathcal{A}$ is of the form (ϖ^n), for some $n \geq 0$.*

The interdependence of is the following diagram:

Sublemma 1

$\mathcal{A}$ Noetherian local domain, $\dim(\mathcal{A}) = 1$, $\mathfrak{p} :=$ the maximal ideal, $K := Frac(\mathcal{A})$. Then $\forall x \in K, \exists n \geq 0$ s.t., $x\mathfrak{p}^n \subseteq \mathcal{A}$,

Proof. Write $x = u/v, 0 \neq v \in \mathcal{A}$. It suffices to find $n \geq 0$ s.t., $\mathfrak{p}^n \subseteq (v)$. But $\dim(\mathcal{A}) = 1$ $\mathfrak{p}$ is the only prime that contains (v). $\dim(\mathcal{A}/(z)) = 0$. Then, by 6.12, $\mathcal{A}/(z)$ is local Artinian with maximal ideal $\mathfrak{p}/(z)$ but by 6.19, $\exists n \geq 0$ s.t. $(\mathfrak{p}/(z))^n = 0$. $\exists n \geq 0$ s.t. $\mathfrak{p} \subseteq (z)$. $\qquad\square$

Sublemma 2

$(\mathcal{A}, \mathfrak{p})$ Noetherian local domain $K := Frac(\mathcal{A})$. Let $y \in K$ s.t. $y\mathfrak{p} \subseteq \mathcal{A}$. Then either

(i) $1/y \in \mathfrak{p}$, or

(ii) y integral over $\mathcal{A}$

Proof. If $y\mathfrak{p} = \mathcal{A}$, then $yt = 1$ for some $t \in \mathfrak{p}$, hence $1/y = t \in \mathfrak{p}$. Else $y\mathfrak{p} \subsetneq \mathcal{A}$, so $y\mathfrak{p} \subset \mathfrak{p}$. $\mathcal{A}$ Noetherian, so $\mathfrak{p}$ finitely generated. $\mathfrak{p}$ is a faithful $\mathcal{A}[y]$-module which is finitely generated as $\mathcal{A}$-module, then by 7.2, y is integral over $\mathcal{A}$. $\qquad\square$

Sublemma 3 $\mathcal{A}$ is Noetherian valuation ring $\iff$ $\mathcal{A}$ is a field or $\mathcal{A}$ is a DVR.

Proof.
$(\Longleftarrow), \checkmark$
$(\Longrightarrow)$:
Suppose $\mathcal{A}$ is a Noetherian VR, by definition it is local integral domain. Then $\mathfrak{p} = (\varpi_1, ..., \varpi_n)$.

Let $v : K \longrightarrow G \cup \{\infty\}$ be valuation that determines $\mathcal{A}$. If $\mathcal{A} = K$, then $\mathcal{A}$ is a field. Else $v(K^\times) = K^\times/\mathcal{A}^\times \neq \{0\}$. Recall the construction of the valuation in 8.10, $\exists x \in \mathcal{A}$ s.t. $1/x \notin \mathcal{A}$. So $\mathcal{A}$ contains nonzero non-units, so $\mathfrak{p} \neq (0)$, and $v(\varpi_j) > 0$. Let $g := \min(v(\varpi_1), ..., v(\varpi_n))$. Say $g = v(\varpi_1)$, Then $v(\varpi_j/\varpi_1) \geq 0$, so $\varpi_j \in \mathcal{A}\varpi_1$, so $\mathfrak{p} = (\varpi_1)$. (PID^-)

Now given $x \in \mathcal{A} - \{0\}$. by Krull's intersection theorem 6.23 that $\cap_{n \geq 0}\mathfrak{p}^n = (0)$, we may choose $n \geq 0$, s.t. $x \in \mathfrak{p}^n$, $x \notin \mathfrak{p}^{n+1}$. Thus $\frac{x}{\varpi^n} =: u \in \mathcal{A} - \mathfrak{p} = \mathcal{A}^\times$. So $(x) = \mathfrak{p}^n$, $v(x) = ng$. (PID^+)

Thus $v : K^\times \twoheadrightarrow \mathbb{Z}g \cong \mathbb{Z}$, the second isomorphism because $g \neq 0$. $\qquad\square$

The proof of sublemma 3 also shows

$$PID^- \Longrightarrow PID^+ \Longrightarrow DVR$$

which finishes the (II) and (III) in the diagram (Under the condition that $\mathcal{A}$ is a Noetherian VR).

Proof.

Now it suffices to show that a normal Noetherian local domain $\mathcal{A}$, with $\dim(\mathcal{A}) = 1$ is VR. As we showed in theorem 8.12, there is a VR $(\mathcal{B}, \mathfrak{m})$, with $\mathcal{A} \subseteq \mathcal{B} \subseteq K$ and $\mathcal{A} \cap \mathfrak{m} = \mathfrak{p}$, it suffices to show that $\mathcal{B} = \mathcal{A}$. Here we choose $K = \mathrm{Frac}(\mathcal{A})$.

Let $v : K \longrightarrow G \cup \{\infty\}$ be a defining valuation for $\mathcal{B}$, then $\mathcal{B} = \{x \in K | v(x) \geq 0\}$, $\mathfrak{m} = \{x \in K : v(x) > 0\}$. So $v(\mathfrak{p}) > 0$. Let $x \in \mathcal{B}$. Then $x \in K$, so by sublemma 1, $\exists n \geq 0$ so that $x\mathfrak{p}^n \subseteq \mathcal{A}$. Choose n minimal with this property.

If $n = 0$, then $x \in \mathcal{A}$, so we are done.

Else $n \geq 1$, and $x\mathfrak{p}^{n-1} \not\subseteq \mathcal{A}$, so $\exists y \in x\mathfrak{p}^{n-1}, y \notin \mathcal{A}$. Then $y\mathfrak{p} \subseteq x\mathfrak{p}^n \subseteq \mathcal{A}$, so by Sublemma 2: either $1/y \in \mathfrak{p}$ or y integral over $\mathcal{A}$.

If $1/y \in \mathfrak{p}$, then $v(1/y) = -v(y) > 0$, but $y \in \mathfrak{p}^{n-1}x$ and $v(x) \geq 0$, $v(\mathfrak{p}) > 0$, so $v(y) \geq 0$. contradiction.

If y is integral over $\mathcal{A}$, then since $\mathcal{A}$ is normal, deduce that $y \in \mathcal{A}$, but $y \notin \mathcal{A}$ contraction.   □

8.3   Lecture 27. Dedekind Domain

Definition 8.26. *A **Dedekind domain** $\mathcal{A}$ is a normal Noetherian domain of dimension one. Equivalently, $\mathcal{A}$ is Noetherian domain s.t.*

- *$\mathcal{A}$ is integrally closed in $K = Frac(\mathcal{A})$,*

- *Every nonzero prime is maximal,*

- *$\mathcal{A} \neq K$*

<u>Restatement of Last theorem:</u> A local Dedekind domain is a DVR.

Lemma 8.27. *If $\mathcal{A}$ is a Dedekind domain. Any localization such that $S^{-1}\mathcal{A} \neq K$ is a Dedekind domain. In particular: $\mathcal{A}$ is Dedekind and $Spec(\mathcal{A}) \ni \mathfrak{p} \neq 0$, then $\mathcal{A}_{\mathfrak{p}}$ is Dedekind domain.*

Proof. Just need to check that every condition is preserved by localization. Remains only to check:

Lemma 8.28. *Let $\mathcal{A}$ domain. Then the following are equivalent:*

(i) $\mathcal{A}$ normal

(ii) $\mathcal{A}_{\mathfrak{p}}$ *is normal* $\forall$ *primes* $\mathfrak{p}$

(iii) $\mathcal{A}_{\mathfrak{m}}$ *normal* $\forall$ *maximal ideals* $\mathfrak{m}$

Proof. $K := Frac(\mathcal{A}) = Frac(\mathcal{A}_{\mathfrak{p}})$, $(i) \implies (ii)$ Let $x \in K$ be integral over $\mathcal{A}_{\mathfrak{p}}$:

$$x^n + a_1 x^{n-1} + ... + a_n = 0$$

with each $a_j \in \mathcal{A}_{\mathfrak{p}}$, say $a_j = \frac{b_j}{s_j}$, $b_j \in \mathcal{A}$, $s_j \in \mathcal{A} - \mathfrak{p}$. Set $s := s_1 \cdots s_n \in \mathcal{A} - \mathfrak{p}$. $y := sx \in K$, $x = y/s$, $sa_j \in \mathcal{A}b_j \subseteq \mathcal{A}$. Then

$$y^n + sa_1 y^{n-1} + ... + s^{n-1} a_n = 0$$

with each coefficients in $\mathcal{A}$, so since $\mathcal{A}$ is normal, deduce that $y \in \mathcal{A}$, hence that $x = y/s \in \mathcal{A}_{\mathfrak{p}}$

$(ii) \implies (iii)$✓

$(iii) \implies (i)$✓: Let $x \in K$ be integral over $\mathcal{A}$. Know each $\mathcal{A}_{\mathfrak{m}}$ is normal. So $\forall \mathfrak{m}$: maximal, we may write

$$x^N + a_1 x^{N-1} + ... + a_N = 0$$

for some $N \geq 0$, $a_j \in \mathcal{A}_{\mathfrak{m}}$. $x \in \mathcal{A}_{\mathfrak{m}}$ because $\mathcal{A}_{\mathfrak{m}}$ is normal. Then there exists an $s_{\mathfrak{m}} \in \mathcal{A} - \mathfrak{m}$ s.t. $s_{\mathfrak{m}} x \in \mathcal{A}$. The ideal $\sum_{\mathfrak{m},\text{max'l}} \mathcal{A}s_{\mathfrak{m}} \not\subseteq \mathfrak{m} \forall \mathfrak{m}$, hence $\sum_{\mathfrak{m}} \mathcal{A}s_{\mathfrak{m}} = \mathcal{A} \ni 1$, so $\exists \mathfrak{m}_1, ..., \mathfrak{m}_n, \lambda_1, ..., \lambda_n \in \mathcal{A}$ s.t.,

$$1 = \sum \lambda_j s_{\mathfrak{m}_j}$$

Then $x = x \cdot 1 = \sum_j \lambda_j s_{\mathfrak{m}_j} x$, where $s_{\mathfrak{m}_j} x \in \mathcal{A} \implies x \in \mathcal{A}$. $\qquad\square$

Being normal is a local property, then $S^{-1}(\mathcal{A})$ is normal for a normal ring $\mathcal{A}$ and arbitrary multiplicative set. $\qquad\square$

Lemma 8.29. $\mathcal{A}$ *Dedekind domain* $\iff$ $\mathcal{A}_{\mathfrak{m}}$ *is Dedekind domain* $\forall \mathfrak{m}$.

Example 8.30. *If* $\mathcal{A}$ *is a PID, not a field, then* $\mathcal{A}$ *is Dedekind.*

Proof. PID $\iff$ every ideal principal (finitely generated) $\implies$ Noetherian.

PID $\implies$ UFD $\implies$ normal.

$\forall \mathfrak{m} \in Spem(\mathcal{A})$, $\mathcal{A}_{\mathfrak{m}}$ Noetherian local domain with principal maximal ideal $\implies \dim(\mathcal{A}_{\mathfrak{m}}) \leq 1$ by Krull principal ideal theorem 6.48.

$\dim(\mathcal{A}) \leq sup_{\mathfrak{m}} \dim(\mathcal{A}_{\mathfrak{m}})$. $\mathcal{A}$ not a field then $\mathcal{A} \neq 0$. $\qquad\square$

Theorem 8.31. *Let $\mathcal{A}$ be a normal Noetherian domain, $K := Frac(\mathcal{A})$, L/K is a finite separable field extension. and $\mathcal{B}$ is the integral closure of $\mathcal{A}$ in L. Then $\mathcal{B}$ is finite over $\mathcal{A}$ and is Noetherian.*

as a corollary, because integral extension preserves dimension, we have:

Proposition 8.32. *$\mathcal{A}$ is Dedekind, $K := Frac(\mathcal{A})$, L/K is a finite separable field extension. Then the integral closure $\mathcal{B}$ of $\mathcal{A}$ in L is also Dedekind.*

Corollary 8.33. *Choose the special case $\mathcal{A} = \mathbb{Z}$ and $K = \mathbb{Q}$. The ring of integers (integral closure of $\mathbb{Z}$ in the number field) in any number field (finite field extension over $\mathbb{Q}$) is Dedekind.*

Proof. Reduced the proof to checking that $\mathcal{B}$ is Noetherian. For this, it suffices to show that $\mathcal{B}$ is finitely generated $\mathcal{A}$-module because $\mathcal{A}$ is Noetherian.

Recall (every finite field extension is algebraic) the proof of 7.18, we saw $\exists u_1, ..., u_n \in \mathcal{B}$, a K-basis of L. $\rightsquigarrow$ dual basis $v_1, ..., v_n \in L$, a K-basis for L/K separable. s.t., with

$$T : L \longrightarrow K$$

$$z \longmapsto trace_{L/K}(M_z),$$

where M_z is multiplication by z we have $T(u_i v_j) = \delta_{ij}$. We had used without proof that L/K : Separable $\implies$ the bilinear form $L \times L \ni (x, y) \longmapsto T(xy) \in K$ is non-degenerate.

Sketch of the proof: non-degeneracy means

$$\nexists 0 \neq x \in L, s.t., T(xy) = 0, \forall y \in L$$

$$\iff L \longrightarrow L^* = Hom_K(L, K)$$

$$x \longmapsto [y \mapsto T(xy)]$$

is isomorphism.

Since this system is linear in x, we can extend scalar: it suffices to check $\nexists 0 \neq x \in L \otimes_K K^s$, K^s is the separable closure of K. s.t., $T(xy) = 0 \forall y \in L \otimes_K K^s$. But $L \otimes_K K^s = (K^s)^{[L:K]} \iff L/K$ separable. Hence T is the K^s-linear extension of T

$$T : L \otimes_K K^s \longrightarrow K^s$$

$$t \otimes z \longmapsto T(t)z$$

$\rightsquigarrow$

$$T : (K^s)^{[L:K]} \longrightarrow K^s$$

$$(z_i) \longmapsto \sum z_i$$

s.t. with $T : L \longrightarrow K$, $z \longmapsto trace_{L/K}(M_z)$, we have $T(u_i v_i) = \delta_{ij}$

Claim: $\mathcal{B} \subseteq \oplus_i \mathcal{A} v_i \subseteq \oplus_i K v_i = L$. $\mathcal{A}$ Noetherian $\Longrightarrow \oplus \mathcal{A} v_i$ is Noetherian $\Longrightarrow \mathcal{B}$ is finitely generated $\mathcal{A}$-module $\Longrightarrow \mathcal{B}$ is Noetherian.

Indeed, let $x \in \mathcal{B}$. Write $x = \sum x_i v_i$ with $x_i \in K$.

Want: $x_i \in \mathcal{A} = \mathcal{B} \cap K$.

Indeed,

$$T(x \cdot u_i) = x_i,$$

where $x \cdot u_i \in \mathcal{B}$ and the equality from $T : K$-linear.

Reduce to checking: $T(\mathcal{B}) \subseteq \mathcal{A}$. Case L/K Galois:

$$T(x) = \sum_{\sigma \in Gal(L/K)} x^\sigma$$

Recall that $G(L/K)$ acts on $\mathcal{B}$, $x \in \mathcal{B} \Longrightarrow$ each $x^\sigma \in \mathcal{B}$. $T(x) \in \mathcal{B} \cap K = \mathcal{A}$, the last equality from $\mathcal{A}$ being normal.

For the purpose of proving that $\mathcal{B}$ Noetherian, we can reduce to the Galois case.

$$
\begin{array}{ccc}
\mathcal{B}_1 & \subseteq & L_1 \\
\cup| & & \cup| \\
\mathcal{B} & \subseteq & L \\
\cup| & & \cup| \\
\mathcal{A} & \subseteq & K
\end{array}
$$

There always exists a extension L_1/L such that L_1/K is Galois, and we define the $\mathcal{B}_1$ to be the integral closure of $\mathcal{B}$ in L_1. Our proof the show that $\mathcal{B}_1$ is fin. gen $\mathcal{A}$-module. since $\mathcal{A}$ is Noetherian, conclude that $\mathcal{B}$ is fin.gen. $\mathcal{A}$-module, thus $\mathcal{B}$ is Noetherian.   □

8.4   Lecture 28. Fractional Ideals

Lemma 8.34. *$\mathcal{A}$ Noetherian domain of dimension 1, (every prime ideal is maximal.) Then every nonzero ideal $\mathfrak{a} \subseteq \mathcal{A}$ factor uniquely(up to reordering) as a product of primary ideals with distinct radicals.*

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

where $rad(\mathfrak{q}_i) =: \mathfrak{p}_i \neq \mathfrak{p}_j := rad(\mathfrak{q}_j)$

Proof. <u>Existence</u>: Let $\mathfrak{q} = \cap_i \mathfrak{q}_i$ be a MPD, $\mathfrak{p}_i = \mathrm{rad}(\mathfrak{q}_i)$. Then, since $\mathfrak{a} \neq 0$, know that each $\mathfrak{p}_i \neq 0$, hence the $\mathfrak{p}_i$ are maximal and distinct: $\mathfrak{p}_i + \mathfrak{p}_j = \mathcal{A}, \forall i \neq j$. Hence the $\mathfrak{q}_i$ are pairwise coprime. Hence $\cap \mathfrak{q}_i = \mathfrak{q} = \prod \mathfrak{q}_i$.

<u>Uniqueness</u>: Suppose $\mathfrak{q} = \prod \mathfrak{q}_i$, with $\mathfrak{p}_i \neq \mathfrak{p}_j \forall i \neq j$. Then as before, the $\mathfrak{p}_i \neq 0$, hence maximal and distinct, hence pairwise coprime, hence $\mathfrak{a} = \cap \mathfrak{q}_i$ is a MPD with each component isolated. we conclude by "2nd uniqueness theorem" 5.29 isolated components in a MPD are unique. $\square$

Theorem 8.35. *In a Dedekind domain,*

 (i) *any power of a nonzero prime is primary,*

 (ii) *any nonzero primary is a power of its radical,*

 (iii) *any nonzero ideal is uniquely a product of prime ideals.*

Proof. (i): nonzero prime $\Longrightarrow$ maximal, (dim $=1$). power of maximal ideals are primary.

(ii) True if $\mathcal{A}$ local, because the $\mathcal{A}$ DVR. In general.

$$\{\mathfrak{p}\text{-primary ideals in } \mathcal{A}\} \longleftrightarrow \{\mathfrak{p}\mathcal{A}_\mathfrak{p}\text{-primary idaels in } \mathcal{A}_\mathfrak{p}\}$$

$$= \{\text{non-zerp ideals in } \mathcal{A}_\mathfrak{p}\} = \{\text{powers of } \mathfrak{p}\mathcal{A}_\mathfrak{p}\}$$

(iii)$\Longleftarrow$ (i)+(ii)+Lemma above. $\square$

Definition 8.36. *Let $\mathcal{A}$ domain. A fractional ideal is a submodule $T \subseteq K := Frac(\mathcal{A})$ s.t. $xI \subseteq \mathcal{A}$ for some $0 \neq x \in \mathcal{A}$.*

Example 8.37. *If $I = \mathcal{A}y$ for some $y \in K$, then I is fractional ideal: $y = u/v$, $u, v \in \mathcal{A}$, $v \neq 0$ So $vI = \mathcal{A}u \subseteq \mathcal{A}$. More generally, any finitely generated submodule $I \subseteq K$ is a fractional ideal:*

$$I = \sum_{i=1}^{n} \mathcal{A}y_i, y_i = \frac{u_i}{v_i}.$$

then $v_1, ..., v_n I \subseteq \sum \mathcal{A}u_i \subseteq \mathcal{A}$.

If $\mathcal{A}$ Noetherian and I fractional ideal, then I finitely generated (Pf. $xI \subseteq \mathcal{A}$ for some $0 \neq x \in \mathcal{A} \Longrightarrow xI$ finitely generated, say $xI = \sum \mathcal{A}z_i, z_i \in \mathcal{A}$,then $I = \sum \mathcal{A}\frac{z_i}{x}$)

Definition 8.38.
$$I \cdot J := \{\sum_i a_i b_j : a_i \in I, b_i \in J\}$$

Definition 8.39. *An **invertible ideal** is a submodule $I \subseteq K$ s.t. $\exists$ submodule $J \subseteq K$ s.t., $IJ = A$*

If I is invertible and $IJ = \mathcal{A} \implies J = (\mathcal{A} : I) := \{x \in K : xI \subseteq \mathcal{A}\}$. This is because $J \subseteq (\mathcal{A} : I) = (\mathcal{A} : I)I \cdot J \subseteq \mathcal{A} \cdot J = J$

So invertible ideals form a group.

Theorem 8.40. *$\mathcal{A}$ Dedekind domain. The every nonzero fractional ideal is invertible. The group of nonzero fractional ideal is free on the nonzero primesL*

$$\oplus_{0 \neq \mathfrak{p} \subset \mathcal{A}} \mathbb{Z} \longrightarrow \{nonzero\ fractional\ ideals\}$$

$$(n_\mathfrak{p})_\mathfrak{p} \longmapsto \prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}}$$

Proof. Let I nonzero fractional idael. Thus $xI \subseteq \mathcal{A}$ for some $0 \neq x \in \mathcal{A}$. If $\mathcal{A}$ local, then

$$x = \varpi^n u, n \geq 0$$

$$xI = (\varpi^m), m \geq 0$$

$$\implies I = \mathcal{A}\varpi^{m-n}$$

$$\implies I \text{ invertible}$$

$$\mathbb{Z} \longrightarrow \{\text{invertible ideals } =\} = \{\text{nonzero fractional ideals}\}$$

$$n \longmapsto \mathfrak{p}^n = (\varpi^n)$$

$\square$

In general, we know that $I_\mathfrak{p}$ is invertible $\forall \mathfrak{p} \neq 0$ by the local case just established. But $I \cdot (\mathcal{A} : I) = \mathcal{A} \impliedby (I \cdot (\mathcal{A} : I))_\mathfrak{p} \stackrel{?}{=} \mathcal{A}_\mathfrak{p}$

But $(I \cdot (\mathcal{A} : I))_\mathfrak{p} = I_\mathfrak{p} \cdot (\mathcal{A} : I)_\mathfrak{p} = (\mathcal{A}_\mathfrak{p} \cdot I_\mathfrak{p})$ because I finitely generated. so the general case reduce to the local case.

The last equality is left as an exercise

What is $\mathbb{Z}/3 \otimes \mathbb{Z}_2$?

What is $\text{Spec}(\mathbb{Z}[1/6])$

What is the $\text{Ker}(\mathcal{A} \longrightarrow \mathcal{A}_f)$

Fluent in goingup going down

Characterization of DVR,

nonexample of 1-dim local ring that is not DVR $k[[x^2, x^3]]$

equivalence of defs like radicals

Show that valuation ring is normal.

example of artin local ring which is not a field.

give an example of non-flat module

Going through homework and exercise of A-M.

Eisenbud chap1 motivation.