Personal Notes for Commutative Algebra by Prof. Nelson

Texed by Lin-Da Xiao

December 5, 2017

Contents

About the Course:

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
- Completions
- Basic dimension theory

Prerequisite:

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

Convention: Ring, we mean a commutative ring with identity. 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 algebraic-closed field $\mathbb{K}$ and an integer $n > 0$, consider the ring $R := \mathbb{K}[x_1, ..., x_n]$. Def: For a subset $S \subset R$ we define the **affine algebraic variety** by

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

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

- $V(\emptyset) = \mathbb{K}^n$
- $V(\{1\}) = \emptyset$
- *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* $\mathbb{K}^n$ *called* ***Zariski topology****.*

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

Definition 1.4. *Conversely for all subset* $X \subset \mathbb{K}^n$*, 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* $\mathbb{K}^n$*, 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* $X \subset X' \subset \mathbb{K}^n$*, we have* $I(X) \supset I(X')$
- $I(X) \subset R$ *is an ideal.*

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

Remark 1.7. *Fact, for every ideal* $\mathfrak{a} \subset R$ *we have* $\mathfrak{a} \subset rad(\mathfrak{a})$*.*
$rad(\mathfrak{a})$ *is an ideal, proof in exercise.*
For $X \subset \mathbb{K}^n$ *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

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

and this correspondence inverse the inclusion.

Example 1.9. *For any point $x = (x_1, ..., x_n) \in \mathbb{K}^n$ 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. □

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

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

$$\{\textit{max ideals of } R \textit{ polynomial ring } \mathbb{K}[X_1, ..., X_n]\} \Longleftrightarrow \{\textit{Points in } \mathbb{K}^n\}$$

Let A be a ring. Remember
An element $a \in A$ is **nilpotent** if there $\exists n > 1 \in \mathbb{Z}$ s.t. $a^n = 0$.
An element $a \in A$ is a **zero divisor** if there is an element $b \in A, b \neq 0$ s.t. $ab = 0$.
Fact: every nilpotent element is a zero divisor but not conversely.

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

Definition 1.12. *The ideal $N : rad((0))$ is called the **nil radical** of A.*

Then we have:

1. $\mathcal{N}$ is the set of all nilpotent elements of A

2. $A/\mathcal{N}$ has no nilpotent elements.

Proof. 1. From definitions. 2. Let $x \in A$ s.t. $\bar{x} \in A/\mathcal{N}$ is nilpotent. Let $n > 0$ s.t. $\bar{x}^n = 0$ then $x^n \in \mathcal{N}$ Thus there exists $k > 0$ s.t. $(x^n)^k = 0$ hence $x^{nk} = 0$, $x \in \mathcal{N}$. □

Proposition 1.13. *The nil radical of A is the intersection of all prime ideals of A.*

Proof. Denote by $\mathcal{N}'$ the intersection of all prime ideals of A. For any nilpotent element $f \in A$ with $n > 0$ s.t. $f^n = 0$, We have $f^n \in \mathfrak{p}$ for every prime ideal $\mathfrak{p}$. Hence $f \in \mathfrak{p}$ We conclude $f \in \mathcal{N}'$ Conversely, suppose $f \in A$ 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 $(a_i)_{i \in I} \subset \Sigma$, the set $\mathfrak{a} := \cup_{i \in I} a_i$ 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. $f^n \in (x), f^m \in \mathfrak{p} + (y)$. 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 $f \notin \mathcal{N}'$. □

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

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

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

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

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

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

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

"$\Longleftarrow$" let $x \notin \mathcal{R}$ then $x \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m} \subset A$. 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. □

1.2 Lecture 2. local rings, coprime ideals, ideal quotients by Paul Steinmann

Definition 1.18. *A ring A is called a* ***local ring*** *if 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.*
- $\mathbb{K}[[X]]$ *is the ring of formal power series over a field* $\mathbb{K}$*, 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 A be a ring and* $\mathfrak{m} \neq (1)$ *is an ideal of A s.t. every* $x \in A - \mathfrak{m}$ *is a unit of A, then A is a local ring with maximal ideal* $\mathfrak{m}$*.*
- *Let A be ring and* $\mathfrak{m} \subset A$ *is a maximal ideal s.t. any element of* $1 + \mathfrak{m} = \{1 + a | a \in \mathfrak{m}\}$ *is a unit in A. Then A is a local ring.*

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 $x \in A - \mathfrak{m}$. Since $\mathfrak{m}$ is maximal , we have $(x) + \mathfrak{m} = (1)$, hence , $\exists y \in A, t \in \mathfrak{m}$, 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. □

Definition 1.21. *A ring A is called* ***semilocal*** *if 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 $\mathfrak{a}, \mathfrak{b} \subset A$ 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 $(\mathfrak{a}_i)_{i\in I} \subset A$ ideals,

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

And we also have

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

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

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. *Let $\mathfrak{a}_1, ..., \mathfrak{a}_n \subset A$ be ideals, denote $\varphi : A \to \prod_{i\in I}^n (A/\mathfrak{a}_i)$ 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 $\cap_{i=1}^n \mathfrak{a}_i = (0)$.

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

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

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

(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

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

□

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

Proof. In fact, we have

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

Details in the exercise sheet. □

Proposition 1.27.
(i) Let $\mathfrak{p}_1, ..., \mathfrak{p}_n \subset A$ prime ideals and let $\mathfrak{a} \subset A$ 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 $\mathfrak{a}_1, ..., \mathfrak{a}_n \subset A$ be ideals and $\mathfrak{p} \subset A$ 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. ☐

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

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

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

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

Notation: For $x \in A$ we write $(a : x) := (a : (x))$.
Fact: (i)The ideal quotient of two ideals is again an ideal.
(ii)The set of zero divisors of A is

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

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

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

where we extend rad to arbitrary subsets. ☐

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

Definition 1.29. *Let $\mathfrak{a} \subset A$ be an ideal $f : A \to B$ a ring homomorphism. We define the* ***extension*** *of $\mathfrak{a}$ by f to be the ideal*

$$\mathfrak{a}^e := f_*(\mathfrak{a}) := Bf(\mathfrak{a})$$

, Which is just the ideal in B generated by $f(a)$
For an dieal $\mathfrak{b} \subset B$. 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 1.30. *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. □

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. *$Q \to (h)M \to (f)N \to (g)P$, then for any P, we get*

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

$$g \mapsto g \circ f$$

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. *1. $ker(f) = 0 \iff f$ is injective.*

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

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

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\pi"] & N \\ M/M' \arrow[ur, "\bar{f}"] & \end{tikzcd}$$

commutes. It 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

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

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

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

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.

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

A is finitely generated by 1 however, the ideal $I = (X_1, .., X_n, ...)$ is note finitely generated

Lemma 2.11.

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

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

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

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.

2. $(M_1 + M_2)/M_2 \cong M_1/(M_1 \cap M_2)$

Definition 2.12. *$I \subset A$ ideal; M module $IM = \langle \{ax | a \in I, x \in M\} \rangle \subset M$ as a submodule.*

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

Definition 2.13. *$(M_i)_{i \in I}$ is a family of $\mathcal{A}$-modules*

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

2. *$\oplus_{i \in I} M_i \subset \prod_{i \in I} M_i$ 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 2.14. *An $\mathcal{A}$-module M is called **free** if there exists a set I s.t. M is isomorphic to $\mathcal{A}^{(I)}$.*

Example 2.15.

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,*

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

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

Proposition 2.16. *(Nakayama's lemma)*
M finitely generated $\mathcal{A}$-module, $I \subset$ 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. $\square$

Corollary 2.17. *M fin. gen. $\mathcal{A}$-module, $I \subset$ Jacobson radical , $N \subset M$. If $M = IM + N$, then $M = N$.*

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

$$M/N = 0.$$

$\square$

Corollary 2.18. *$\mathcal{A}$ local ring, $\mathfrak{m} \subset \mathcal{A}$ the maximal ideal. M fin. gen. 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. $\square$

Exact sequence

Definition 2.19.
(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 2.20.

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"* $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ *For instance,*

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

   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*

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

   the exact sequence does not split.

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

Proposition 2.21. *(Snake Lemma) Suppose we have such a commutative diagram, each row is exact,*

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

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

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

is exact.

Proof. Consider the kernels and cokernels with the induced map between them. For notion consideration, we write $Ker(f')$ as K' and $Coker(f')$ as C' and so on. We have the extended commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & K' \arrow[r, "\hat{u}"] \arrow[d, hook, "k'"] & K \arrow[r, "\hat{v}"] \arrow[d, hook, "k"] & K'' \arrow[d, hook, "k''"] & \\
0 \arrow[r] & M' \arrow[r, "u"] \arrow[d, "f'"] & M \arrow[r, "v"] \arrow[d, "f"] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\
0 \arrow[r] & N' \arrow[r, "u'"] \arrow[d, two heads, "q'"] & N \arrow[r, "v'"] \arrow[d, two heads, "q"] & N'' \arrow[r] \arrow[d, two heads, "q''"] & 0 \\
 & C' \arrow[r, "\bar{u}"] & C \arrow[r, "\bar{v}"] & C'' \arrow[r] & 0,
\end{tikzcd}$$

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 $Im(f) \subset Ker(q'' \circ v')$. One can also check that the above diagram is commutative. For example $x \in K'$, we have $f(\hat{u}(x)) = f(u(x)) = u'(f'(x)) = 0 \Longrightarrow \hat{u}(x) \in K$, then we have $u \circ k' = k \circ \hat{u}$.

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

2. Exactness at K
   We easily check that $Im(\hat{u}) \subset Ker(\hat{v})$, 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 $x \in Ker(\hat{v}) = Ker(v) \cap Ker(f)$, then $x \in Im(u) \cap Ker(f)$. $\exists y \in M'$ s.t. $u(y) = x \Longrightarrow f(u(y)) = 0 \Longrightarrow u'(f'(y)) = 0$. Then because u' is injective, $f'(y) = 0 \Longrightarrow y \in K' \Longrightarrow x = \hat{u}(y)$. Then we conclude $Ker(\hat{v}) \subset Im(\hat{u})$, thus $Ker(\hat{v}) = Im(\hat{u})$.

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

5. Construct δ

$$\begin{tikzcd}
0 \arrow[r] & K' \arrow[r, "\hat{u}"] \arrow[d, hook, "k'"] & K \arrow[r, "\hat{v}"] \arrow[d, hook, "k"] & K'' \arrow[d, hook, "k''", "x \mapsto x"'] \arrow[dddll, rounded corners, "\delta"] & \\
0 \arrow[r] & M' \arrow[r, "u"] \arrow[d, "f'"] & M \arrow[r, "v", "\exists y \mapsto x"'] \arrow[d, "f", "y \mapsto f(y)"'] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\
0 \arrow[r] & N' \arrow[r, "u'", "\exists z \mapsto f(y)"'] \arrow[d, two heads, "q'", "z \mapsto {[z]}"'] & N \arrow[r, "v'"] \arrow[d, two heads, "q"] & N'' \arrow[r] \arrow[d, two heads, "q''"] & 0 \\
 & C' \arrow[r, "\bar{u}"] & C \arrow[r, "\bar{v}"] & C'' \arrow[r] & 0,
\end{tikzcd}$$

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 $f''(x) = f''(v(y)) = v'(f(y)) = 0 \implies f(y) \in Ker(v') = Im(u')$. 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** $\delta : K'' \longrightarrow C', x \mapsto [z] = z + Im(f')$. 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 $\tilde{z} + Im(f') = z + Im(f')$. Then we conclude that δ is well defined.

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

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

For the converse inclusion. $\forall x \in Ker(\delta)$, we trace back to the construction of δ, and select the corresponding $y \in M,\ z \in N'$, where $v(y) = x$ and $u'(z) = f(y)$. $\because x \in Ker(\delta), \therefore z \in Im(f')$. $\Longrightarrow \exists w \in M'$ 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 $\tilde{y} \in Ker(f) = K$, we conclude that $\hat{v}(\tilde{y}) = x$, thus $Ker(\delta) \subset Im(\hat{v})$.

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

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

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

□

Example 2.22. *(Application of snake lemma) We have such a commutative diagram, each row is exact. Suppose the middle map is isomorphism.*

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

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 2.23.

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

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

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

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

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 $v^*(f) = f \circ v = 0 \Longrightarrow f(Im(v)) = 0 \Longrightarrow f = 0$ because v is surjective.

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

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "p"] & N \\ M/Ker(v) \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

We know that v induces an isomorphism

$$\begin{tikzcd}
Im(v) = M'' \arrow[dr, bend right, "\bar{v}^{-1}"'] & M \arrow[l, "v"'] \arrow[r, "f"] \arrow[d, "p"] & N \\
& M/Ker(v) \arrow[ul, "\bar{v}"] \arrow[ur, "\bar{f}"'] &
\end{tikzcd}$$

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 $f \in Im(v^*)$

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.

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

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,

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z} \arrow[r, "\times 2"] \arrow[d, "Id"] & \mathbb{Z} \arrow[dl, dashed, "?g"] \\
& \mathbb{Z} &
\end{tikzcd}$$

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 $M'' = Ker(p) = Im(v)$ so v is surjective.

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

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

$$\begin{tikzcd}
M' \arrow[r, "f"] & N = M/Im(u) \\
M \arrow[u, "v"] \arrow[ur, "p"] &
\end{tikzcd}$$

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

The above steps proves the first statement and proof of the second statement is similar. $\square$

Tensor Product

Definition 2.24. *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 2.25. *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 2.26. *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.*

$$\begin{tikzcd}
M \times N \arrow[r, "b"] \arrow[d, "\beta"] & P \\
T \arrow[ur, "\exists! f"'] &
\end{tikzcd}$$

*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 2.27. *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.*

$$\begin{tikzcd} M \times N \arrow[r, "b"] \arrow[d, "f"] & P \\ T \arrow[ur, "\exists! \tilde{b}"'] & \end{tikzcd}$$

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

$$\begin{tikzcd} M \times N \arrow[r, "f'"] \arrow[d, "f"] & T' \arrow[dl, "\exists! k"'] \\ T \arrow[ur, bend right, "\exists! j"'] & \end{tikzcd}$$

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 $P := T$, $b := f$

$$\begin{tikzcd} M \times N \arrow[r, "f"] \arrow[d, "f"] & T \\ T \arrow[ur, "\exists! \tilde{b}"'] & \end{tikzcd}$$

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

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

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 $b: M \times N \to P$, $Ker(\tilde{b}) \supseteq D$.

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 $\bar{g}: M\times N \to C/D = T$. ☐

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 2.28. *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:

$$\begin{aligned} b : M \times (N_1 \oplus N_2) &\to M \otimes N_1 \oplus M \otimes N_2 \\ (m, (n_1, n_2)) &\mapsto (m \otimes n_1, m \otimes n_2). \end{aligned}$$

We can check that b is bilinear, for example

$$\begin{aligned} &b(m + m', (n_1, n_2)) \\ &= ((m + m') \otimes n_1, (m + m') \otimes n_2) \\ &= (m \otimes n_1 + m' \otimes n_1, m \otimes n_2 + m' \otimes n_2) \\ &= (m \otimes n_1, m \otimes n_2) + (m' \otimes n_1, m' \otimes n_2) \\ &= b(m, (n_1, n_2)) + b(m', (n_1, n_2)). \end{aligned}$$

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

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

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

$$\begin{aligned} g_1 : M \otimes N_1 &\longrightarrow M \otimes (N_1 \oplus N_2) \\ (m \otimes n_1) &\longmapsto m \otimes (n_1, 0) \end{aligned}$$

similarly, we can construct

$$\begin{aligned} g_2 : M \otimes N_2 &\longrightarrow M \otimes (N_1 \oplus N_2) \\ (m \otimes n_2) &\longmapsto m \otimes (0, n_2) \end{aligned}$$

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

$$\begin{aligned} &f \circ g(m \otimes n, m' \otimes n_2) \\ &= f(m \otimes (n_1, 0) + m' \otimes (0, n_2)) \\ &= (m \otimes n_1, 0) + (0, m' \otimes n_2) \\ &= (m \otimes n_1, m' \otimes n_2) \end{aligned}$$

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. $\square$

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.

$$\begin{tikzcd}
\mathcal{A}^m \times \mathcal{A}^n \arrow[r, "(e_i^{(1)}, e_j^{(2)}) \longmapsto e_i^{(1)} \otimes e_j^{(2)}"] \arrow[d, "f"] & \mathcal{A}^{\oplus \{e_i^{(1)} \otimes e_j^{(2)}\}} \arrow[dl, "\exists! \tilde{f} \ s.t. \ \tilde{f}(e_{ij}) = a_{ij}"] \\
P &
\end{tikzcd}$$

Remark 2.29. *More generally, we may define the n-fold tensor products $M_1 \otimes ... \otimes M_n$.*

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

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

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

Remark 2.30. ***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 2.31.

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

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 2.32. $\mathcal{A} = \mathbb{Z}$, $M' = 2\mathbb{Z} \subseteq M = \mathbb{Z}$, $N' = \mathbb{Z}/2 = N$, *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

$$\begin{aligned} f : M' &\longrightarrow M \\ g : N' &\longrightarrow N \\ \exists! f \otimes g : M' \otimes N' &:\longrightarrow M \otimes N \\ x \otimes y &\longmapsto f(x) \otimes g(y) \end{aligned}$$

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

$$f : \textit{injective} \implies f \otimes 1_N \textit{ is injective}$$

In other words,

$$M' \subset M \implies \text{“}M' \otimes N \subset M \otimes N\text{”}$$

Example 2.34.

- *$\{0\}$ 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 2.35. *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. $z \in Ker(f \otimes 1_N) \neq 0$. Let N denote $\oplus_i N_i$ and the i-th projection $\pi_i : N \longrightarrow N_i$.

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

$z \neq 0 \implies \exists i \in I$ 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. $\square$

Corollary 2.36. *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. $\square$

Example 2.37. *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 2.38. *(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, $Im(f \otimes 1) \subseteq Ker(g \otimes 1)$ because $(g \otimes 1) \circ (f \otimes 1) = (g \circ f) \otimes 1 = 0$. Then it remains to show

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

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

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

$$\begin{tikzcd}
M'' \otimes N \arrow[r, dashed, "\exists\varphi"] & \frac{M \otimes N}{Im(f \otimes 1)} \\
M'' \times N \arrow[u] \arrow[ur, dashed, "\exists\varphi_0"] & \\
M \times N \arrow[u, "g\times 1"] \arrow[uur, "\varphi_1"'] &
\end{tikzcd}$$

Consider the map φ_1, it is the composition of the canonical projection and the defining map of tensor product. $\varphi_1(x, y) \mapsto x \otimes y + Im(f \otimes 1)$. 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

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

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

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

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

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

and

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

$$\Longrightarrow$$
$$\psi \circ \varphi(x'' \otimes y) = g(x) \otimes y = x'' \otimes y$$
$$\varphi \circ \psi(x \otimes y + Im(f \otimes 1)) = x_1 \otimes y + Im(f \otimes 1) = x \otimes y + Im(f \otimes 1),$$

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

Corollary 2.39. *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. □

Example 2.40. *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 $\mathfrak{a} \hookrightarrow \mathcal{A}$, $\psi : x \otimes m \mapsto xm$. $Im(\psi) = \mathfrak{a}M$ Then by the exactness, we have

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

□

Example 2.41.
$$\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/gcd(m,n)\mathbb{Z}.$$

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 2.40, 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 2.42. *$\mathcal{A}$ a ring, M an $\mathcal{A}$-module, we call M* ***torsion free*** *if $\forall a \in \mathcal{A}$ non-zerodivisor. $m \in M$ $am = 0 \Longrightarrow m = 0$*

Theorem 2.43.

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

Proof. Bosch section 4.2 □

Some other facts about tensor product

Example 2.44. *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*

- $1 \in S$
- $s, t \in S \Longrightarrow st \in S$

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 $\mathcal{A} \times S$:*

$$(a, s) \sim (a', s') \Longleftrightarrow \exists t \in S \ s.t. \ as't = a'st$$

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

Proof. reflectivity and symmetricity are trivial, for the transtivity

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

$$\begin{aligned}
&\Longrightarrow \\
&\exists t \in S : as't = a'st \\
&\exists t' \in S : a's''t' = a''s't' \\
&as''(tt's') = as'ts''t' = a's''t'st = a''s(tt's') \\
&\Longrightarrow (a, s) \sim (a'', s'')
\end{aligned}$$

□

Definition 3.4. *We define $S^{-1}\mathcal{A} : (\mathcal{A} \times S/ \sim)$. 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.

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

$$\begin{aligned} &\frac{a}{b} \cdot \frac{0}{1} \stackrel{?}{=} \frac{0}{1} \\ \iff &\frac{a \cdot 0}{b \cdot 1} \stackrel{?}{=} \frac{0}{1} \\ \iff &\frac{0}{b} \stackrel{?}{=} \frac{0}{1} \\ \iff &\exists t \in S : 0 \cdot 1 \cdot t = 0 \cdot b \cdot t \end{aligned}$$

Remark 3.6. *The above definition does not exclude the possibility that S contains zero. But if $0 \in S$ then we trivially have $\frac{1}{1} = \frac{0}{1}$, 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 to following property*

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

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

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

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

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

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

(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) "$\Longrightarrow$" Suppose $\mathcal{A} \neq \{0\}$, then ι is isomorphism $\iff$ ι 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, $\frac{1}{s} = \frac{c}{1} \Longrightarrow \exists t \in S$, such that $t(s \cdot c - 1) = 0$, and by the

fact S has no zero divisors $s \cdot c = 1$, which means $S \subseteq \mathcal{A}^\times$.
"$\Longleftarrow$" Assume $\mathcal{A} \neq \{0\}$. $S \subseteq \mathcal{A}^\times$, then S does not contain any zero divisors. $\forall \frac{a}{s} \in S^{-1}\mathcal{A}, \exists v \in S$ s.t. $sv = 1$. Then $\frac{a}{s} = \frac{av}{1} \in Im(\iota)$, 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. *Let $B := \{functions\ U \longrightarrow \mathbb{R}\}$. Then the natural map $j : S^{-1}\mathcal{A} \longrightarrow B$ 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 $k : B \longrightarrow S^{-1}\mathcal{A},\ b \longmapsto \tilde{b}/1$, where

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

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

$j \circ k = 1$, $b \in B$ $\frac{\tilde{b}(x)}{1(x)} = b(x) \forall x \in U$
$k \circ j = 1$ Say $b = j(\frac{a}{s})$, 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 $1 \in U$ and 0 for $x \notin U]$ $\square$

Universal property of localization

Recall $Hom(M \otimes N, P) \cong \{bilinear M \times N \longrightarrow P\}$ and $Hom(\oplus_i M_i, N) \cong \prod_i Hom(M_i, N)$.

Lemma 3.10. *$Hom(S^{-1}\mathcal{A}, \mathcal{B}) \cong \{f : \mathcal{A} \longrightarrow \mathcal{B}$ s.t. $f(S) \subseteq \mathcal{B}^\times\}$ where 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. 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* $\iota : \mathcal{A} \longrightarrow S^{-1}\mathcal{A} : a \mapsto \frac{a}{1}$*.*

$$\begin{tikzcd}
S \arrow[r, hook] & \mathcal{A} \arrow[r, "f"] \arrow[d, "\iota"] & \mathcal{B} \\
 & T \arrow[ur, "\exists ! \tilde{f}"'] &
\end{tikzcd}$$

This universal property of localization can serve as an alternative definition of localization. $S^{-1}\mathcal{A}$ *is defined to be a pair* (T, ι)

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 $f(t) \in \mathcal{B}^\times \Longrightarrow f(a)f(s') - f(a')f(s) = 0$ □

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* $\mathcal{A} - \mathfrak{p}$ *is multiplicatively closed (By the definition of prime ideals). We can define (In fact then* $\mathcal{A} - \mathfrak{p}$ *is multiplicatively closed is equivalent to* $\mathfrak{p}$ *is prime)* $\mathcal{A}_\mathfrak{p} := S_\mathfrak{p}^{-1}\mathcal{A}$

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 (1.29) 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** $\Longrightarrow \varphi^*(\mathfrak{q})$ **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 $\mathfrak{a} \subseteq \mathcal{A}$*,* $\iota_*(\mathfrak{a}) = \{a/s | a \in \mathfrak{a}, s \in S\}$ *and*

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

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

(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. Notice that $\mathfrak{q} \cap \{\frac{a}{1} | a \in \mathcal{A}\}$ is not necessarily an ideal in $S^{-1}\mathcal{A}$.The explicit presentation of ι^* and ι_* shows that they preserve the proper inclusion "$\subsetneq$"

(c) $\iota_*(\mathfrak{a}) = S^{-1}\mathcal{A} \Longleftrightarrow \exists a \in \mathfrak{a}, s \in S$ s.t. $a/s = 1/1 \Longleftrightarrow \exists t \in S$ 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 1.30, $\iota_*(\iota^*(\mathfrak{b})) \subset \mathfrak{b}$ 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 $a \in \iota^*(\mathfrak{b}) \Longrightarrow a/s \in \iota_*(\iota^*(\mathfrak{b}))$.

□

3.2 Lecture 8: Properties of localization of rings and localization of module

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

- $\iota_*(\mathfrak{a}) = \{\frac{a}{s} | a \in \mathfrak{a}, s \in S\}$
- $\iota_*\iota^*(\mathfrak{b}) = \mathfrak{b}, \forall \mathfrak{b} \subseteq S^{-1}\mathcal{A}$
- $\iota_*\mathfrak{a} = (1) \Longleftrightarrow \mathfrak{a} \cap S \neq \emptyset$

Proposition 3.13. *S is a multiplicative set in a ring $\mathcal{A}$, then for the canonical morphism $\iota : \mathcal{A} \longrightarrow S^{-1}\mathcal{A}$:*

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

is bijection with the inverse ι^*.

Proof. The proof contains the following points

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

(b) $\iota^*\iota_*\mathfrak{p} = \mathfrak{p}$,

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

(d) $\iota_*\iota^*\mathfrak{q} = \mathfrak{q}$ (true for any $\mathfrak{q}$, not necessarily prime),

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

See Proposition 1.30, $\iota^*\iota_*\mathfrak{p} \supseteq \mathfrak{p}$ is a general fact. For the converse inclusion, $\iota^*\iota_*\mathfrak{p} = \iota^{-1}(\iota_*\mathfrak{p}) \overset{?}{\subseteq} \mathfrak{p}$, choose an $a \in \iota^{-1}(\iota_*\mathfrak{p})$, $\iota(a) = \frac{a}{1} \in \iota_*\mathfrak{p} \Longrightarrow \exists b \in \mathfrak{p}, s \in S$ s.t. $\frac{a}{1} = \frac{b}{s} \Longrightarrow ast = bt \in \mathfrak{p}$ and $s, t \in S \subseteq \mathcal{A} - \mathfrak{p} \Longrightarrow a \in \mathfrak{p}$ because $\mathfrak{p}$ is a prime ideal.

$\mathfrak{p}$ prime $\overset{?}{\Longrightarrow} \iota_*\mathfrak{p}$ 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 $uv \in S$ $cstv \in \mathfrak{p}$, $uv \notin \mathfrak{p} \Longrightarrow ab \in \mathfrak{p} \Longrightarrow$ at least one of $a, b \in \mathfrak{p} \Longrightarrow$ at least one of $\frac{a}{s}, \frac{b}{t} \in \iota_*\mathfrak{p}$. □

With the one to one correspondence, we can see that ι^* and ι_* preserve the inclusion, whats more, they preserve "$\subsetneq$"

- $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \Longleftrightarrow \iota^*\mathfrak{q}_1 \subseteq \iota^*\mathfrak{q}_2$
- $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \Longleftrightarrow \iota_*(\mathfrak{p}_1) \subseteq \iota_*(\mathfrak{p}_2)$.

Definition 3.14. *$k(\mathfrak{p}) := Frac(\mathcal{A}/\mathfrak{p})$ 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 $S^{-1}\mathcal{A}/\mathfrak{q}$.

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

$\iota_*\iota^*\mathfrak{q} = \mathfrak{q} \Longrightarrow Ker(\bar{\iota}) = 0 + \iota^*\mathfrak{q}$. And see for example this stack exchange 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 3.15. *$\mathcal{A} = \mathbb{Z}$, 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 3.16. $\mathfrak{p} = (y) \subseteq \mathcal{A} = \mathbb{C}[x,y]$, $\mathcal{A}/\mathfrak{p} \cong \mathbb{C}[x], k(\mathfrak{p}) \cong \mathbb{C}(x)$

Example 3.17. *$S = S_f = \{f^n : n \geq 0\} \Longrightarrow S^{-1}\mathcal{A} = \mathcal{A}_f = \mathcal{A}[1/f]$. Let $\mathfrak{p} \cap S \neq \emptyset \Longleftrightarrow$ 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 3.18. $\mathcal{A} = \mathbb{Z}$, $f = 2$, $\mathcal{A}_f = \mathbb{Z}[1/2]$

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

Example 3.19. *$\mathcal{A} = \mathbb{C}[x,y]$, 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

$$\begin{aligned}
&\{maximal\ ideals\ in\ \mathcal{A}_f = \mathbb{C}[x,f,1/f]\}\\
&\xleftrightarrow{bij} \{maximal\ ideal\ \mathfrak{m} \in \mathbb{C}[x,y] s.t. f \notin \mathfrak{m}\}\\
&\xleftrightarrow{bij} \big\{(X,Y) \in \mathbb{C}^2 | f(X,Y) \neq 0\big\}
\end{aligned}$$

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.

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

$$\begin{tikzcd}
\mathcal{A} \arrow[r] \arrow[rr, bend right] & \mathcal{A}_f \arrow[r] & \mathcal{A}_{fg}
\end{tikzcd}$$

Example 3.20. *$\mathcal{A}$ an integral domain, $\mathcal{A}_f \subseteq \mathcal{A}_{fg}$ $(\frac{a}{(f)^n} = \frac{ag^n}{(fg)^n})$, $Frac(\mathcal{A}) = \cup_f \mathcal{A}_f$. For any $\mathfrak{p} \in Spec(\mathcal{A}_f) \subseteq Spec(\mathcal{A})$, $\mathcal{A}_f \Longrightarrow k(\mathfrak{p})$*

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

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, $\iff \mathcal{A} - \mathfrak{m} \subseteq \mathcal{A}^\times$

$\mathfrak{p} \subseteq \mathcal{A}$ prime $\implies \mathcal{A}_\mathfrak{p} := S_\mathfrak{p}^{-1}\mathcal{A}$

Proposition 3.21.

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

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

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

Proof. By Proposition 3.13,

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

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. □

Example 3.22. $\mathfrak{p} = (p) \subseteq \mathbb{Z} = \mathcal{A}$, *then* $\mathcal{A}_\mathfrak{p} = \mathbb{Z}_{(\mathfrak{p})}$ *is local ring with maximal ideal* $\mathfrak{p}_\mathfrak{p}$ *generated by image of* $\mathfrak{p}$. $\mathit{Spec}(\mathbb{Z}_{(\mathfrak{p})}) \cong \{\mathfrak{q} \in \mathit{Spec}(\mathbb{Z}) | \mathfrak{q} \subseteq \mathfrak{p}\} = \{(0), (p)\})$

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 3.23. *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 3.24. $\Omega \subseteq \mathbb{C}$ *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. Want $\mathcal{A} - \mathfrak{p} \subseteq \mathcal{A}^\times$

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. □

Example 3.25. $\mathcal{A} = \mathbb{C}[x,y], \mathfrak{p} = (y)$

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

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

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

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

localization of module

Definition 3.26. $S \subseteq \mathcal{A}$ *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 3.27. $S^{-1}\mathcal{A} \otimes_{\mathcal{A}} M \cong S^{-1}M$, *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 3.28. *Given* $f : M \longrightarrow N$ *a morphism of* $\mathcal{A}$*-module.* S^{-1}. *We define*

$$\begin{aligned} S^{-1}f : & S^{-1}M \longrightarrow S^{-1}N \\ & \frac{m}{s} \longmapsto \frac{f(m)}{s}. \end{aligned}$$

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: Localization of Modules and Noetherian Rings

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 $Ker(S^{-1}g) \supseteq Im(S^{-1}f)$. For the converse inclusion, consider an element $\frac{x}{s} \in Ker(S^{-1}g)|x \in Ms \in S$, $S^{-1}g(\frac{x}{s}) = \frac{g(x)}{s} = \frac{0}{1}, \implies \exists t \in S \; s.t. \; g(tx) = tg(x) = 0$. $Im(f) = Ker(g) \implies \exists y :$ $f(y) = tx$. 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. ∎

Corollary 3.29. *$S^{-1}\mathcal{A}$ 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

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

∎

Lemma 3.30. *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,

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

□

Local Properties

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

Lemma 3.31. ***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 $x \neq 0 \iff Ann(x) := \{a \in \mathcal{A} | ax = 0\} \neq (1)$

Proof. $x \neq 0 \iff 1 \cdot x \neq 0 \iff 1 \notin Ann(x) \iff Ann(x) \neq (1)$ □

Calim2: $\mathfrak{m}$ maximal $x \in M$. Then $x \notin Ker(M \longrightarrow M_{\mathfrak{m}}) \iff \mathrm{Ann}(x) \subseteq \mathfrak{m}$.

Proof. $x \in Ker(M \longrightarrow M_{\mathfrak{m}}) \iff \exists s \in \mathcal{A} - \mathfrak{m}$ s.t. $\frac{x}{1} = \frac{0}{s}, \exists t \in \mathcal{A} - \mathfrak{m} : tsx = 0$ $\iff \mathrm{Ann}(x) \nsubseteq \mathfrak{m}$.

□

Proof. (of Lemma 3.31). 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,
$\Longrightarrow Ann(x) \neq (1) \Longrightarrow \exists$*maxmal ideal* $\mathfrak{m} \supseteq \mathrm{Ann}(x)$. Then by Claim 2,
$x \notin \mathrm{Ker}(M \longrightarrow M_{\mathfrak{m}}) \Longrightarrow M_{\mathfrak{m}} \neq 0$ □

Proposition 3.32. ***(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 3.31
$\Longleftrightarrow K_{\mathfrak{p}} = 0 \forall \mathfrak{p}$
$\Longleftrightarrow \phi_{\mathfrak{p}}$ 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 $0 \longrightarrow Ker(\phi) \longrightarrow M \xrightarrow{\phi} N$ □

Proposition 3.33. ***(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 $N \hookrightarrow P$, want $N \otimes M \hookrightarrow P \otimes M \Longleftrightarrow (N \otimes M)_{\mathfrak{m}} = (N_{\mathfrak{m}} \otimes_{\mathcal{A}_{\mathfrak{m}}} M_{\mathfrak{m}}) \hookrightarrow P_{\mathfrak{m}} \otimes_{\mathcal{A}_{\mathfrak{m}}} M_{\mathfrak{m}} = (P \otimes M)_{\mathfrak{m}} \forall \mathfrak{m}$
$\Longleftarrow N_{\mathfrak{m}} \hookrightarrow P_{\mathfrak{m}} \forall \mathfrak{m}$
$\Longleftrightarrow N \hookrightarrow P$ by Proposition 3.32. □

Definition 3.34. ***(Lemma)***

(a) $\mathcal{A}$ satisfies the ***ascending chain condition on ideals*** *(All the sequence $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots$ 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. $\forall \mathfrak{b} \in S \Longrightarrow \mathfrak{b} \not\supset \mathfrak{a}$*

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

Proof. (a)$\Longrightarrow$(b). Let $\mathfrak{a}$ ideal. we may assume that $\mathcal{A}$ is **NOT** finitely generated. Inductively construct $x_1, x_2, x_3... \in \mathfrak{a}$ such that $(x_1) \neq 0$ and $\mathfrak{a} \supsetneqq (x_1, x_2) \supsetneqq (x_1)$ an also $\mathfrak{a} \supsetneqq (x_1, x_2, x_3) \supsetneqq (x_1, x_2)$, 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 $\mathfrak{a}_{j+1} \supsetneq \mathfrak{a}_j, \forall j \in \mathcal{N}$ 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 $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq ...$ Want to show that $\exists n_0, \mathfrak{a}_n = \mathfrak{a}_{n_0} \forall n \geq n_0$ $\mathfrak{a} := \cup_n \mathfrak{a}_n$. 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 $x_1, ..., x_r \in \mathfrak{a}_{n_0} \Longrightarrow \mathfrak{a} = \mathfrak{a}_{n_0}$. $\Longrightarrow \mathfrak{a}_n = \mathfrak{a}_{n_0}, \forall n \geq n_0$. □

Definition 3.35. ***(Lemma)***
M is an $\mathcal{A}$-module. The followings are equivalent:

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

(b) *Every submodule of M s 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 $\Longleftrightarrow$ $\mathcal{A}$ is a Noetherian $\mathcal{A}$-module.

Lemma 3.36. *Let $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ be a short exact sequence of $\mathcal{A}$-modules. Then M is Noetherian $\Longleftrightarrow$ both M', M'' Noetherian.*

Proof. $\Longleftarrow$,Use ACC. Let $N_1 \subseteq N_2 \subseteq ...$ be submodules of M. Want to 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)

$$\begin{tikzcd}
0 \arrow[r] & N'_i \arrow[r] \arrow[d, equal] & N_i \arrow[r] \arrow[d] & N''_i \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & N'_j \arrow[r] & N_j \arrow[r] & N''_j \arrow[r] & 0
\end{tikzcd}$$

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**(See part of proof of Corollary 3.38). □

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

Theorem 3.37. *(Hilbert basis theorem) $\mathcal{A}$ Noetherian $\Longrightarrow$ $\mathcal{A}[X]$ is Noetherian.*

Corollary 3.38. *$\mathcal{A}$ Noetherian $\Longrightarrow \mathcal{A}[x_1, ..., x_n]$ Noetherian $\mathcal{A}[x_1, ..., x_n]/\mathfrak{a}$ Noetherian $\forall \mathfrak{a} \subseteq \mathcal{A}[x_1, .., x_n]$*

Proof. **of Theorem 3.37** Let $\mathfrak{a} \subseteq \mathcal{A}[x]$. We want to show $\mathfrak{a}$ finitely generated. Consider the ideal $\mathcal{L} \subseteq \mathcal{A}$ generated by leading coefficients of elements of $\mathfrak{a}$ i.e. for an element $ax^n + ... \in \mathfrak{a}, a \in \mathcal{L}$ Then $\mathcal{A}$ is Noetherian, $\mathcal{L}$ is finitely generated, $\Longrightarrow \mathcal{L} = (t_1, ..., t_r), t_i \in \mathcal{L}\ \exists f_1, ..., f_r \in \mathfrak{a} : f_j = t_j x^{n_j} + ...$ 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 $\Longrightarrow \mathcal{A}^n$ 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 3.36 and induct on n.

And finally, we claim that

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

The $\subseteq$ part is obvious.

The remaining part of the proof is left till the next lecture. □

4 Noetherian Ring and Nullstellensatz

4.1 Lecture 10

Recall:

Theorem 4.1. *$\mathcal{A}$ Noetherian $\implies \mathcal{A}[x]$ Noetherian.*

Proof. $\mathfrak{a} \subseteq \mathcal{A}[x]$ want to show that $\mathfrak{a}$ is finitely generated.

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

Because $\mathfrak{a}$ is Noetherian, $\mathfrak{a}'$ is finitely generated.
Let $f \in \mathfrak{a}$ with $f = ax^n + ...$, where $n \geq (n_1, ..., n_r)$.

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

Last time : we constructed $M_n := \oplus_{j=0}^{n} \mathcal{A}x^j \cap \mathfrak{a}$ is finitely generated $\mathcal{A}$-module. M_N is finitely generated. If we iterated it for $n, n-1, ..., N$, $\implies \mathfrak{a} \subseteq (f_1, ..., f_r) + M_N \subseteq \mathfrak{a}$, then the equality holds and $\mathfrak{a}$ is finitely generated. $\square$

Applications:

- $\mathcal{A}[x_1, ..., x_r]/\mathfrak{a}$ 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 $\mathfrak{a} = \langle S \rangle$. By Hilbert basis theorem $\implies \mathfrak{a}$ finitely generated $\iff \mathfrak{a} = (f_1, ..., f_r)$ $\square$

Non-Example:
$\mathcal{A} = \mathbb{C}[x_1, x_2, ...]$ 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: $\Longrightarrow x_n \notin \langle S \rangle, x_n \in \mathfrak{m}$

Lemma 4.2. *$\mathcal{A}$ Noetherian $\Longrightarrow$ 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 $\mathcal{A}\}$ and $\{$ ideals in $\mathcal{A}/\mathfrak{a}\}$. The maximal condition also holds in $\mathcal{A}\mathfrak{a}$ $\square$

Lemma 4.3. *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. There is a one to one inclusion preserving correspondence between $\{$ideals in $\mathcal{A}\}$ and $\{$ideals in $S^{-1}\mathcal{A}\}$. Then the maximal property is also inherited to $S^{-1}\mathcal{A}$ $\square$

Definition 4.4. *An $\mathcal{A}$-**algebra** is a ring $\mathcal{B}$ together with a homomorphism $f : \mathcal{A} \longrightarrow \mathcal{B}$.*

Example 4.5. *$\mathcal{A}[x_1, ..., x_n]$ is an $\mathcal{A}$-algebra, with the obvious choice of f.*

Example 4.6.

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

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

Example 4.7. *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 4.8. *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 4.9. *WE say that an $\mathcal{A}$-algebra $\mathcal{B}$ is a finitely generated $\mathcal{A}$-algebra is there exists $x_1, ..., x_n \in \mathcal{B}$ s.t. $\mathcal{B}$ is generated by $f(\mathcal{A}), x_1, .., x_n$. By the Hilbert basis theorem, we know if $\mathcal{A}$ is Noetherian, the finitely generated $\mathcal{A}$-algebra $\mathcal{B}$ is Noetherian.*

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

$$\begin{tikzcd} \mathcal{B} \arrow[r] & \mathcal{C} \\ \mathcal{A} \arrow[u] \arrow[ur] & \end{tikzcd}$$

Now we come back to the proof of the statement

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, then we have $\mathcal{B}$ is Noetherian. □

Definition 4.10. *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.*

¿¿¿¿¿¿¿¿¿1

Example 4.11.

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

Theorem 4.12. *Assume $\mathbb{K}$a field $\mathbb{K} \subseteq \mathbb{L}$, where $\mathbb{L}$ is also a field. Assume $\mathbb{L}$ is a finitely generated $\mathbb{K}$-algebra. Then $\mathbb{L}$ is a finite $\mathbb{K}$-algebra $\Longleftrightarrow \mathbb{L}/\mathbb{K}$ is a finite field extension.*

Corollary 4.13. *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. Thm $\Longrightarrow$ Cor, Let $\mathfrak{m} \subseteq \mathcal{A}$ be any maximal ideal, then $\mathbb{L} = \mathcal{A}/\mathfrak{m}$ is a field.

$$\begin{tikzcd} \mathbb{C} \arrow[r] \arrow[rr, bend right, "j"'] & \mathbb{C}[x_1, ..., x_d] = \mathcal{A} \arrow[r, two heads, "q"] & \mathbb{L} = \mathcal{A}/\mathfrak{m} \end{tikzcd}$$

Note: $\mathbb{L}$ is a finitely generated $\mathbb{C}$-algebra, generated by $q(x_1), ..., q(x_d)$

$$\begin{aligned} Thm &\Longrightarrow \mathbb{L}/j(\mathbb{C}) \text{ is finite field extension} \\ &\Longrightarrow \mathbb{L} \cong \mathbb{C}(\mathbb{C} \text{ algebraically closed}) \end{aligned}$$

Set $X := (j^{-1}(q(x_1)), ..., j^{-1}(q(x_d))) \in \mathbb{C}^d$. Check $\mathfrak{m} = \mathfrak{m}_X$ ◻

Corollary 4.14. *Let $d \geq 1$. Then $\mathbb{C}(x_1, ..., x_d)$ is **NOT** a finitely generated $\mathbb{C}$-algebra.*

Proof. $\mathbb{K} = \mathbb{C}, \mathbb{L} = \mathbb{C}(x_1, .., x_d)$, then $\mathbb{L}/\mathbb{K}$ NOt finite (by thm) $\Longrightarrow$ $\mathbb{L}$ is NOT finitely generated $\mathbb{C}$-algebra.

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

Alternatively, we can also prove this directly, Let $f_1, .., f_n \in \mathbb{K}(x_1, .., x_d)$, each $f_i = \frac{g_i}{h_i} \in \mathbb{C}[x_1, ..., x_d]$. Set $u := 1 + x_1 h_1 \cdot h_n$ ¿¿¿¿¿¿.? $\Longrightarrow 1/u \notin \mathbb{K}[f_1, .., f_n]$ because denominator is coprime to the denominators of the f_j. ◻

Then we come back to the proof of the Theorem 4.12

Proof. Any $\mathbb{L}$ generated by $x_1, ..., x_n$. Any $\mathbb{L}/\mathbb{K}$ NOT finite. Then the transcendence degree d is larger than 1 $\Longleftrightarrow$ after reordering $x_1, ..., x_n$, $x_1, ..., x_d$ algebraically independent over $\mathbb{K}$ and $x_{d+1}, ..., x_n$ is algebraic over $\mathbb{K}(x_1, ..., x_d)$ ¿¿¿¿¿¿¿¿¿¿¿2 ◻

4.2 Lecture 11

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

Theorem 4.15. *$S \subseteq V$, vector space over $\mathbb{F}$.*

*(a) Suppose S is linear independent. Then S is **maximal**$\Longleftrightarrow$ 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 $\{s_1, ..., s_n\} \subseteq S$, $\forall p \in F[X_1, ..., X_n]$ $p(s_1, ..., s_n) = 0 \Longrightarrow p = 0$.

Theorem 4.16. *E/F field extension.*

(a) Suppose $S \subseteq E$ is algebraic independent. Then S is maximal $\Longleftrightarrow$ $E/F(S)$ 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) “$\Longrightarrow$” Assume S maximal algebraic independent. Want: $E/F(S)$ 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 $s_1, ..., s_n$. 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 $p_m \neq 0 \Longrightarrow [F(\alpha, s_1, ..., s_n) : F(s_1, ..., s_n)] \leq m \Longrightarrow \alpha$ is algebraic over $F(S)$.

“$\Longleftarrow$”, If $E/F(S)$ is algebraic, Want 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 $S \cap \{\alpha\}$

□

Example 4.17.
$tr.deg(\overline{\mathbb{Q}}/\mathbb{Q}) = 0$
$tr.deg(\mathbb{C}/\mathbb{Q}) = \infty$
$tr.deg(F(t_1, ..., t_n)/F) = n$
If $E/F(t_1, ..., t_n)$ is algebraic, then $tr.deg(E/F)$ is n
$tr.deg(F/F) = 0 \Longleftrightarrow (E/F)$ is algebraic.

And then we resume our goal in last lecture. Give a field extension L/K such that L is finitely generated as K-algebra, then L/K is finite.

Proof. Write, $L = \langle x_1, ..., x_n \rangle_{K-alg}$. $r := tr.deg(L/K)$. Conclusion $\Longleftrightarrow r = 0$. Suppose not. Then $r \geq 1$. By part (f) of the Theorem 4.16 that after relabeling, $\{x_1, ..., x_r\}$ is a transcendence basis of L/K. Each $x_{r+1}, ..., x_n$ is algebraic over $K(x_1, .., x_r) =: M \Longrightarrow L/M$ is finite. ¿¿¿¿¿¿¿¿¿¿¿1

Lemma 4.18. *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.*

Proof. (Of Lemma) $C = \langle y_1, ..., y_m \rangle_{\mathcal{B}-mod}$ and $C = \langle x_1, ..., x_n \rangle_{\mathcal{A}-alg}$ write $x_i = \sum_j b_{ij} y_j$ for some $b_{ij} \in \mathcal{B}$. $y_i \cdot y_j = \sum_k b_{ijk} y_k$. $\mathcal{B}_0 := \mathcal{A}[\{b_{ij}\} \cup \{b_{ijk}\}] \subseteq \mathcal{B}$. $\mathcal{B}_0$ finitely generated $\mathcal{A}$-algebra $\Longrightarrow$(Hilbert basis theorem) $\mathcal{B}_0$: Noetherian, $\mathcal{C} = \{$polynomials in $\{x_j\}$ with coefficients in $\mathcal{A}\}$ and by substitution if equals $\{$linear combinations of y_i with coefficients in $\mathcal{B}_0\} \Longrightarrow \mathcal{C}$ is a finite $\mathcal{B}_0$-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 □

□

Relation to Nullstellensatz $rad(\mathfrak{a}) = I(V(\mathfrak{a}))$, where $K = \overline{K}$ field. $\mathfrak{a} \subseteq K[t_1, ..., t_d] = \mathcal{A}$. $V(\mathfrak{a}) : \{X \in K^d, f(X) = 0 \forall f \in \mathfrak{a}\}$. $I(S) = \{f \in \mathcal{A} : f(X) = 0 \forall X \in S\}$ and $rad(\mathfrak{a}) = r(\mathfrak{a}) = \{f \in \mathcal{A} : f^n \in \mathfrak{a}$ for some $n\}$

Proof. $r(\mathfrak{a}) \subseteq I(V(\mathfrak{a}))$, $f \in r(\mathfrak{a}) \Longrightarrow f^n \in \mathfrak{a} \Longrightarrow f^n|_{V(\mathfrak{a})=0}$, 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 $r(\mathfrak{a}) = \cap_{\mathfrak{p} \ni \mathfrak{a}, prime} \mathfrak{p}$. suppose $f \notin r(\mathfrak{a})$. Want: $f \notin I(V(\mathfrak{a}))$.Choose $\mathfrak{p} \subseteq \mathfrak{a}, \mathfrak{p} \not\ni f$. Then $0 \neq \overline{f} \in \mathcal{A}/\mathfrak{p}$. $\Longrightarrow (\mathcal{A}/\mathfrak{p})_{\overline{f}} = (\mathcal{A}/\mathfrak{p})[\frac{1}{f}] \neq 0$. 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 t_j in L. Check that $f(X) \neq 0, X \in V(\mathfrak{a}) \Longrightarrow f \notin I(V(\mathfrak{a}))$. □

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 zerodivisor in $\mathcal{A}/\mathfrak{q}$ is nilpotent.*

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

$$\text{prime} \Longrightarrow \text{primary}$$

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

Definition 5.2. *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 5.3. *$\mathcal{A}$ is Noetherian, $\Longrightarrow$ 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 "$n \in S \Longrightarrow n+1 \in S$)"
$\Longrightarrow S = \mathbb{N}$
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) $\forall \mathfrak{a} : [\mathfrak{b} \supsetneq \mathfrak{a} \Longrightarrow \mathfrak{b} \in S] \Longrightarrow [\mathfrak{a} \in S]$
Then $S = \{\text{ideals in } \mathcal{A}\}$

5.1 Lecture 12

Lemma 5.4. *$\mathcal{A}$ is Noetherian, $\mathfrak{a} \subseteq \mathcal{A}$ is an ideal. $\Longrightarrow$ $\mathfrak{a}$ 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 $\Longleftrightarrow xy \in \mathfrak{q} \Longrightarrow x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some n*

Proof. Define: An ideal r is **irreducible** if whenever $r = r' \cap r''$, we have either $r = r'$ or $r = r''$. NOtice $(6) = (2)(3)$ is not irreducible.
Claim1: $\mathcal{A}$ Noetherian. Then irreducible $\Longrightarrow$ primary.

Proof of Claim1

Let $\mathfrak{a}$ irreducible. Let $x, y \in \mathcal{A}$ with $xy \in \mathfrak{a}$. Assume $x \notin \mathfrak{a}$. Want $\exists n, y^n \in \mathfrak{a}$. 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 $Ann(y^n)$. Theses ideals goes up as n increases $\Longrightarrow$, $Ann(y^n) = Ann(y^{n+1})$ for some n because $\mathcal{A}$ is Noetherian. Then we know, $xy = 0$, $x \in Ann(y)$, $(x) \subseteq Ann(y)$.
subclaim: $Ann(y) \cap (y) = 0$.
Assuming the subclaim,(since (0) is irreducible) deduce that either $Ann(y) = (0) \Longrightarrow x \in (0)$ or $(y^n) = (0) \Longrightarrow y^n = 0$. Now we turn to prove the subclaim: Let $z \in Ann(y) \cap (y^n)$. Then $z = y^n t, t \in \mathcal{A}$ and $zy = 0 \Longrightarrow ty^{n+1} = 0 \Longrightarrow t \in Ann(y^{n+1}) = Ann(y^n) \Longrightarrow z = ty^n = 0$. This finishes the proof of subclaim thus also the proof of Claim1.

Calim2: $\mathcal{A}$ Noetherian, $S :=$ {ideals in $\mathcal{A}$ that are finite intersection of irreducible *ideals*} $\Longrightarrow S =$ {ideals in $\mathcal{A}$}.
Proof of Claim2: Consider the complement $S^c =${idaels in $\mathcal{A}$ that are not finite intersections of irreducible ideals}. Want: $S^c = \emptyset$. If not, then it contains a maximal element $\mathfrak{a}$. Claim $\mathfrak{a} \neq (1)$, because $\mathfrak{a}$ not irreducible.

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

$\mathfrak{a}$ maximal in S^c, $\mathfrak{b}, \mathfrak{c} \notin S^c$. $\Longrightarrow \mathfrak{b}, \mathfrak{c} \in S$. So $\mathfrak{b}$ and $\mathfrak{c}$ are finite intersections of irreducible ideals $\Longrightarrow \mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ 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** Then $\mathfrak{a} \in S$. If not, then$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}, \mathfrak{c}, \mathfrak{b} \supsetneq \mathfrak{a} \Longrightarrow \mathfrak{b}, \mathfrak{c} \in S$. conclude as before. □

Basics on primary ideals:

Lemma 5.5. *Let $\mathfrak{q}$ primary. Then $\mathfrak{p} := rad(\mathfrak{q})$ is prime. It is the smallest prime containing $\mathfrak{q}$.*

Proof. It 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 such prime.) 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. $x^n \notin \mathfrak{q} \Longrightarrow (y^n)^m \in \mathfrak{q}$ for some $m \Longrightarrow y \in \mathfrak{p}$. □

Definition 5.6. *If* $\mathfrak{q}$ *is primary with radical* $\mathfrak{p}$*, we call* $\mathfrak{q}$ $\mathfrak{p}$***-primary****.*

Lemma 5.7. *If* $\mathfrak{q}_1, .., , \mathfrak{q}_n$*,* $\mathfrak{p}$*-primary, then* $\mathfrak{q} = \mathfrak{q}_1 \cap ... \cap \mathfrak{q}_n$ *is* $\mathfrak{p}$*-primary.*

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

Suppose $xy \in \mathfrak{q}, x \notin \mathfrak{p}$. Want $y \in \mathfrak{q}$. We have $xy \in \mathfrak{q}_i, x \notin \mathfrak{p} \implies y \in \mathfrak{q}_i \forall i \implies y \in \mathfrak{q}$ □

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. For example: If $\mathfrak{m}$ maximal ideal, $\mathfrak{q}$ any ideal, and $\mathfrak{m} = rad(\mathfrak{q})$, then $\mathfrak{q}$ is primary.

Proof. Then $\mathfrak{m}/\mathfrak{q} = Nil(\mathcal{A}/\mathfrak{q})$ is both a maximal ideal and the intersection of all prime ideals $\implies \mathcal{A}/\mathfrak{q}$ 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 $Nil(\mathcal{A}/\mathfrak{q}) = \mathfrak{m}/\mathfrak{q}$) In other words, want if $x \in \mathcal{A}/\mathfrak{q}, x \notin \mathfrak{m}/\mathfrak{q}$, then x not a zero divisor. Because $x \in \mathcal{A}/\mathfrak{q} adn x \notin \mathfrak{m}/\mathfrak{q} \implies \mathcal{A}/\mathfrak{q}$is local ring with unique prime $\mathfrak{m}/\mathfrak{q} \implies x$ is a unit. □

Lemma 5.8. $\mathfrak{m}$ *maximal,*$\implies \mathfrak{m}^n$ *is* $\mathfrak{m}$*-primary* $\forall n$

Example 5.9. $\mathfrak{m} = (X, Y) \subseteq K[X, Y] \implies \mathfrak{m}^n$ *is primary.*

Example 5.10. $\mathfrak{q} = (X^2, Y) \subseteq K[X, Y]$ *is* $\mathfrak{m}$*-primary.*

Example 5.11. $\mathfrak{a} = \prod_{j=1}^{J} (X - z_j)^{n_j} \subseteq \mathbb{C}[X]$ *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 5.12. $\mathfrak{q}_1 = (X, Y)^2 = (X^2, XY, Y^2) \subseteq K[X, Y], \mathfrak{p} = (X, Y)$. $\mathfrak{q}_2 = (Y) \implies \mathfrak{p}_2 = (Y)$

$\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 = (XY, Y^2)$

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

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

Definition 5.13. *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 5.14. *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 5.15. *Let $\mathfrak{q}$ $\mathfrak{p}$-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.*

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

We first show that the lemma leads to the theorem.

Proof. $\{p_j\} \supseteq Ass(\mathfrak{a})$. Let $x \in \mathcal{A}$ s.t. $rad(\mathfrak{a} : x) = \mathfrak{p}$ is prime. want $\mathfrak{p}$ =some $\mathfrak{p} + j$. $rad(\mathfrak{a} : x) = \cap rad(\mathfrak{q}_j : x) = \cap_{x \notin \mathfrak{q}_j} \mathfrak{p}_j \Longrightarrow \mathfrak{p}$ =some $\mathfrak{q}_j$ ¿¿¿¿¿¿¿¿1 ☐

5.2 Lecture 13

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 $\{\mathfrak{p}_1, ..., \mathfrak{p}_n\} = Ass(\mathfrak{a})$. 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 $\mathfrak{p}_i = rad(\mathfrak{q}_i)$ $Ass(\mathfrak{a}) = \{\mathfrak{p}_1, ..., \mathfrak{p}_n\}$

Example 5.16. *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* $p_2 = (x, y)$

And now we come back to the proof of the Lemma 5.15

Proof. (a) let $yz \in (\mathfrak{q} : x), y \notin (\mathfrak{q} : x)$.

Want: 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) Want: $rad(\mathfrak{q} : x) = \mathfrak{q}$

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

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

(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, $\Longrightarrow y \in \mathfrak{q}$

□

Proposition 5.17. *If $\mathcal{A}$ is Noetherian, then $\exists x \in \mathcal{A}$ s.t. $(\mathfrak{q} : x) = \mathfrak{p}$ (necessarily $x \notin \mathfrak{q}$)*

Proof. $\mathfrak{p}$ finitely generated ideal $x \in \mathfrak{p} \Longrightarrow$ some $x^n \in \mathfrak{q} \Longrightarrow$ some $\mathfrak{p}^n \subseteq \mathfrak{q}$
Choose $n \geq 1$ minimal with this property. Then $\mathfrak{p}^{n-1} \nsubseteq \mathfrak{q} \Longrightarrow \exists x \in \mathfrak{p}^{n-1}, x \notin \mathfrak{q}$.

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 $xy \in \mathfrak{p}^n \subseteq \mathfrak{q} \Longrightarrow y \in (\mathfrak{q} : x)$ □

Example 5.18. *k is field, and $\mathcal{A} = k[t]$, $\mathfrak{q} = (t^N), N \geq 1$, $\mathfrak{p} = (t)$.*

$x \in \mathcal{A} \Longrightarrow x = ct^n + c't^{n+1} + ...$, 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 $m = max(N - n, 0)$

$x \in \mathfrak{q} \Longleftrightarrow n \geq N \Longleftrightarrow m = 0$

$x \notin \mathfrak{q} \Longleftrightarrow m \geq 1 \Longrightarrow (\mathfrak{q} : x)$ is $\mathfrak{p}$-primary.

$x \in (t^{N-1})$, but $x \notin (t^N) \Longrightarrow (\mathfrak{q} : x) = \mathfrak{p}$

$x \notin \mathfrak{p} \Longleftrightarrow n = 0 \Longleftrightarrow m = N \Longrightarrow (\mathfrak{q} : x) = \mathfrak{q}$

Now we come to the proof of Theorem 5.14

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

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

Since this decomposition is minimal, we may find for each i an element $x \in \cap_{j \neq i} \mathfrak{q}_j$, $x \notin \mathfrak{q}_i$
$\Longrightarrow rad(\mathfrak{a} : x) = \mathfrak{p}_i$
$\Longrightarrow \mathfrak{p}_i \in Ass(\mathfrak{a})$.
$(\mathfrak{q}_i \nsupseteq \cap_{j \neq i} \mathfrak{q}_j)$

Conversely, if $\mathfrak{p}$ is a prime of the form $\mathfrak{p} = rad(\mathfrak{a} : x)$ 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. $\Longrightarrow Ass(\mathfrak{a}) \subseteq \{\mathfrak{p}_1, ..., \mathfrak{p}_n\}$ □

This completes the proof the Theorem 5.14. Moreover, if $\mathcal{A}$ is Noetherian, we may find for each i an element x with $(\mathfrak{a} : x) = \mathfrak{p}_i$, by applying the final part of the last lemma.

Note that $rad(\mathfrak{a}) = \cap \mathfrak{p}_j$ if $\mathfrak{a} = \cap \mathfrak{q}_j$ is a MPD. We want to define **Zero-divisors modulo** $\mathfrak{a}$,

$$\begin{aligned} Z(\mathfrak{a}) &:= \{x \in \mathcal{A} | \exists y \in \mathcal{A} - \mathfrak{a} \; s.t. \; xy \in \mathfrak{a}\} \\ &= \cup_{y \in \mathcal{A} - \mathfrak{a}} (\mathfrak{a} : y) \\ &\overset{(*)}{=} \cup_{y \in \mathcal{A} - \mathfrak{a}} rad((\mathfrak{a} : y)) \end{aligned}$$

Proof. of the (*), if some prower x^n of x satisfies $x^m \in (\mathfrak{a} : y)$, i.e. $x^n y \in \mathfrak{a}$, then we may choose $n \geq 1$ minimal with thei property. Then $x \cdot x^{n-1} y \in \mathfrak{a}$ but $x^{n-1} y \notin \mathfrak{a}$. As $x \in (\mathfrak{a} : x^{n-1} y) \Longrightarrow (*)$ □

Proposition 5.19. *$\mathfrak{a} = \cap \mathfrak{q}_j$ MPD, $\Longrightarrow Z(\mathfrak{a}) = \cup \mathfrak{p}_j$.*

Proof. $rad(\mathfrak{a} : y) = \cap_{j : \mathfrak{q}_j \not\ni y} \mathfrak{p}_j$,
$Z(\mathfrak{a}) \subseteq \cup \mathfrak{p}_j$: Let $x \in Z(\mathfrak{a})$. We want to show that x is contained in some $\mathfrak{p}_j$. The fact that $x \in Z(\mathfrak{a}) \Longrightarrow (\mathfrak{a} : x) \nsubseteq \mathfrak{a}$. On the other hand, we know $(\mathfrak{a} : x) = \cap_j (\mathfrak{q} : x)$ 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 $x \in Z(\mathfrak{a})$.

For the reverse inclusion, suppose $x \notin Z(\mathfrak{a})$. Want to show that $x \notin \mathfrak{p}_j \forall j$. Alternatively, we might try to show $\cup \mathfrak{p}_j \subseteq Z(\mathfrak{a})$.

Recall: give j, we can find y s.t. $rad(\mathfrak{a} : y) = \mathfrak{p}_j$. Necessarily, $y \notin \mathfrak{a}$. So if $x \in \mathfrak{p}_j$, then $x \in rad(\mathfrak{a} : y) \subseteq Z(\mathfrak{a})$ because $rad(\mathfrak{a} : y) = \cap_{j : \mathfrak{q}_j \not\ni y} \mathfrak{p}_j$ □

A good example for intuition, $\{z_1, ..., z_n\} \subseteq k$ where k is a field. $\mathfrak{a} = \cap \mathfrak{q}_j, \mathfrak{q}_k = (t - z_j)^{N_j}$ and $\mathcal{A} = k[t]$. by the theoremm $0 \neq x \in \mathcal{A} \Longrightarrow n_j := ord_{t - z_j}(x)$:=largest $n_j \geq 0$ such that $(t - z_j)^{n_j}$ divides x.
Then $x \in Z(\mathfrak{a}) \Longleftrightarrow \exists j : n_j \geq 1$.
$x \in rad(\mathfrak{a}) \Longleftrightarrow \forall j, n_j \geq 1$. **NB:** n_j = order of vanishing of x at z_j, $n_j \geq c \Longleftrightarrow$ first c Taylor coefficients of x at z_j

Definition 5.20. *$Ass(\mathfrak{a}) \ni \mathfrak{p}$ is either*
minimal/isolated *is $\mathfrak{p}$ is a minimal element of $Ass(\mathfrak{a})$ (We usually denote the set of isolated primes in $Ass(\mathfrak{a})$ by $Ass'(\mathfrak{a})$)or*
embedded *if $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \Longrightarrow V(\mathfrak{p}_1) \supseteq V(\mathfrak{p}_2)$ embedded in $V(\mathfrak{p}_1)$.*

Example 5.21. $\mathfrak{p}_1 = (x), \mathfrak{p}_2 = (x, y)$
$\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2^2 = (xy, x^2)$, $\mathfrak{p}_1$ *is isolated/minimal while* $\mathfrak{p}_2$ *is embedded.*

Then we state the second unique decomposition theorem:

Theorem 5.22. *In any MPD* $\mathfrak{a} = \cap \mathfrak{q}_j$, $\{\mathfrak{q}_j : \mathfrak{p}_j$ *is minimal*$\}$ *depends only upon* $\mathfrak{a}$. *More precisely, for* $\mathfrak{p}_j$ *minimal, we have* $\mathfrak{q}_j = \iota^*(\iota_*(\mathfrak{a}))$, *where* $\iota : \mathcal{A} \longrightarrow \mathcal{A}_{p_j}$

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

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 5.24. $S \subseteq \mathcal{A}$ *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) $\mathfrak{p} \cap S = \emptyset$*(*$\iota_*\mathfrak{p}$ *is prime)*$\Longrightarrow \iota_*\mathfrak{q}$ *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 $s_0 \in \mathfrak{p} \cap S. \Longrightarrow \exists n \geq 1 : s_0^n \in \mathfrak{q} \cap S$

$$\iota_*\mathfrak{q} = \{\frac{x}{s} : x \in \mathfrak{q}, s \in S\}$$

Want $\frac{1}{1} \in \iota_*\mathfrak{q} \Longrightarrow \frac{1}{1} = \frac{s_0^n}{s_0^n} \in \iota_*\mathfrak{q}$

(b) Suppose $\mathfrak{p} \cap S = \emptyset$. Then $rad(\iota_*(\mathfrak{q})) = \iota_*(rad(\mathfrak{q})) = \iota_*\mathfrak{p}$.
Let $\frac{x}{s}, \frac{y}{t} \in S^{-1}\mathcal{A}$, Suppose $(\frac{x}{s})\frac{y}{t} \in \iota_*\mathfrak{q}$, $\frac{y}{t} \notin \iota_*\mathfrak{q}$, Want : some $(\frac{x}{s})^n \in \iota_*\mathfrak{q}$

□

5.3 Lecture 14

Last lecture we ended before we prove the second uniqueness theorem of primary decomposition 5.24. Now we continue:

Proof. Last time $rad(\iota_*\mathfrak{q}) = \iota_* rad(\mathfrak{q}) = \iota_*\mathfrak{p}$.
Note : we may assume $\mathfrak{q} = (0)$, because localization is exact, hence commutes with taking quotients

$$S^{-1}(\mathcal{A}/\mathfrak{q}) \cong S^{-1}\mathcal{A}/\iota_*\mathfrak{q}$$

Thus take $\mathfrak{q} = (0)$, Assume $S \cap \mathfrak{q} = \emptyset$, i.e. $S \not\ni 0$
Want:

(i) ι : injective (i.e. $\iota^*(0) = \iota^*\iota_*(0) \stackrel{?}{=} (0)$)

(ii) $\iota_*(0) = (0)_{S^{-1}\mathcal{A}}$ is primary.

These implies the remaining assertions (for $\mathfrak{q} = (0)$).

Proof of (i):
By the general fact that $\frac{x}{1} = \frac{0}{1} \iff \exists s \in S : xs = 0 \iff x = 0$ or S contains a zerodivisor s : $xs = 0$,
(i) $\iff S$ contains no nonzero zerodivisors.
$\iff$((0) $\subseteq \mathcal{A}$ is primary) S contains no nilpotents
$\iff S \cap \mathfrak{p} = \emptyset \iff S \cap \mathfrak{q} = \emptyset \iff S \not\ni 0$

Thus (i) holds.

proof of (ii):

$$\left\{\begin{matrix}\text{Zerodivisors}\\ \text{in } S^{-1}\mathcal{A}\end{matrix}\right\} = \left\{\begin{array}{l}\dfrac{x}{s} : x \in \mathcal{A}, s \in S\\ \text{such that } \exists \dfrac{y}{t} \in S^{-1}\mathcal{A} \text{ nonzero}\\ \text{so that } \dfrac{x}{s}\dfrac{y}{t} = \dfrac{0}{1}\end{array}\right\}$$
$$= \left\{\begin{array}{l}\dfrac{x}{s} : \exists y \in \mathcal{A} \text{ with } y \cdot t \neq 0, \forall t \in S\\ \text{s.t. } \exists u \in S \text{ with } xuy = 0\\ \text{where } uy \neq 0\end{array}\right\}$$
$$= \left\{\begin{array}{l}\dfrac{x}{s} : s \in S\\ x \in \mathcal{A} \text{ is zerodivisor}\end{array}\right\}$$
$$= \left\{\frac{x}{s} : s \in S, x \in \mathcal{A} \text{ is nilpotent}\right\} ((0) \subseteq \mathcal{A} \text{ is primary})$$
$$= Nil(S^{-1}\mathcal{A}), (\text{ by the general fact that radical commutes with localizations})$$

Thus {zerodivisors in $S^{-1}\mathcal{A}$}=$Nil(S^{-1}\mathcal{A})$, so $(0)_{S^{-1}\mathcal{A}}$ is primary. ¿¿¿¿¿¿¿¿¿1

The $\Longleftarrow$ direction of (c) is trivial. For the "$\Longrightarrow$" direction of (c) Suppose $\exists s \in S \cap \mathfrak{p}$. Since $\mathfrak{p} = rad(\mathfrak{q})$, $\exists n \geq 1$ s.t. $s^n \in \mathfrak{q}$. S multiplicative closed $\Longrightarrow s^n \in S$. Thus $s \in S \cap \mathfrak{q}$. So $S \cap \mathfrak{p} \neq \emptyset \Longrightarrow S \cap \mathfrak{q} \neq \emptyset$

□

Definition 5.25. *In that case call $\mathfrak{q}_j$ the $\mathfrak{p}_j$-primary component of $\mathfrak{q}$.*

Lemma 5.26. *Let $\mathfrak{a}$ decomposable. Then $Ass'(\mathfrak{a}) = \{$minimal primes $\mathfrak{p}$ containing $\mathfrak{a}\}$*

Proof. ¿¿¿¿¿¿¿¿¿¿2 □

Theorem 5.27. *$\mathcal{A} \supseteq \mathfrak{a} = \cap_{j=1}^{n} \mathfrak{q}_j$ MPD. If $\mathfrak{p}_{\in} Ass'(\mathfrak{a})$, then*

$$\mathfrak{q}_j = \iota^* \iota_* \mathfrak{a}, \iota : \mathcal{A} \longrightarrow \mathcal{A}_{\mathfrak{p}_j}$$

As a Corollary
$\mathfrak{q}_j$ depends only on $\mathfrak{a}, \mathfrak{p}_j$

Proof.

$$\begin{aligned}\iota^*\iota_*\mathfrak{a} &= \iota^*(\iota_*(\cap \mathfrak{q}_i)) = \iota^*(\cap \iota_* \mathfrak{q}_i) = \cap \iota^* \iota_* \mathfrak{q}_i \\ &= \begin{cases} \mathfrak{q}_i : i = j \\ (1) : i \neq j \end{cases} \text{(By the lemma from start of the class)}\end{aligned}$$

For the second identity, we must check that $\forall i \neq j$, $S \cap \mathfrak{q}_i \neq \emptyset \Longleftrightarrow \mathfrak{q}_i \not\subseteq \mathfrak{p}_j$

If $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ $x \in \mathfrak{p}_i, x \notin \mathfrak{p}_j$ then some $x^n \in \mathfrak{q}_i$, $\mathfrak{p}_i = rad(\mathfrak{q}_i)$, $x^n \notin \mathfrak{p}_j$ because $\mathfrak{p}_j$ is prime $\Longrightarrow \mathfrak{q}_i \not\subseteq \mathfrak{p}_j$ □

Definition 5.28. *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) $\Longleftrightarrow$ (ii) same as the proof in definition of Noetherian ring.*

Definition 5.29. *$\mathcal{A}$ is an **Artin ring** if it satisfies the following equivalent conditions*

(i) $\mathcal{A}$ is an Artin $\mathcal{A}$-module

(ii) $\mathcal{A}$ *DCC on ideals*

(iii) $\mathcal{A}$ *MIN on ideals*

Lemma 5.30. *If* $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ *is a short exact sequence of modules, then* M *Artin* $\Longleftrightarrow M', M''$ *Artin.*

Corollary 5.31. *Any finitely generated modules over an Artin ring is Artin.*

Corollary 5.32. $\mathcal{A}$ *Artin* $\Longleftrightarrow \mathcal{A}/\mathfrak{a}$: *Artin* $\forall \mathfrak{a}$ *ideals.*

Example 5.33.

- $\mathbb{Z}$ *is not Artin,* $(2) \supsetneq (2^2) \supsetneq (2^3)$....
- *Any finite ring is Artin + Noetherian e.g.* $\mathbb{Z}/n\mathbb{Z}, n \neq 0$
- *Any finite product of Artin ring is Artin.*
- k *is field,* $\mathfrak{m} := (X_1, ..., X_n) \subset k[X_1, ..., X_n] = \mathcal{A}$. *Then* $\mathcal{A}/\mathfrak{m}^l$ *is Artin* $\forall l \geq 0$ *where* $\mathcal{A}/\mathfrak{m}^l$ *is finite dimensional vector space over* k.
- $k[X]/(X^l)$ *is Artin* $\forall l \geq 0$
- $k[X^2, X^3]/(X^{10})$ *is Artin*
- $k[X]$ *is NOT Artin.*

Lemma 5.34. *Let* $\mathcal{A}$ *Artin. Then every prime in* $\mathcal{A}$ *is maximal* $\mathcal{A}$ *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 $(x) \supseteq (x^2) \supseteq (x^3) \supseteq ....$ $\mathcal{B}$ Artin $\Longrightarrow \exists n \geq 0 : (x^n) = (x^{n+1})$, $\exists u \in \mathcal{B} : x^n = ux^{n+1} \Longrightarrow 1 = ux$ 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 $n_0 : \mathfrak{m}_1 \cap ... \cap \mathfrak{m}_{n_0} = \mathfrak{m}_1 \cap .. \cap \mathfrak{m}_n \forall n \geq n_0 \Longrightarrow \mathfrak{m}_1 \cap ... \cap \mathfrak{m}_{n_0} \subseteq \mathfrak{m}_n \Longrightarrow \mathfrak{m}_n = \mathfrak{m}_j$ for some $j \leq n_0$. $\square$

Proposition 5.35. $\mathcal{A}$ *is Artin* $\Longrightarrow \mathcal{N} := Nil(\mathcal{A})$ *is nilpotent:* $\exists n \geq 0, \mathcal{N}^n = (0)$

Remark 5.36.

$$\mathcal{A} = \oplus_{i=1}^{n} k[X_i]/(X_i^i)$$

hence $\mathcal{N} = \oplus_{i=1}^{n}(X_i)$, *where* $(X_i) \subseteq k[X_i]/(X_i^i)$ $N^n = (0), N^{n-1} \neq (0)$, *If* $n < \infty, \mathcal{A}$ *is Artin . If* $n = \infty, \mathcal{A}$ *is NOT Artin,* $\mathcal{A}$ *not Nilpotent.*

Proof. Let $\mathcal{J} := Nil(\mathcal{A}) = Jac(\mathcal{A})$ by the lemma. Consider $\mathcal{J} \supseteq \mathcal{J}^2 \supseteq \mathcal{J}^3 \supseteq ...$ $\mathcal{A}$ is Artin $\implies \mathcal{J}^n = \mathcal{J}^{n+1}$ for some n, Want $\mathcal{J}^n = (0)$

Denote $\mathcal{I} := \mathcal{J}^n$. Note that $\mathcal{J}\mathcal{I} = \mathcal{I}$, if we know that $\mathcal{I}$ were finitely generated, suppose $\mathcal{I} \neq (0)$. Then Nakayama lemma $\implies \mathcal{I} = (0)$

Let l be a minimal element of $\{\text{ideals } l \subseteq \mathcal{I} : \mathcal{J}^n l \neq (0)\}$. Then $\exists 0 \neq x \in l$ with $\mathcal{J}^n(x) \neq (0)$. Then $(x \subseteq l \subseteq \mathcal{I}), \mathcal{J}^n(x) \neq (0)$, so by minimality, $l = (x)$. $\mathcal{J}^n(x) = \mathcal{J}^{n+1}(x) = \mathcal{J}^n\mathcal{J}(x)$. Want $\mathcal{J}(x) = (x)$
If not, then $\mathcal{J}(x)$ is a nonut now (x) finitely generated, so we conclude by Nakayama ☐

6 Dimension Theory

6.1 Lecture 15

Definition 6.1. *The* ***Krull dimension*** *of a nonzero ring* $\mathcal{A}$, *denoted* $dim(\mathcal{A})$, *is the supremum of all* $r \geq 0$ *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 6.2.

- 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 6.3. $\mathcal{A}$ *an Artin ring* $\iff \mathcal{A}$ *Noetherian and* $dim(\mathcal{A}) = 0$.

Recall last lecture, by the Proposition 5.34 says all primes in Artin ring is maximal, $dim(\mathcal{A}) = 0$.

Lemma 6.4. $\mathcal{A}$ *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 6.5. *$\mathcal{A}$ Noetherian, $\mathfrak{q}$ is $\mathfrak{p}$-primary, $\exists n \geq 0 : \mathfrak{q} \supseteq \mathfrak{p}^n$. (By definition)*

Lemma 6.6. *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 Artin $\iff dim_k(V) < \infty \iff V$ is Noetherian. Thus M_j/M_{j+1} is Artin $\iff M_j/M_{j+1}$ is Noetherian.

To conclude, we apply the following Lemma:

Lemma 6.7. *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 Artin iff M_j/M_{j+1} is Artin.*

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 3.36 and Lemma 5.30, we know M_1 Noetherian (Artin) $\iff$ each M_j/M_{j+1} is Noetherian (Artin) □

□

Now we come back to the proof of Theorem 6.3

Proof. **Want:** Artin $\iff$ Noetherian + $dim = 0$
Know: Artin $\iff dim = 0$
By Lemma 6.6, it reduces to showing

(i) Artin $\iff$ (0) = finite product of maximal ideals.

(ii) Noetherian $\implies (0) =$ finite product of maximal ideals $+ \; dim = 0$.

For the part (i). Recall $\mathcal{A}$ Artin $\implies \{\text{primes } \in \mathcal{A}\} = \{\mathfrak{m}_1, ..., \mathfrak{m}_r\}$ finite set of maximal ideals.

$$(\mathfrak{m}_1 \cdots \mathfrak{m}_r)^N \subseteq (\mathfrak{m}_1 \cap ... \cap \mathfrak{m}_r)^N = Jac(\mathcal{A})^N = (0)$$

for some N by a proposition in last lecture.

For part (ii), $\mathcal{A}$ Noetherian $\implies (0) = \cap_j \mathfrak{q}_j$:MPD with $\mathfrak{p}_j = rad(\mathfrak{q}_j)$.

$$\begin{aligned}(dim = 0) &\implies \text{Each } \mathfrak{p}_j \text{ is maximal}\\ &\implies \text{Every } \mathfrak{p}_j \text{ is isolated/minimal}\\ &\implies \{\text{primes in } \mathcal{A}\} = \{\mathfrak{p}_1, ..., \mathfrak{p}_r\} \text{ are all maximal.}\end{aligned}$$

Consider $(\mathfrak{p}_1, ..., \mathfrak{p}_r)^N \subseteq (\mathfrak{p}_1 \cap ... \cap \mathfrak{p}_r)^N \subseteq (0)$, where $(\mathfrak{p}_1 \cap ... \cap \mathfrak{p}_r) = Nil(\mathcal{A}) = rad(0)$ and we can conclude the last inclusion by Lemma 6.4 □

Definition 6.8. *A ring $\mathcal{A}$ is called* ***primary*** *iff* (0) *is primary.*

Proposition 6.9. *$\mathcal{A}$ is Artin. Then $\mathcal{A}$ local $\iff$ primary.*

Proof. "$\implies$":
$(\mathcal{A} : \mathfrak{m})$ is local $\iff \mathfrak{m}$ is the unique prime ideal.
$\implies \mathfrak{m} = Jac(\mathcal{A}) = Nil(\mathcal{A})$
$\implies \mathfrak{m}^N = 0$ for some $N \geq 0$
$\mathcal{A} - \mathfrak{m} = \mathcal{A}^\times \implies \mathfrak{m} = \{\text{zero divisors}\} =$ Nilpotents $=$ Non-units because (0) is primary.
"$\impliedby$", (0) primary $\implies \mathfrak{p} = rad(0)$ 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.

□

Question: What are the Artin integral domains?
Answer: The fields. (0) prime $\implies$ (0) maximal $\implies \mathcal{A}$ is a field.

Proposition 6.10. *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 $\mathfrak{m}^n = 0$, *$\mathcal{A}$ Artin.*

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 $\mathfrak{p} = \mathfrak{m}$. Indeed, $r(\mathfrak{m}^n) = r(0)$. $\Longrightarrow \mathfrak{m} = \cap_{\mathfrak{p}}\mathfrak{p} \Longrightarrow \mathfrak{m}$ unique prime$\Longrightarrow dim(\mathcal{A}) = 0 \Longrightarrow \mathcal{A}$ is Artin. □

Example 6.11.

- $\mathbb{Z}/(p^n)$*: Artin local*
- $k[[x]]$*: Noetherian* $\mathfrak{m} = (x)$ *not Artin local*
- $k[[x]]/(x^n)$*: Artin local*
- $k[x^2, x^3]/(x^{10})$*: Artin 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 Artin ring in terms of Artin local ring.

Theorem 6.12. *Every Artin ring is a finite direct product of local Artin local rings, unique up to reordering/isomorphism.*

Proof. $\mathcal{A}$ Artin $\Longrightarrow \mathcal{A}$ Noetherian with $dim 0 \Longrightarrow \exists (0) = \cap \mathfrak{q}_j$: MPD with $\mathfrak{p}_j = rad(\mathfrak{q}_j)$ being maximal. $\exists n \geq 0$ s.t. $\mathfrak{q}_j \subseteq \mathfrak{p}_j^n \forall j$, $\mathfrak{p}_j$ maximal $\Longrightarrow$ the $\mathfrak{p}_j$ are pairwise coprime $\Longrightarrow \mathfrak{q}_j$ are pairwise coprime. Then we know from Chinese remainder theorem: the map

$$\mathcal{A}/\cap_j \mathfrak{q}_j \longrightarrow \prod_j \mathcal{A}/\mathfrak{q}_j$$

is an isomorphism, Which means

$$\mathcal{A} \cong \prod_j \mathcal{A}/\mathfrak{q}_j$$

is a finite product of Artin local rings.

Uniqueness: Suppose $\phi : \mathcal{A} \xrightarrow{\cong} \prod_j \mathcal{A}_j$ finite product of Artin 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 the above lemma we know Artin local indicate primary. Then we know $\mathcal{A}/\mathfrak{q}_i'$ primary $\mathfrak{q}_i'$ is primary. ¿¿¿¿¿¿¿¿1 □

6.2 Lecture 16 Krull's Intersection Theorem

Theorem 6.13. *(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 6.14. *In the above setting,*

$$\cap_{i\geq 0}\mathfrak{a}^i = (0)$$

Example 6.15. *(Nonexample) k 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 6.13) $\mathfrak{a} \subseteq Jac(\mathcal{A})$, which suggests us to try Nakayama's Lemma 2.16. $M' := \cap_{i\geq 0}\mathfrak{a}^i M$. 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 $\mathfrak{a}M' \subseteq M'$(easy to check).
To proceed, we need the following lemma:

Lemma 6.16. *(Artin-Rees) $\mathcal{A}$ 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 6.16, $\mathfrak{a}^i M \cap M' = \mathfrak{a}^{i-k}(\mathfrak{a}^k M \cap M')$. 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 2.16, $\implies M' = 0$ done.

□

The "$\supseteq$" part of Artin-Rees Lemma 6.16 is clear, because $\mathfrak{a}^{i-k}(\mathfrak{a}^k M \cap M') \subseteq \mathfrak{a}^i M \cap \mathfrak{a}^{i-k} M'$.

Our aim next is to prove "$\subseteq$" part of Artin-Rees lemma.

Definition 6.17. *Let I be a **monoid** (Set with associative binary operation and with identity). An I-**graded ring** is a ring together with a decomposition $\mathcal{A} = \oplus_{i\in I}\mathcal{A}_i$ such that $\mathcal{A}_i\mathcal{A}_j \subseteq \mathcal{A}_{i+j}$. Thus $1 \in \mathcal{A}_0$*

Example 6.18. *$\mathcal{A} = k[X_1, ..., X_n]$, $I = \mathbb{Z}_{\geq 0}$, 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 $I = (\mathbb{Z}_{\geq 0})^n$ and $\mathcal{A}_I = kX_1^{i_1}...X_n^{i_n}$

Definition 6.19. *A **graded module** M over a graded ring $\mathcal{A} = \oplus_{i\in I}\mathcal{A}_i$ is a module equipped with a decomposition $M = \oplus_{i\in I}M_i$ s.t. $\mathcal{A}_i \cdot M_j \subseteq M_{i+j}$. A **graded submodule** $M' \subseteq M$ is then a submodule for which $M' = \oplus_{i\in I}(M'\cap M_i)$. 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.*

Example 6.20. *$\mathcal{A} = k[x, y]$ 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 $\mathbb{Z}^2_{\geq 0}$-grading and visualized. Try to show $\mathfrak{a} \cap \mathcal{A}_1 = 0$. Since $x^2 \in \mathcal{A}_2$ and $y \in \mathcal{A}_1$ and $\mathcal{A} = \oplus\mathcal{A}_i$, this implies that $x^2 + y \notin \sum(\mathfrak{a} \cap \mathcal{A}_i)$

Lemma 6.21. *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

$$\begin{aligned}\sum_i(M_i \cap M') \subseteq M' &\subseteq \sum_\alpha \mathcal{A}x_\alpha \\ &= \sum_{j,\alpha} \mathcal{A}_j x_\alpha \\ &\subseteq \sum_{j,\alpha} M_{i(\alpha)+j} \cap M' (\text{By def of graded-module}) \\ &\subseteq \sum_i (M_i \cap M').\end{aligned}$$

(ii) $M' \subseteq M$ graded, finitely generated.
Similar proof. But now we start with a possibly infinite generating set of homogeneous elements H and a finite generating set F. And notice that each element in H can be expressed as a finite linear expansion by elements in H. Then altogether, we can select a finite homogeneous generating set in H.

$\square$

Recall the setup for Artin-Rees. $\mathcal{A}$ 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 $\tilde{\mathcal{A}} := \boxplus_{i\geq 0}\mathfrak{a}^i := \{(x_i)_{i\geq 0} : x_i \in \mathfrak{a}^i, \text{with } x_i = 0 \text{ for almost all } i\}$ $\tilde{\mathcal{A}}_j = \mathfrak{a}^j = \{(x_i)_{i\geq 0} \in \tilde{\mathcal{A}} : x_i = 0, \forall i \neq j\}$. Multiplication on $\tilde{\mathcal{A}}$ linearly extends the maps:

$$\mathfrak{a}^i \times \mathfrak{a}^j \longrightarrow \mathfrak{a}^{i+j}$$

This is a natural source of graded $\tilde{\mathcal{A}}$-modules. $\tilde{M} = \boxplus_{i\geq 0} M_i$ coming from **$\mathfrak{a}-$filtration** (M_i)**:**

- M_i is a submodule of some module M.
- $\mathfrak{a}M_i \subseteq M_{i+1} \Longrightarrow \mathfrak{a}^j M_i \subseteq M_{i+j}$
- $M_{i+1} \subseteq M_i$. Thus $\mathfrak{a}^i \times M_j \longrightarrow M_{i+j}$ is defined.

$\tilde{M}$ is a graded $\tilde{\mathcal{A}}$-module.

Definition 6.22. *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 $\tilde{\mathcal{A}}$ 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 3.37, we know $\tilde{\mathcal{A}}$ is Noetherian.

Lemma 6.23. *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 $\Longrightarrow \tilde{M} = \tilde{\mathcal{A}}\sum_{i\leq k} M_k$, where we claim that each M_k is finitely generated $\mathcal{A}$-module. This is true because M is finitely generated ring over a Noetherian ring $\mathcal{A}$, thus it is Noetherian. 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

$$\tilde{M} = \tilde{\mathcal{A}} \sum_{i \le k} M_k.$$

If we pick $j-$th component for $j \ge k$, 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. $\square$

6.3 Lecture 17: Artin-Rees, Krull principal ideal theorem

Now we come back to the proof of Artin-Ress Lemma 6.16 thus the Krull-intersection theorem 6.13. Last time we proved the following are equivalent ($\mathcal{A}-$Noetherian), $\mathfrak{a}$ any ideal, $(M_i)_{i \ge 0}$: $\mathfrak{a}-$ filtration, $\mathfrak{a} M_i \subseteq M_{i+1}$

$$\tilde{\mathcal{A}} = \boxplus_{i \ge 0} \mathfrak{a}^i, \quad \tilde{M} = \boxplus_{i \ge 0} M_i$$

(i) (M_i) is stable,i.e. if $\exists k \ge 0 : \forall i \ge k, \mathfrak{a} M_i = M_{i+1} \Longrightarrow (\mathfrak{a}^j M_i = M_{i+j})$.

(ii) $\tilde{M}$ is finitely generated $\tilde{\mathcal{A}}$-module.

$\tilde{\mathcal{A}}$: Noetherian $\Longleftrightarrow$ $\mathcal{A}$ Noetherian $\Longrightarrow$ $\mathfrak{a}$: 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
Assume its hypothesis, choose $\forall i \ge 0, M_i := \mathfrak{a}^i M$: then it is a stable $\mathfrak{a}$-filtration $(\mathfrak{a} M_i = \mathfrak{a} \cdot \mathfrak{a}^i M = \mathfrak{a}^{i+1} M = M_{i+1})$

$M_i' = \mathfrak{a}^i M \cap M'$: an $\mathfrak{a}$-filtration. $\tilde{M}' := \boxplus_{i \ge 0} M_i'$. $\tilde{M}$ is naturally a $\tilde{\mathcal{A}}-$submodule of $\tilde{M}$

$M_i' = \mathfrak{a}^{i-k} M_k' \Longleftrightarrow$ (conclusion of Artin-Rees lemma) $\Longleftarrow$ (M_i')*stable* $\Longleftrightarrow$ $(\tilde{M}'$, finitely generated $\tilde{\mathcal{A}}$-module)

But we can derive this form (M_i) stable $\Longrightarrow$ $\tilde{M}$ is finitely generated $\tilde{\mathcal{A}}$-module $\Longrightarrow$ ($\tilde{M}'$ is finitely generated $\tilde{\mathcal{A}}$-module) because $\tilde{\mathcal{A}}$ is Noetherian and $\tilde{M}$ is Noetherian. $\square$

Recall The theorem of Krull intersection says that if $\mathcal{A}$ is Noetherian, $\mathfrak{a} \subseteq Jac(\mathcal{A})$, M is a finitely generated $\mathcal{A}$-module, then $\cap_i \mathfrak{a}^i M = 0$. Then we have the following corollaries

Cor2 Suppose $\mathcal{A}$ Noetherian, $\mathfrak{a} \subseteq Jac(\mathcal{A})$, then

$$\cap_i \mathfrak{a}^i = 0$$

Cor3 Suppose $(\mathcal{A}, \mathfrak{m})$ Noetherian, local, $\mathfrak{m} = Jac(\mathcal{A})$, then

$$\cap_i \mathfrak{m}^i = 0$$

Exercise 6.24. *Deduce Krull intersection theorem form Cor3*

Kernel of localization with respect to a prime

Question: Let $\mathfrak{p} \in Spec(\mathcal{A})$. What is $Ker(\mathcal{A} \longrightarrow \mathcal{A}_{\mathfrak{p}})$?

Definition 6.25. *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 $\iota : \mathcal{A} \longrightarrow \mathcal{A}_{\mathfrak{p}}$. This is a $\mathfrak{p}-$primary ideal. $(\iota_*(\mathfrak{a}\mathfrak{b}) = \iota_*(\mathfrak{a})\iota_*(\mathfrak{b}))$*

Theorem 6.26. *$\mathcal{A}-$Noetherian, then $Ker(\mathcal{A} \longrightarrow \mathcal{A}_{\mathfrak{p}}) = \cap_{i \geq 0} \mathfrak{p}^{(i)}$.*

Proof. We know $Ker(\mathcal{A} \longrightarrow \mathcal{A}_{\mathfrak{p}}) = \iota^*((0)) \stackrel{?}{=} \cap_{i \geq 0} \iota^*(\iota_*(\mathfrak{p})^i)$. The last equality is guaranteed by the Cor3 above because $(0) = \cap_{i \geq 0} \iota_*(\mathfrak{p})^i$.

Note that $(\mathcal{A}_{\mathfrak{p}}, \iota_*(\mathfrak{p}))$ is local, Noetherian. □

Lemma 6.27. *(A special use of Krull dimension theorem) $\mathcal{A}$ 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.* , $(0) \subsetneq \mathfrak{p} \subsetneq \mathfrak{m}$

Example 6.28. $\mathcal{A} = k[[X, Y]] \supseteq \mathfrak{m} = (X, Y) \supseteq (0)$. *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.* $f = Y \in \mathfrak{m}$

NB $(ii) \Longrightarrow (i)$ is clear: take $f = 0$

Definition 6.29. *$dim(\mathcal{A}) = \sup\{t \geq 0 : \exists$ 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 6.30. *$0 \neq f($ non-unit $) \in \mathcal{A}$: Noetherian integral domain. Then any minimal prime $\mathfrak{m}_0$ of (f) satisfies $ht(\mathfrak{m}_0) = 1$*
$\mathfrak{m}_0 \supseteq (f)$ minimal for this property "$\mathfrak{m}_0 \in Ass'((f))$"

Reduce Lemma 6.30 to Lemma 6.27, 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

$$\{\text{primes } \mathfrak{p} \ni f\} \longleftrightarrow \{\text{ primes of } \mathcal{A}_\mathfrak{m} | \mathfrak{p} \ni f/1\}$$

So assume $(\mathcal{A}, \mathfrak{m})$ Noetherian local domain, $\mathfrak{m} := \mathfrak{m}$.

Know $\mathfrak{m} \in Ass'((f))$, i.e., $\not\exists$ 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)).

Want $ht(\mathfrak{m}) = 1$, i.e., $1 = \sup T$ where $T := \{t \geq 0, \exists \text{chain} \mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_t = \mathfrak{m}\}$. which is equivalent to

- $(0) \subsetneq \mathfrak{m}, (\Longleftarrow \mathfrak{m} \ni f \neq 0)$, $T \ni 1$
- $\not\exists$ prime $\mathfrak{p} : (0) \subsetneq \mathfrak{p} \subsetneq \mathfrak{m}$,$T \not\ni 2$

Now we come back to the proof of Lemma 6.27.

Proof. "$(i) \Longrightarrow (ii)$" in Lemma 6.27

$(ii) \Longleftrightarrow dim(\mathcal{A}/(f)) \geq 1, \forall f \in \mathfrak{m}$, there are two bijections: $\mathfrak{m} \longleftrightarrow$ a maximal ideal in $\mathcal{A}/(f)$, $\mathfrak{m} \supsetneq \mathfrak{p} \supsetneq (f) \longleftrightarrow$ 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 6.3, $\frac{\mathcal{A}}{(f)}$ is Artin. $\Longrightarrow \exists k$ s.t., $\forall i \geq k$ $\mathfrak{p}^{(k)} + (f) = \mathfrak{p}^{(i)} + (f)$

Indeed, $\frac{\mathfrak{p}^{(k)}+(f)}{(f)}$ is a descending chain in $\frac{\mathcal{A}}{(f)}$

The negation of $(ii) \Longrightarrow \exists f \in \mathfrak{m}$ 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>: $f \notin \mathfrak{p} \subseteq \mathfrak{m}$.

<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:

"$\supseteq$" OK

"$\subseteq$". 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 $\mathfrak{p} \not\ni f$)

Taking $i \geq k$, $\mathfrak{p}^{(k)} \subseteq \mathfrak{p}^{(i)} + f\mathfrak{p}^{(k)}$, hence we have prove the claim. □

Then consider the module $M := \mathfrak{p}^{(k)}/\mathfrak{p}^{(i)}$. (Claim:$\mathfrak{p}^{(k)} = \mathfrak{p}^{(i)} + f\mathfrak{p}^{(k)}$)$\Longrightarrow$

$$\mathfrak{p}^{(k)}/\mathfrak{p}^{(i)} = (\mathfrak{p}^{(k+1)} + f\mathfrak{p}^{(k)})/\mathfrak{p}^{(i)} = f\mathfrak{p}^{(k)}/\mathfrak{p}^{(i)}$$

$\mathcal{A}$ is local Noetherian, then $(f) \subseteq Jac(\mathcal{A}) = \mathfrak{m}$

$$(f)M = M \Longrightarrow M = \mathfrak{p}^{(k)}/\mathfrak{p}^{(i)} = 0 \text{ by Nakayama 2.16}$$

$\Longrightarrow \mathfrak{p}^{(i)} = \mathfrak{p}^{(k)}$, $\forall i \geq k \Longrightarrow \mathfrak{p}^{(k)} = \cap_i \mathfrak{p}^{(i)} =$ (by Theorem 6.26) $Ker(\mathcal{A} \longrightarrow \mathcal{A}_{\mathfrak{p}}) = \{0\}$ the last equality because $\mathcal{A}$ is a domain. $\mathfrak{p}^k \subseteq \mathfrak{p}^{(k)} = (0)$ (because $\mathcal{A}$ is a domain) $\Longrightarrow \mathfrak{p} = (0)$ as desired. □

Remark 6.31. *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.

6.4 Lecture 18 Krull Dimension Theorem

Theorem 6.32. *(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 6.33. *$\mathfrak{a}$ 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 6.32 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, $\mathfrak{p}_i = rad(\mathfrak{q}_i)$

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 $\{\mathfrak{p}_i\} \supseteq \{\text{minimal primes of } \mathcal{A}\}$)

$a \in \mathfrak{p}, a \notin \mathfrak{p}_i, \Longrightarrow \mathfrak{p}_i \subsetneq \mathfrak{p} \Longrightarrow ht(\mathfrak{p}) \geq 1$

Want: $ht(\mathfrak{p}) = 1$. 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) that $\mathfrak{p}'' = \mathfrak{p}_i$.

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 6.30$\Longrightarrow \nexists \mathfrak{p}' : (0) \subsetneq \mathfrak{p}' \subsetneq \mathfrak{p}$ ∎

Geometric Interpretation: suppose $k = \overline{k}$, 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 $rad(\mathfrak{a}) = \mathfrak{a} \longleftrightarrow Z \subseteq X$ closed subvariety

$\mathfrak{p}_i \in Ass'(\mathfrak{a}) i.e. \mathfrak{p}_i \supseteq \mathfrak{a}$ minimal $\longleftrightarrow$ irreducible components $Y_i \subseteq Z$

$codim_X(Z) = \inf_{Y_i}\{codim_X(Y_i) | Y_i$ is irreducible component of $Z\}$

$coht(\mathfrak{p}) = dim(\mathcal{A}/\mathfrak{p}) \longleftrightarrow dim(Y)$

$coht(\mathfrak{a}) = dim(\mathcal{A}/\mathfrak{a}) = \sup_i\{coht(\mathfrak{p}_i)\}$

$dim(Z) = \sup\{dim(Y_i) | Y_i$ 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 6.34. *(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 $r \geq 1$. Suppose $\exists$ chain $\mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_t = \mathfrak{p}$
Want $t \leq r$. Replace $\mathcal{A}$ by $\mathcal{A}/\mathfrak{p}$. Reduce to the case $(\mathcal{A}, \mathfrak{p})$ $\mathcal{A}-$Noetherian local domain and $\mathfrak{p}$ maximal ideal in $\mathcal{A}$. We know $\mathfrak{p}$ is the minimal among those primes containing $\mathfrak{a}$, $\implies \mathfrak{p}$ 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 prime between $\mathfrak{p}_{t-1}$ and $\mathfrak{p}_t$. (Varying that $\mathcal{A}$: Noetherian to see that $\exists$ a maximal prime $\mathfrak{q}$ s.t. $\mathfrak{p}_{t-1} \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}_t$, then add $\mathfrak{q}$ to our chain.)

$\mathfrak{p}_{t-1} \subsetneq \mathfrak{p}_{t-1} + (a_r) \subseteq \mathfrak{p}_t \implies$ "$\mathfrak{p} = \mathfrak{p}_t$ is the only prime containing $\mathfrak{p}_{t-1} + (a_r)$" $\implies (\mathfrak{p}_{t-1} + (a_r)) = \mathfrak{p} \supseteq \mathfrak{a} \ni a_i$

$\implies \exists N \geq 1 : a_i^N = a_i' + a_r y_i \in scp_{t-1} + (a_r)$
Define $\mathfrak{a}' := (a_1', ..., a_{r-1}') \subseteq \mathfrak{p}_{t-1}$.

Want:$\mathfrak{p}_{t-1} \in Ass'(\mathfrak{a}')$. If we can show this, then our inductive hypothesis gives $t-1 \leq r-1 \implies t \leq r$. Let $\mathfrak{p}' \in Ass'(\mathfrak{a}')$ 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 $ht(\mathfrak{p}/\mathfrak{p}') \leq 1$ in $\mathcal{A}/\mathfrak{p}'$. Let $\overline{a}_r :=$ images of a_r in $\mathcal{A}/\mathfrak{p}'$. By the Krull Princial ideal theorem 6.32, it will suffice to show that $\mathfrak{p}/\mathfrak{p}' \in Ass'((\overline{a}_r)) \implies \mathfrak{p}' = rad(\mathfrak{p}' + (a_r))$
To see this:
$\mathfrak{p} = rad(\mathfrak{a}) = rad(\mathfrak{a}' + (a_r)) \subseteq rad(\mathfrak{p}' + (a_r)) \subseteq \mathfrak{p}$ □

Corollary 6.35. *$\mathcal{A}$ Noetherian, $\mathfrak{a}$ is an ideal in $\mathcal{A}$*
$\implies ht(\mathfrak{a}) < \infty$, $dim(\mathcal{A}) < \infty$

Proof. $\mathfrak{a} = (a_1, ..., a_r) \implies ht(\mathfrak{a}) \leq r$ by the above theorem. □

Corollary 6.36. *$(\mathcal{A}, \mathfrak{m})$: Noetherian local ring with the maximal ideal. $k := \mathcal{A}/\mathfrak{m}$ field. Then $dim(\mathcal{A}) \leq dim_k(\mathfrak{m}/\mathfrak{m}^2)$*

<u>NB</u>: $\forall$ $\mathcal{A}$-module M, the quotient $M/\mathfrak{m}M$ is a $k-$vector space.

Proof. Suppose, $r = dim_k(\mathfrak{m}/\mathfrak{m}^2)$, $a_1, ...a_r$ is a basis of $\mathfrak{m}/\mathfrak{m}^2$. Let $\tilde{a}_1, ..., \tilde{a}_r \in \mathfrak{m}$ be lifts of the a_i.

Set $M = \mathfrak{m}$, $N := M/(\tilde{a}_1, ..., \tilde{a}_r)$, by hypothesis $\mathfrak{m}N = N$, then by Nakayama lemma$N = 0 \implies \mathfrak{m} = (\tilde{a}_1, ...\tilde{a}_r) \implies ht(\mathfrak{m}) = ht(\mathcal{A}) \leq r$ □

Corollary 6.37. *$\mathcal{A}$ 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 6.34

$ht(a_1, ..., a_s) \geq s$ by considering MPD.

For a complete proof, see the Theorem 6.39 □

6.5 Lecture 19: Converse of Krull dimension theorem, System of Parameters

Recall:

Theorem 6.38. *$\mathcal{A}$ 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 $ht(\mathfrak{p}) = 1$

Theorem 6.39. *(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) $\mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_r$, then we can find $x_1, ..., x_r \in \mathfrak{p}_r$ 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 $(a_1, ..., a_r)$

Note: $(i) \implies (iii)$ 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): $ht(\mathfrak{a}) = r$, then we can find some chain $\mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_s$. We induct on s, Assume we have found $x_1, ..., x_s$ s.t. $\mathfrak{p}_i \supset (x_1, ..., x_s)$ minimal $\forall i \leq s$, then $ht(\mathfrak{p}_i) \leq i$ by Theorem 6.38. On the other hand, $ht(\mathfrak{p}_i) \geq i$ by the existence of $\mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_i \implies (\mathfrak{p}_i) = i$.

Consider the minimal primes $\{\mathfrak{q}_i\} = Ass'((x_1, ..., x_s))$. Claim: $\mathfrak{p}_{i+1} \not\subset \cup_j \mathfrak{q}_j$. Indeed, if not, then since $\mathfrak{q}_j$ prime $\mathfrak{p}_{i+1} \subseteq \mathfrak{q}_j$ for some j. By the "avoidance of primes".

Then $ht(\mathfrak{q}_j) \leq i$, by Krull, but $ht(\mathfrak{p}_{i+1}) \geq i+1$. Contradiction, thus the claim fails. Choose $x_{i+1} \in \mathfrak{p}_{i+1} - \cup_j \mathfrak{q}_j$. Then $\mathfrak{p}_{i+1} \supseteq (x_1, .., x_{i+!}.)$

Want:$\mathfrak{p}_{i+1} \in Ass'((x_1, ..., x_{i+1}))$, so $\mathfrak{p}_{i+1} \supseteq$ some $\mathfrak{q}_j$ as above.

Take $\mathfrak{p}' \in Ass'(x_1, .., x_s)$ s.t. $\mathfrak{p}_{i+1} \supseteq \mathfrak{p}'$. Then claim: $ht(\mathfrak{p}') = i+1$,

for the proof of the claim: $ht(\mathfrak{p}') \leq i+1$ by Krull, and $ht(\mathfrak{p}') geqi + 1$ because $\mathfrak{p}'$ is not a minimal prime $\mathfrak{q}_i$ of $\mathfrak{p}_i$ because $\mathfrak{p}' \ni x_{i+1} \notin \mathfrak{q}_j$,

If $(\mathfrak{p}' \subsetneq \mathfrak{p}_{i+1})$ we can get a contradiction on the height of $\mathfrak{a}$ $\square$

Recall: $\mathfrak{p}_i$ are primes. then $\mathfrak{a} \subset \cap \mathfrak{p}_j \iff \exists j \mathfrak{a} \subseteq \mathfrak{p}_j$

Corollary 6.40. *: $(\mathcal{A}, \mathfrak{m})$ 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 $\mathfrak{m} = rad((x_1, ..., x_n))$ and $(x_1, ..., x_n)$ is $\mathfrak{m}-$primary. (recall that any idal whose radical is maximal is primary)

Definition 6.41. *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.*

Corollary 6.42. $(\mathcal{A}, \mathfrak{m})$ *is Noetherian Local,* $dim(\mathcal{A}) = ht(\mathfrak{m}) = min\{n \geq 1 : \exists x_1, ..., x_n \text{ s.t. } \mathfrak{m} \subseteq (x_1, .., x_n) \text{ minimal.}\}$

Proof. $\geq$ converse of Krull

$\leq$ Krull ∎

Theorem 6.43. $(\mathcal{A}, \mathfrak{m})$ *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 $(i) \iff (ii) \Longleftarrow (iii)$

Proof. $(iii) \implies (i)$: 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 result before 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 $(i) \iff (ii)$.

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

$\iff$ $\mathfrak{m}$ is the only prime containing $(x_1, .., y_s)$

$\iff \overline{\mathfrak{m}}$ is the only prime containing $(\overline{y}_1, ..., \overline{y}_s)$
$\iff (\overline{y}_1, ..., \overline{y}_s)$: $\overline{\mathfrak{m}}-$primary
$\{\overline{y}_1, ..., \overline{y}_s\}$ system of parameters for $(\overline{\mathcal{A}}, \overline{\mathfrak{m}}) \iff s = dim(\overline{\mathcal{A}})$ 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] $\implies dim(\mathcal{A}) \leq r+s$, by Krull's dimension theorem 6.34.

And in fact, if we start we a system of parameters $(\overline{z}_1, ..., \overline{z}_t)$ of $\overline{A}$, 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 $dim(\mathcal{A}) \leq t + r = dim(\overline{\mathcal{A}}) + r$

$(i) \implies \exists y_1, .., y_s$ s.t., $\{x_1, ...x_r, y_1, ..., y_s\}$ is system of parameters. $\implies r + s = dim(\mathcal{A})$ 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. $\{\overline{y}_1, ..., \overline{y}_s\}$ us a system of parameters. $\implies (\overline{y}_1, ..., \overline{y}_s)$ $\overline{\mathfrak{m}}-$primary $\implies (x_1, .., x_r, y_1, ..., y_s)\mathfrak{m}-$primary.

Want: $\{x_1, .., x_r, y_1, ..., y_s\}$ is a system of parameters. Indeed, $r+s = dim(\mathcal{A})$, so this holds by definition. $\square$

Corollary 6.44. $(\mathcal{A}, \mathfrak{m})$, *Noetherian local,* $a \in \mathcal{A}$ *non-zerodivisor. Then* $dim(\mathcal{A}/(a)) = dim(\mathcal{A}) - 1$

Proof. Recall: $ht((a)) = 1$ by Krull principal ideal theorem.

By the above ((iii)implies (i) and (ii)), we may extend $\{a\}$ to a system of parameters $\{a_0, ..., a_n\}$, $a_0 = a$, with $dim(\mathcal{A}) - 1 = dim(\mathcal{A}/(a))$ $\square$

Theorem 6.45. $\mathcal{A}$ *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 $\mathfrak{p}_0\mathcal{A}[X] \subsetneq ... \subsetneq \mathfrak{p}_n\mathcal{A}[X] \subsetneq \mathfrak{p}_n\mathcal{A}[X] + X\mathcal{A}[X]$

<u>NB</u>, 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 $\mathfrak{p}_0 \subseteq ...$ $\square$

6.6 Lecture 20

Proof. Last time, we proved $dim(\mathcal{A}[X]) \geq dim(\mathcal{A}) + 1$ by exhibiting, for each length r chain $\mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_r \in \mathcal{A}$. The length $r+1$ chain $\mathfrak{p}_0\mathcal{A}[X] \subsetneq ... \subsetneq \mathfrak{p}_r\mathcal{A}[X] \subsetneq \mathfrak{p}_r\mathcal{A}[X] + (X)$ in $\mathcal{A}[X]$.

Now $dim(\mathcal{A}[X]) \leq dim(\mathcal{A})+1$. Because $dim\mathcal{A}[X] = \sup\{\mathfrak{m} \subseteq \mathcal{A}[X] \text{ maximal } |ht(\mathfrak{m})\}$

So it suffices to show $\forall \mathfrak{m} \subseteq \mathcal{A}[X]$ that $ht(\mathfrak{m}) \leq r+1$, where $r := dim\mathcal{A}$. May assume $r \leq \infty$.

Consider $\mathfrak{p} := \mathfrak{m} \cap \mathcal{A}$ prime in $\mathcal{A}$. 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 $S^{-1}(\mathcal{A}[X]) = (S^{-1}\mathcal{A})[X] = \mathcal{A}_{\mathfrak{p}}[X]$. $S^{-1}\mathfrak{m} \subseteq S^{-1}\mathcal{A}[X]$ remains a maximal ideal, and $ht(S^{-1}\mathfrak{m}) = ht(\mathfrak{m})$, because the localization with respect to S, preserves the primes and their inclusions for those ideals not intersecting S.

We now assume that $(\mathcal{A}, \mathfrak{p})$: Noetherian local ring, $\mathfrak{m} \subseteq \mathcal{A}[X]$ maximal, $\mathfrak{m} \cap \mathcal{A} = \mathfrak{p}$. $r = dim\mathcal{A} \leq \infty$.

Want $ht(\mathfrak{m}) \leq r+1$

It suffices by a theorem in last lecture to construct $r+1$ elements of $\mathcal{A}[X]$ that generate an ideal with radical $\mathfrak{m}$.

Know $r = dim(\mathcal{A}) = ht(\mathfrak{p})$, 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., $rad((x_1, ..., x_r)) = \mathfrak{p}$.

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 $\mathfrak{q}$ that contains $x_1, .., x_r, f$.

Indeed, $\mathfrak{q} \cap \mathcal{A}$ 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 $\mathfrak{q} = \mathfrak{m}$

$\square$

Example 6.46. *(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 $x,y\} = \{\sum_{ij} c_i j x^i y^j\}$, $k[[x,y]]$ 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 $\Longrightarrow (x) \subsetneq (x,y)$ is a chain of prime, notice that $\mathcal{A}$ is not a integral domain$\Longrightarrow dim(\mathcal{A}) \geq 1$

$\mathcal{A} \supseteq \mathfrak{m} = (x,y)$ (x and y here means the image of x and y in the quotient ring.)

Claim $rad((y)) = \mathfrak{m}$

Proof. $x^2 = 0 \in (y), y^1 \in (y) \to \mathfrak{m} \subseteq rad((y))$, and by the fact the t$\mathfrak{m}$ is maximal $\mathfrak{m} = rad((y))$ $\square$

By the theorem on parameters, deduce that $dim(\mathcal{A}) \leq 1$. hence $dim\mathcal{A} = 1$

Lemma 6.47. *$k = \overline{k}$ 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 $ht(\mathfrak{m}) = n$, and $\mathcal{A}_\mathfrak{m}$ a local ring of dimension n whose maximal ideal $\mathfrak{m}\mathcal{A}_\mathfrak{m}$ has n generators.*

Proof. $dim(\mathcal{A}_\mathfrak{m}) = ht(\mathfrak{m}\mathcal{A}_\mathfrak{m}) = ht(\mathfrak{m}) \leq dim(\mathcal{A}) = n$. $ht(\mathfrak{m}) \geq n$ because $\mathfrak{m} = \mathfrak{p}_n \supsetneq ... \supsetneq \mathfrak{p}_0$, $\mathfrak{p}_i = (X_1 - x_1, ..., X_i - x_i)$ $\square$

Now let $(\mathcal{A}, \mathfrak{m})$: Noetherian local of $d := dim(\mathcal{A}) = ht(\mathfrak{m})$ and we set $k = \mathcal{A}/\mathfrak{m}$.

Lemma 6.48.

(a) *In general , $d \leq dim_k(\mathfrak{m}/\mathfrak{m}^2)$ (The late is a $k-$vector space because M and $\mathcal{A}$-module $\Longrightarrow M/\mathfrak{m}M$ 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 6.49. *$k[x_1, .., x_n]_\mathfrak{m}$ is regular.*

Proof.

(a) Set $n := dim_k(\mathfrak{m}/\mathfrak{m}^2)$. Choose $x_1, .., x_n \in \mathfrak{m}$ s.t. $\overline{x}_1, ..., \overline{x}_n \in \mathfrak{m}/\mathfrak{m}^2$ form a basis.

By Nakayama Lemma $\Longrightarrow \mathfrak{m} = (x_1, ..., x_b) \Longrightarrow d \leq n$ by Krull dimension theorem.

(b) $(i) \Longrightarrow (ii)$
$\mathfrak{m} = (x_1, ..., x_d) \Longrightarrow \mathfrak{m}/\mathfrak{m}^2$ is spannd by $\overline{x}_1, ..., \overline{x}_d$, so $dim_k(\mathfrak{m}/\mathfrak{m}^2) \leq d$. Combine with (a) to get (ii).

$(ii) \Longrightarrow (i)$ Same proof as (a)

$\square$

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: $\mathcal{A} = k[x_1, .., x_n]$

Want Machinery for comparing a general ring $\mathcal{A}$ as above to this example.

7 Integral extension of rings

We will cover the contents of §5 of A-M and §3 pf Bosch

7.1 Lecture 20

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.

$(ii) \implies (iii)$ $\mathcal{C} := \mathcal{A}[x]$,

$(iii) \implies (iv)$ $M := \mathcal{C}$

$(iv) \implies (i)$ $M = \sum_i^n \mathcal{A}e_i, e_i \in M$. 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.

□

7.2 Lecture 21

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:*

$$[x \textit{ integral over } \mathcal{A}] \implies [x \textit{ integral over } \mathcal{B}]$$

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 of integral.*

Proof. $\mathcal{C} = \sum_{i=1,..,m} \mathcal{B} y_i$ and $\mathcal{B} = \sum_{j=1,..,n} \mathcal{A} x_j \implies$

$$\mathcal{C} = \sum_{i,j} \mathcal{A} x_j y_i, \quad x_j \in \mathcal{B}, y_i \in \mathcal{C} \implies x_j y_i \in \mathcal{C}$$

□

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. □

Lemma 7.7. *$\mathcal{A} \subseteq \mathcal{B}$. The following are equivalent:*

(i) $\mathcal{B}$ is integral over $\mathcal{A}$, 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. "$(i) \implies (ii)$":$\mathcal{B}$ is finitely generated $\mathcal{A}$-algebra, then $\mathcal{B} = \mathcal{A}[x_1, .., x_n]$, for some $x_j \in \mathcal{B} \implies$(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

"$(ii) \implies (i)$": By Lemma 7.2, part iii). $\implies i$)., $\forall x \in \mathcal{B}, \mathcal{A}[x] \subseteq \mathcal{B} \subseteq \mathcal{B}$, where $\mathcal{B}$ is itself finitely generated $\mathcal{A}$-module, then we know x is integral over $\mathcal{A}$. □

Lemma 7.8. *$\mathcal{A} \subseteq \mathcal{B}$ are rings. Then $\overline{\mathcal{A}} := \{x \in \mathcal{B} | x$ 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 $\mathcal{A}$ $\implies \mathcal{A}[x, y]$ 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 $\mathcal{A}$. □

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

$$x^n + b_1 x^{n-1} + ... + b_n = 0 \text{ for some } b_1, ..., b_{n-1} \in \mathcal{B}.$$

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 $\mathcal{A}$. $\square$

Definition 7.10. *$\mathcal{A} \subseteq \mathcal{B}$ rings, $\overline{\mathcal{A}} := \{x \in \mathcal{B} | x$ 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 $\mathcal{A} \Longrightarrow x \in \overline{\mathcal{A}} \Longrightarrow \overline{\overline{\mathcal{A}}} = \overline{\mathcal{A}}$ $\square$

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 $\mod \mathfrak{b}$. $\square$

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 $S^{-1}\mathcal{A}$. $\square$

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

$$r^n = -(a_1 r^{n-1} s + a_2 r^{n-2} s^2 + ... + a_n s^n)$$

$\Longrightarrow s|r^n$, $gcd(r^n, s) = 1, \Longrightarrow s \in \mathbb{Z}^{\times} \Longrightarrow x \in \mathbb{Z}$. □

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. 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.

$$x^n + k_1 x^{n-1} + ... + k_n = 0$$

□

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. 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 $\Longleftrightarrow$ $\mathcal{B}$ is a field) provided that $\mathcal{A}$ and $\mathcal{B}$ are domains

(ii) Let $\mathfrak{q} \subseteq \mathcal{B}$ prime, and $\mathfrak{p} := \mathfrak{q} \cap \mathcal{A}$. prime (in $\mathcal{A}$). Then $\mathfrak{q}$ maximal $\Longleftrightarrow$ $\mathfrak{p}$ maximal.

Proof. "$(i) \Longrightarrow$", 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 $a_n \in \mathcal{A}^{\times}$) ¿¿¿¿¿¿¿¿¿. ☐

Primes in integral extensions

7.3 Lecture 22

Corollary 7.23. *If $(\mathcal{A}, \mathfrak{m})$: local ring and $\mathcal{A} \subseteq \mathcal{B}$: integral extension, then*

$$\{\textit{primes } \mathfrak{q} \textit{ of } \mathcal{B} \textit{ with } \mathfrak{q} \cap \mathcal{A} = \mathfrak{m}\} = \{\textit{maximal ideals in } \mathcal{B}\}$$

Proof. $\subseteq$: $\mathfrak{q} \cap \mathcal{A}$: maximal $\Longrightarrow$ $\mathfrak{q}$ maximal by (ii) if Lemma above.
$\supseteq$: $\mathfrak{q}$ maximal implies by Lemma above $\mathfrak{q} \cap \mathcal{A}$ maximal, $\mathfrak{q} \cap \mathcal{A} = \mathfrak{m}$. ☐

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) (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.)

(ii) (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 $\mathfrak{q} \cap \mathcal{A} \supsetneq \mathfrak{q}' \cap \mathcal{A}$

(iii) (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 $\mathfrak{p}_1 \subseteq ....subseteq \mathfrak{p}_n = \mathfrak{p} \in Spec(\mathcal{A})$, then there exists a chain $\mathfrak{q}_1 \subseteq ... \subseteq \mathfrak{q}_n = \mathfrak{q} \in Spec(\mathcal{B})$ 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, $\mathfrak{a} := \mathfrak{b} \cap \mathcal{A}$*

1. *$dim(\mathcal{A}) = dim(\mathcal{B})$*
2. *$dim(\mathcal{A}/\mathfrak{a}) = dim(\mathcal{B}/\mathfrak{b})$*
3. *$ht(\mathfrak{b}) \leq ht(\mathfrak{a})$*

Proof. (i),

(ii),

(iii), $ht(\mathfrak{b}) \subseteq ht(\mathfrak{a}) = \inf_{\mathfrak{p} \supseteq \mathfrak{a}} ht(\mathfrak{p})$. ¿¿¿¿¿5 Want: if $\mathfrak{p} \supseteq \mathfrak{a}$, then $ht(\mathfrak{p}) \geq ht(\mathfrak{b})$ ¿¿¿¿¿¿¿¿¿6 □

Proof. (of Theorem 7.25) Lying over: Let $\mathfrak{p} \in Spec(\mathcal{A})$. $\mathcal{A}_{\mathfrak{p}} \subseteq \mathcal{B}_{\mathfrak{p}}$ integral, where $\mathcal{A}_{\mathfrak{p}}$ is local with maximal $\mathfrak{m} := \mathfrak{p}\mathcal{A}_{\mathfrak{p}}$.

¿¿¿¿¿¿¿¿3

Going up:

¿¿¿¿¿¿4 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 $\mathfrak{q}' \in Spec(\mathcal{B})$

Then $\mathfrak{q}'$ lies over $\mathfrak{p}'$ □

Galois Transitivity

Definition 7.27. *A **normal** extension L/K of fields, is an extension s.t., each irredusible $f \in K[X]$ 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."

NB $char(K) = 0 \Longrightarrow$ 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:*

$$\#Hom_K(K(\alpha), \overline{K}) = 1 \ \forall \alpha \in L$$

FACT: let L/K be a normal extension. Let $G := Aut(L/K), L^G := \{\alpha \in L : g(\alpha) = \alpha \forall g \in G\}$ ¿¿¿¿¿¿¿.7

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) $\mathfrak{q} \in Spec(\mathcal{B}) \Longrightarrow g(\mathfrak{q}) \in Spec(\mathcal{B}), \forall g \in G$???????

(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) aa

(ii) ¿¿¿¿¿¿¿¿¿8

(iii) Assume first that L/K finite, then $\#G < \infty$. Let $\mathfrak{q}, \mathfrak{q}' \in Spec(\mathcal{B})$ 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, claim $\Longrightarrow \exists g \in G, \mathfrak{q}; \subseteq g(\mathfrak{q})$ both lying over $\mathfrak{q}$ (by part (ii)), then by incomparability we know $\mathfrak{q}' = g(\mathfrak{q})$, as desired.

Proof of the claim: Let $x \in \mathfrak{q}'$. St $y := \prod_{g \in G} g(x) \in L^G$. 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 belong s to K. Since $\mathcal{A}$ is normal, we get that $y^n \in \mathcal{A} \cap \mathfrak{q}'$ ¿¿¿¿¿¿10 Since $\mathfrak{q}$ is prime, and $y^n = \prod_{g \in G} g(x)^n$, deduce that $g(x) \in \mathfrak{q}$ for some $g \in G$, hence that $x \in g^{-1}(\mathfrak{q})$. 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.

□

7.4 Lecture 23

In this lecture, we will continue to proof the part (iii) of Theorem 7.31 for infinite field extension L/K.

Re call 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 lie over $\mathfrak{p}$

$$A := \left\{ \begin{array}{l} (E,g) : E \text{ as above} \\ \qquad g \in Aut(E/K) \\ \qquad \text{s.t. } g(\mathfrak{q} \cap E) = \mathfrak{q}_2 \cap E \end{array} \right\}$$

define an order on A by $(E, q \leq (E', g'))$ iff $E \subseteq E', g'|_E = g$

<u>Want</u>: $\exists g \in Aut(L/K)$ s.t. $(L, g) \in A$

$A \neq \emptyset$ $(K, id) in A$. 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 $(E, g) \in A$

$$\begin{cases} E := \cup_i E_i \\ \exists! g \in Aut(E/K) \\ \text{s.t. } g|_{E_j} = g_j \end{cases}$$

Thus by Zorn;s lemma, $\exists$ maximal $(E, g) \in A$. We want to claim that $E = L$.

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

¿¿¿¿¿¿¿¿¿¿¿¿¿¿1

Let $\tilde{g} \in Aut(E'/K)$ be any extension of g such that $\tilde{g}$ exists.

Then $\tilde{g}(\mathfrak{q}_q \cap E')$ 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)

Then let's talk about the so called going-down property.

Let $\mathcal{A} \subseteq \mathcal{B}$ ring extension. We say that $\mathcal{A} \subseteq \mathcal{B}$ has property **Going-Down** (GD) if

$$\forall \text{ primes}, \mathfrak{p}' \subsetneq \mathfrak{p} \subset \mathcal{A}, \mathfrak{q} \subset \mathcal{B}$$

with $\mathfrak{q} \cap \mathcal{A} = \mathfrak{p}$, $\exists$ prime $\mathfrak{q}' \subsetneq \mathfrak{q}$ with $\mathfrak{q}' \cap \mathcal{A} = \mathfrak{p}'$

¿¿¿¿¿¿¿2

See P239 of Eisenbud or 32-33 of Matsumura for a non-example.

Theorem 7.32. *Let $\mathcal{A} \subseteq \mathcal{B}$ be domains with $\mathcal{A}$ normal, $\mathcal{A}$ normal, $\mathcal{B}$ integral over $\mathcal{A}$. Then $\mathcal{A} \subseteq \mathcal{B}$ has GD.*