

Personal Notes for Commutative Algebra

by P. Nelson

Texed by Lin-Da Xiao

October 26, 2017

Contents

1	Rings, ideals, radicals	2
1.1	Lecture 1. Motivation and Basics by Paul Steinmann	2
1.2	Lecture 2. local rings, coprime ideals, ideal quotients by Paul Steinmann	6
2	Modules	10
2.1	Lecture 3. Modules, Exact sequences by Professor Kowalski	10
2.2	Lecture 4. Snake Lemma, Tensor Product by Professor Kowalski	16
2.3	Lecture 5. Properties of Tensor Product	23
2.4	Lecture 6. Flatness	28
3	Localization	33
3.1	Lecture 7 : Localization of rings	33
3.2	Lecture 8: Properties of localization of rings and localization of module	38
3.3	Lecture 9: Localization of Modules	42
4	Noetherian Ring and Nullstellensatz	45
4.1	Lecture 10	45
4.2	Lecture 11	49
4.3	Lecture 12	52

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. In particular for a ring homomorphism $f : R \rightarrow S$. 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 $f : \mathbb{R}^n \rightarrow \mathbb{R}$. 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 $R := \mathbb{K}[x_1, \dots, x_n]$. Def: For a subset $S \subset R$ we define the **affine algebraic variety** by

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

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

$$\bigcap_{i \in I} V(S_i) = V(\bigcup_{i \in I} S_i)$$

- 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 $S \subset S' \subset R$, 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 $\text{rad}(\mathfrak{a}) := \{a \in R | \exists n \geq 1 \text{ s.t. } a^n \in \mathfrak{a}\} \subset R$. An ideal $\mathfrak{a} \subset R$ with $\text{rad}(\mathfrak{a}) = \mathfrak{a}$ is called **radical**.

Remark 1.7. Fact, for every ideal $\mathfrak{a} \subset R$ we have $\mathfrak{a} \subset \text{rad}(\mathfrak{a})$.

$\text{rad}(\mathfrak{a})$ 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

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

An important consequence of the theorem:

the maps V and I induce the one to one correspondence between

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

and this correspondence inverse the inclusion.

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

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

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. \square

Weak Nullstellensatz the ideals \mathfrak{m}_x are precisely the maximal ideals of $\mathbb{K}[x_1, \dots, x_n]$, 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

$$\{\text{max ideals of } R \text{ polynomial ring } \mathbb{K}[X_1, \dots, X_n]\} \iff \{\text{Points in } \mathbb{K}^n\}$$

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 $N : \text{rad}((0))$ 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 $x^{nk} = 0$, $x \in \mathcal{N}$. \square

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 $\Sigma := \{\mathfrak{a} \subset A \text{ ideals} \mid \forall n > 0 : f^n \notin \mathfrak{a}\}$. We will apply Zorn's lemma. We have

1. $(0) \in \Sigma$, so Σ is nonempty,
2. Σ is partially ordered by inclusion.
3. For any chain $(\mathfrak{a}_i)_{i \in I} \subset \Sigma$, the set $\mathfrak{a} := \cup_{i \in I} \mathfrak{a}_i$ is an ideal and for all $n > 0$, we have $f^n \notin \mathfrak{a}$, hence $\mathfrak{a} \in \Sigma$. By Zorn's lemma we conclude that there is a maximal element $\mathfrak{p} \in \Sigma$. We show that \mathfrak{p} is a prime ideal.

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

Remember let $f : A \rightarrow B$ 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, $\pi : A \rightarrow A/\mathfrak{a}$. 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 $\text{rad}(\mathfrak{a})$ is the intersection of all prime ideals which contain \mathfrak{a} .*

Proof. consider the homomorphism $\pi : A \rightarrow A/\mathfrak{a}$. Then $\text{rad}(\mathfrak{a}) = \pi^{-1}(\mathcal{N}_{A/\mathfrak{a}})$. 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. \square

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. “ \implies ” 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.

“ \impliedby ” 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. \square

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. $(a_0(1 - g))^{-1} = a_0^{-1}(1 + g + g^2 + \dots)$*

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. \square

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

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

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

¹In 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 $\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1} (1 - y_i) \equiv 1 \pmod{\mathfrak{a}_n}$. 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) “ \implies ”, Suppose φ is surjective. Let $i \neq j$, There exists an element $x \in A$ s.t. $\varphi(x) = (0, \dots, 0, 1, 0, \dots, 0)$, nonzero only at the i -th entry. Thus $x \equiv 1 \pmod{\mathfrak{a}_i}$ and $x \equiv 0 \pmod{\mathfrak{a}_j}$. So $1 = (1 - x) + x \in \mathfrak{a}_i + \mathfrak{a}_j$.

“ \impliedby ” We show that for all $k \in \{1, \dots, n\}$ there exists an element $x \in A$ s.t. $\varphi(x) = (0, \dots, 0, 1, 0, \dots, 0)$, nonzero at the k -th entry. Let $k \in \{1, \dots, n\}$. For every $j \in \{1, \dots, n\} \setminus \{k\}$. 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 $x \equiv 0 \pmod{\mathfrak{a}_j}, \forall j \neq k$ and $x = \prod_{i \neq k} (1 - u_i) \equiv 1 \pmod{\mathfrak{a}_k}$. Hence, $\varphi(x) = (0, \dots, 0, 1, 0, \dots, 0)$ 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. $\text{rad}(\mathfrak{a}), \text{rad}(\mathfrak{b})$ are coprime. Then $\mathfrak{a}, \mathfrak{b}$ are coprime.*

Proof. In fact, we have

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

Details in the exercise sheet.

□

Proposition 1.27.

(i) Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n \subset A$ 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 $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subset A$ 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 $y \equiv \prod_{j \neq k} x_j \pmod{\mathfrak{p}_k}, \forall k$. 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 $i \in \{1, \dots, n\}$ 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. \square

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

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

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

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

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

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

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

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

where we extend rad to arbitrary subsets. \square

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 $f : A \rightarrow B$ 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 $f(\mathfrak{a})$
For an ideal $\mathfrak{b} \subset B$. We define the **contraction** of \mathfrak{b} via f to be the ideal

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

Properties: Let $f : A \rightarrow B$ 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 $f_* : C \rightarrow E$ is a bijection with inverse f^* .

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

2 Modules

2.1 Lecture 3. Modules, Exact sequences by Professor Kowalski

Outline of this chapter

- Definition examples and Nakayama's Lemma
- exact sequences , snake lemma
- tensor products
- Algebra over a ring

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

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

$$\begin{aligned}\mathcal{A} \times M &\rightarrow M \\ (a, x) &\mapsto ax\end{aligned}$$

so that

$$\begin{aligned}a(x + y) &= ax + ay \\ (a + b)x &= ax + bx \\ a(bx) &= abx \\ 1x &= x\end{aligned}$$

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 $f : M \rightarrow N$ is **\mathcal{A} -linear** if $f(ax + by) = af(x) + bf(y)$. The set of such $\rho : M \rightarrow N$ is denoted $\text{Hom}_{\mathcal{A}}(M, N)$. It is an \mathcal{A} -module with

$$\begin{aligned}(f + g)(x) &= f(x) + g(x), \\ (af)(x) &= af(x).\end{aligned}$$

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

Definition 2.4. $f : M \rightarrow N$ is an **isomorphism** iff $\exists g : N \rightarrow M$ s.t. $g \circ f = \text{id}_N$ and $f \circ g = \text{id}_M$.

Remark 2.5. $Q \rightarrow (h)M \rightarrow (f)N \rightarrow (g)P$, then for any P , we get

$$\begin{aligned}f^* : \text{Hom}_{\mathcal{A}}(M, P) &\rightarrow \text{Hom}_{\mathcal{A}}(M, P) \\ g &\mapsto g \circ f\end{aligned}$$

and

$$\begin{aligned} f_* : \text{Hom}_{\mathcal{A}}(Q, M) &\rightarrow \text{Hom}_{\mathcal{A}}(Q, N) \\ h &\mapsto f \circ h \end{aligned}$$

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 $\pi : M \rightarrow M/N$ is \mathcal{A} -linear. $a(x+N) = ax+N$ is well defined because $aN \subset N$.

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

- $\text{Ker}(f) = f^{-1}(\{0\}) \subset M$ is a submodule of M .
- $\text{Im}(f) = f(M) \subset N$ is a submodule of N .
- $\text{Coker}(f) = N/\text{Im}(f)$ is an \mathcal{A} -module.

Remark 2.8. 1. $\text{ker}(f) = 0 \iff f$ is injective.

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

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

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

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

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

and

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

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

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

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

$$\begin{aligned}\langle X \rangle &= \{\text{linear combination of elements of } X\} \\ &= \left\{ \sum_i a_i x_i \mid K \geq 0\mathbb{Z}, a_i \in \mathcal{A}, x_i \in X \right\}\end{aligned}$$

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.

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

A is finitely generated by 1 however, the ideal $I = (X_1, \dots, X_n, \dots)$ is not finitely generated

Lemma 2.11.

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

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

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

Rigorously: $\pi : L \rightarrow L/M$ is surjective

$\implies \bar{\pi} : L/N \rightarrow L/M$ is surjective

and $\text{Ker}(\bar{\pi}) = M/N$ so

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

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,

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

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 just $\bigcap_{\mathfrak{m} \subset \mathcal{A}} \mathfrak{m}$, where \mathfrak{m} are 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 $\{x_1, \dots, x_n\}$ 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

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

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

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

and $(1 - c_n) \equiv 1 \pmod{I} \implies c_n \in \text{the Jacobson radical}$, 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. □

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

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

$$M/N = 0.$$

□

Corollary 2.18. *\mathcal{A} local ring, $\mathfrak{m} \subset \mathcal{A}$ the maximal ideal. M fin. gen. Then if $(x_1, \dots, x_n) \in M$ 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. $N = \langle x_1, \dots, x_n \rangle$ and apply Nakayama's lemma. □

Exact sequence

Definition 2.19. (1) $M' \rightarrow (f)M \rightarrow (g)M''$ is **exact** if $\text{Im}(f) = \ker(g)$
(2) $M' \rightarrow (f_1)M \rightarrow (f_2)M'' \rightarrow \dots$ is **exact** if it is exact at each node.

Example 2.20.

1. $0 \rightarrow M \xrightarrow{g} M''$ is exact, is equivalent to say that g is injective
2. $M' \xrightarrow{f} M \rightarrow 0$ is exact, it is equivalent to say that f is surjective.
3. "Short exact sequence" $0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0$ For instance,

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

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

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

the exact sequence does not split.

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

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

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

then we have a map $\delta : \text{Ker}(f'') \rightarrow \text{Coker}(f')$ s.t.

$0 \rightarrow \text{Ker}(f') \rightarrow \text{Ker}(f) \rightarrow \text{Ker}(f'') \xrightarrow{\delta} \text{Coker}(f') \rightarrow \text{Coker}(f) \rightarrow \text{Coker}(f'') \rightarrow 0$
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:

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

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

1. Exactness at K'

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

5. Construct δ

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

δ

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

6. Exactness at K''

For $x \in K$, we formally write

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

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

7. Exactness at C'

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

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

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

□

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

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

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

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

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

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

3. $\text{Ker}(u^*) \subset \text{Im}(v^*)$

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

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

We know that v induces an isomorphism

$$\begin{array}{ccccc} \text{Im}(v) = M'' & \xleftarrow{v} & M & \xrightarrow{f} & N \\ & \nwarrow \bar{v} & \downarrow p & \nearrow \bar{f} & \\ & & M/\text{Ker}(v) & & \end{array}$$

\bar{v}^{-1} (curved arrow from $M/\text{Ker}(v)$ to M'')

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

We then give an example where the surjectivity of u^* fails

Consider $\mathcal{A} = \mathbb{Z}$, $0 \rightarrow \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$ is exact.

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

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

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\times 2} & \mathbb{Z} \\ & & \downarrow \text{Id} & \nearrow ?g & \\ & & \mathbb{Z} & & \end{array}$$

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

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

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

1. Let $N = \text{Coker}(v)$ and $[p : M'' \longrightarrow \text{Coker}(v)] \in \text{Hom}(M'', N)$, then $v^*(p) = p \circ v = 0$. Since v^* is injective, we have $p = 0$, in other words $M'' = \text{Ker}(p) = \text{Im}(v)$ so v is surjective.
2. Take $N = M''$ and $f = \text{Id}_{M''}$, $(u^* \circ v^*)(f) = 0$ means $\text{Id}_{M''} \circ v \circ u = 0 \implies v \circ u = 0$, hence $\text{Im}(u) \subset \text{Ker}(v)$.
3. Take $N = M/\text{Im}(u)$, and $p : M \longrightarrow N$ projection, we have $u^*(p) = p \circ u = 0$. So $p \in \text{Ker}(u^*)$, so there exists $f \in \text{Hom}(M'', N)$ s.t. $v^*(f) = f \circ v = p$.

$$\begin{array}{ccc}
 M' & \xrightarrow{f} & N = M/\text{Im}(u) \\
 \uparrow v & \nearrow p & \\
 M & &
 \end{array}$$

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

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

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

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

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

$\text{Bil}_{\mathcal{A}}(M, N, P)$ 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 $\text{Bil}_{\mathcal{A}}(M, N; P) = \text{Hom}_{\mathcal{A}}(M \otimes_{\mathcal{A}} N, P)$. $\text{Bil}_{\mathcal{A}}(M, N; P)$ 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 $f : T \rightarrow P$ s.t. the following diagram commutes.

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

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** $M \times N \rightarrow M \otimes N$. That is to say : there exists a module T (denoted $M \otimes N$ or $M \otimes_{\mathcal{A}} N$) and a bilinear map $f : M \times N \rightarrow T$. By “best possible”, we mean: For all module P and all bilinear map $b : M \times N \rightarrow P$, there exists a unique $\tilde{b} : T \rightarrow P$ s.t. the following diagram commutes.*

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

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

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

Proof. **Uniqueness**

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

Consider $k \circ j : T \rightarrow T$, apply the universal property with $P := T$, $b := f$

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

We know $\exists! \tilde{b}$ s.t. the diagram commutes. Then we have $\tilde{b} \circ f = f$, but another obvious map having this property is just id_T . Then, we get to the conclusion $k \circ j = id_T$ by the uniqueness of \tilde{b} . Similarly, we get $j \circ k = id_T$. Altogether, we conclude that (T, f) is unique up to unique isomorphism.

Existence

Form the free module $C := \mathcal{A}^{M \times N}$, where

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

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

Let submodule $D \subseteq C$, then there is an induced map $\bar{g} : M \times N \rightarrow C/D$ for defining map $g : M \times N \rightarrow C$ 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 $\bar{g} : M \times N \rightarrow C/D$ is bilinear.
- D is the submodule generated by the following elements

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

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

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

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 $\bar{g} : M \times N \rightarrow C/D = T$. \square

Also note that, in general

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

, 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:

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

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 $f : M \otimes (N_1 \oplus N_2) \rightarrow M \otimes N_1 \oplus M \otimes N_2$.

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

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

define

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

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

$$\begin{aligned} \mathcal{A} \otimes \mathcal{A} &\cong \mathcal{A} \\ x \otimes y &\mapsto xy \end{aligned}$$

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

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

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.

$$\mathcal{A}^m \ni x = x_1 e_1^{(1)} + \dots + x_m e_m^{(1)}, \quad x_i \in \mathcal{A}$$

$$\mathcal{A}^n \ni y = y_1 e_1^{(1)} + \dots + y_n e_n^{(1)}, \quad y_i \in \mathcal{A}$$

Then

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

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

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

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

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

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

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

Remark 2.30. Extension of scalars Consider a ring morphism $f : \mathcal{A} \rightarrow \mathcal{B}$ 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.

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

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 $\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \ni 2 \otimes 1 = 0$

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 always 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.

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

In other words,

$$M' \subset M \implies "M' \otimes N \subset M \otimes N"$$

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

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

$z \neq 0 \implies \exists i \in I$ 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*

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

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: " \implies " 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 $f = (f_1, \dots, f_m)$. $\mathcal{A} = \mathbb{R}$, $N = \mathbb{C} \cong \mathbb{R} \oplus \mathbb{R}i$ is free, then by the above corollary, we know N is flat. Then S has a solution over \mathbb{R} iff $\text{Ker}(f) \neq 0$,

and S has a solution over \mathbb{C} iff $\text{Ker}(f \otimes 1_{\mathbb{C}}) \neq 0$. 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, $\text{Im}(f \otimes 1) \subseteq \text{Ker}(g \otimes 1)$ because $(g \otimes 1) \circ (f \otimes 1) = (g \circ f) \otimes 1 = 0$. Then it remains to show

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

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

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

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

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

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

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

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

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

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

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

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

and

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

\implies

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

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

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. \square

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 \mathcal{A} -modules). Tensoring it with M , we have

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

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

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

□

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. Tensoring 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

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

, 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. $m \in M$ $am = 0 \implies m = 0$

Theorem 2.43.

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

Proof. Bosch section 4.2 □

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}

$$\begin{aligned} V^* \otimes W &\cong \text{Hom}_{\mathbb{F}}(V, W) \\ l \otimes w &\mapsto [v \mapsto l(v)w] \end{aligned}$$

3 Localization

3.1 Lecture 7 : Localization of rings

Motivation For \mathcal{A} an integral domain, we defined the quotient field $\text{Frac}(\mathcal{A})$. In general, one may want to invert part of \mathcal{A} . For example, we may consider $\mathbb{Z}[1/2] = \{a/(2^n) | a \in \mathbb{Z} \text{ and } n \in \mathbb{N}\}$. 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 $\text{Frac}(\mathcal{A})$ generated by \mathcal{A} and $\{1/s | s \in S\}$.

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

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

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

$$\overline{S} := \{s_I | I = (i_1, \dots, i_n), \forall n, s_{i_n} \in S\}$$

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

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

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

Lemma 3.3. “ \sim ” is indeed an equivalence relation.

Proof. reflectivity and symmetricity are trivial, for the transtivity

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

\implies

$$\exists t \in S : as't = a'st$$

$$\exists t' \in S : a's''t' = a''s't'$$

$$as''(tt's') = as'ts''t' = a's''t'st = a''s(tt's')$$

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

□

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:

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

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

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

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.

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

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 $S^{-1}\mathcal{A} = \text{Frac}(\mathcal{A})$.

Lemma 3.6. 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) $\text{Ker}(\iota) = \{a \in \mathcal{A} \mid sa = 0 \text{ for some } s \in S\}$
- (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.
- (b) $a \in \text{Ker}(\iota) = \{b \in \mathcal{A} \mid \frac{b}{1} = \frac{0}{1}\} \iff \exists t \in S : t(a1 - 01) = ta = 0 \iff a \in \{\text{Zero divisors in } \mathcal{A}\}$.
- (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. $t \cdot 1 = 0$, $\iff S \ni 0$.
- (e) “ \implies ” Suppose $\mathcal{A} \neq \{0\}$, then ι is isomorphism $\iff \iota$ is surjective and injective $\iff \forall \frac{a}{s} \in S^{-1}\mathcal{A} : \exists c \in \mathcal{A}$ s.t. $\frac{a}{s} = \frac{c}{1}$ and S has no zero divisors. Then we know, $\frac{1}{s} = \frac{c}{1} \implies \exists t(s \cdot c - 1) = 0$, and by the fact S has no zero divisors $s \cdot c = 1$, which means $S \subseteq \mathcal{A}^\times$.
“ \impliedby ” Assume $\mathcal{A} \neq \{0\}$. $S \subseteq \mathcal{A}^\times$, then S does not contain any zero divisors. $\forall \frac{a}{s} \in S^{-1}\mathcal{A}, \exists v \in S$ s.t. $sv = 1$. Then $\frac{a}{s} = \frac{av}{1} \in \text{Im}(\iota)$, because $asv = a$.

□

Example 3.7. X any set $U \subseteq X$ any subset. $\mathcal{A} := \{\text{functions } f : X \rightarrow \mathbb{R}\}$ is a ring of the the multiplication is defined value-wisely, $S := \{f \in \mathcal{A} \mid f(x) \neq 0, \forall x \in U\}$ is multiplicatively closed. Question, what is the localization $S^{-1}\mathcal{A}$?

Lemma 3.8. Let $B := \{\text{functions } U \rightarrow \mathbb{R}\}$. Then the natural map $j : S^{-1}\mathcal{A} \rightarrow B$ 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 $t : 1_U = [x \mapsto 1 \text{ for } 1 \in U \text{ and } 0 \text{ for } x \notin U]$ \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 3.9. $Hom(S^{-1}\mathcal{A}, \mathcal{B}) \cong \{f : \mathcal{A} \longrightarrow \mathcal{B} \text{ s.t. } f(S) \subseteq \mathcal{B}^\times\}$ 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 $\iota : \mathcal{A} \longrightarrow S^{-1}\mathcal{A} : a \mapsto \frac{a}{1}$.

$$\begin{array}{ccc} S & \hookrightarrow & \mathcal{A} \xrightarrow{f} \mathcal{B} \\ & & \downarrow \iota \nearrow \exists! \tilde{f} \\ & & T \end{array}$$

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:

$$\frac{a}{s} = \frac{a'}{s'} \stackrel{?}{\implies} f(a)f(s)^{-1} = f(a')f(s')^{-1}$$

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

Example 3.10. (*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 the extension and contraction of ideals as $\mathfrak{b}^c = \varphi^*(\mathfrak{a}) := \varphi^{-1}(\mathfrak{b})$ and $\mathfrak{a}^c = \varphi_*(\mathfrak{a}) := \mathcal{B}\varphi(\mathfrak{a})$

Notice that $\mathfrak{q} \subseteq \mathcal{B}$ prime $\implies \varphi^*(\mathfrak{q})$ prime, thus $\varphi^* : \text{Spec}(\mathcal{B}) \longrightarrow \text{Spec}(\mathcal{A})$.

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

Proposition 3.11.

- (a) $\iota^* : \text{Spec}(S^{-1}\mathcal{A}) \longrightarrow \{\mathfrak{p} \in \text{Spec}(\mathcal{A}) | \mathfrak{p} \cap S = \emptyset\}$ is a bijection.
- (b) For any ideal $\mathfrak{a} \subseteq \mathcal{A}$, $\iota_*(\mathfrak{a}) = \{a/s | a \in \mathfrak{a}, s \in S\}$
- (c) $\iota_*(\mathfrak{a}) = S^{-1}(\mathcal{A}) \iff \mathfrak{a} \cap S \neq \emptyset$
- (d) For any ideal $\mathfrak{b} \subseteq S^{-1}\mathcal{A}$, $\varphi_*(\varphi^*(\mathfrak{b})) = \mathfrak{b}$

Proof.

- (a) $\mathfrak{q} \subseteq S^{-1}\mathcal{A}$, $\iota^*(\mathfrak{q}) = \iota^{-1}(\mathfrak{q})$, $\iota(S) \subseteq (S^{-1}\mathcal{A})^\times, \implies \iota(S) \cap \mathfrak{q} = \emptyset$ otherwise $1 \in \mathfrak{q}$ (In fact this part of proof also works for other ideals.)
- (b) Just check that $S^{-1}\mathcal{A} \cdot V \subset V$
- (c) $\iota_*(\mathfrak{a}) = S^{-1}\mathcal{A} \iff \exists a \in \mathfrak{a}, s \in S \text{ s.t. } a/s = 1/1 \iff \exists t \in S \text{ s.t. } \mathfrak{a} \ni ta = ts \in S$, 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) $\varphi_*(\varphi^*(\mathfrak{b})) \subset \mathfrak{b}$ 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 $a \in \varphi^*(\mathfrak{b}) \implies a/s \in \varphi_*(\varphi^*(\mathfrak{b}))$.

□

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

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

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

Proposition 3.12.

$$\{\mathfrak{p} \in \text{Spec}(\mathcal{A}) \mid \mathfrak{p} \cap S = \emptyset \ (S \subseteq \mathcal{A} - \mathfrak{p})\} \longleftrightarrow \{\text{Spec}(S^{-1}\mathcal{A})\}$$

is bijection.

- $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \iff \iota^*\mathfrak{q}_1 \subseteq \iota^*\mathfrak{q}_2$
- $k(\mathfrak{p}) := \text{Frac}(\mathcal{A}/\mathfrak{p})$ is called the residue field of the prime ideal \mathfrak{p} .

Then the above bijection induces isomorphism $k(\iota^*\mathfrak{q}) \cong k(\mathfrak{q})$

Example 3.13. $\mathcal{A} = \mathbb{Z}$, and $\mathfrak{p} = (p)$ where p is a prime number. $k(\mathfrak{q}) = \text{Frac}(\mathbb{Z}/p) = \mathbb{Z}/p$.

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

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

Example 3.14. $\mathfrak{p} = (y) \subseteq \mathcal{A} = \mathbb{C}[x, y]$, $\mathcal{A}/\mathfrak{p} \cong \mathbb{C}[x]$, $k(\mathfrak{p}) \cong \mathbb{C}(x)$

Proof. (Proof of the proposition) the proof contains the following points

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

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

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

Example 3.15. $S = S_f = \{f^n : n \geq 0\} \implies S^{-1}\mathcal{A} = \mathcal{A}_f = \mathcal{A}[1/f]$. Let $\mathfrak{p} \cap S \neq \emptyset \iff \text{some } f^n \in \mathfrak{p} \iff f \in \mathfrak{p}$. Then $\text{Spec}(\mathcal{A}_f) \cong \{\mathfrak{p} \in \text{Spec}(\mathcal{A}) \mid f \in \mathfrak{p}\}$

Example 3.16. $\mathcal{A} = \mathbb{Z}, f = 2, \mathcal{A}_f = \mathbb{Z}[1/2]$
 $\{\text{primes in } \mathbb{Z}[1/2]\} \cong \{(0), (3), (5), \dots\} \subseteq \text{Spec}(\mathbb{Z})$

Example 3.17. $\mathcal{A} = \mathbb{C}[x, y]$, there is a bijection between $\{\text{maximal ideals in } \mathcal{A}\}$ and \mathbb{C}^2 . The maximal ideal $\{f \in \mathbb{C}[x, y] \mid f(X_0, Y_0) = 0\} = (x - X_0, y - Y_0)$ corresponds to the point $(X_0, Y_0) \in \mathbb{C}^2$
Fix $f \in \mathbb{C}[x, y], f \neq 0$, e.g. $f = u - x^2$ Then

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

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

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

$$\mathcal{A} \longrightarrow \mathcal{A}_f \longrightarrow \mathcal{A}_{fg}$$

Example 3.18. \mathcal{A} an integral domain, $\mathcal{A}_f \subseteq \mathcal{A}_{fg}$ ($\frac{a}{(f)^n} = \frac{ag^n}{(fg)^n}$), $\text{Frac}(\mathcal{A}) = \cup_f \mathcal{A}_f$. For any $\mathfrak{p} \in \text{Spec}(\mathcal{A}_f) \subseteq \mathcal{A}$, $\mathcal{A}_f \implies k(\mathfrak{p})$

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

Aside: \mathcal{A} is a local ring $\iff \exists 1\mathfrak{m} \in \text{Specm}(\mathcal{A}) \iff \exists \text{ideal } \mathfrak{m} \text{ with } 1 + \mathfrak{m} \subseteq \mathcal{A}^\times, \mathfrak{m} \text{ maximal, } \iff \mathcal{A} - \mathfrak{m} \subseteq \mathcal{A}^\times$
 $\mathfrak{p} \subseteq \mathcal{A} \text{ prime} \implies \mathcal{A}_{\mathfrak{p}} := S_{\mathfrak{p}}^{-1}\mathcal{A}$

Proposition 3.19. (a) $\text{Spec}(\mathcal{A}_{\mathfrak{p}}) \cong \{\mathfrak{q} \in \text{Spec}(\mathcal{A}) \mid \mathfrak{q} \subseteq \mathfrak{p}\}$

(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.

$$S_{\mathfrak{p}}^{-1} \stackrel{\iota_*}{\cong} \{\mathfrak{q} \in \text{Spec}(\mathcal{A}) \mid \mathfrak{q} \cap S_{\mathfrak{p}} = \emptyset \ (\mathfrak{q} \subseteq \mathfrak{p})\}$$

. 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. \square

Example 3.20. $\mathfrak{p} = (p) \subseteq \mathbb{Z} = \mathcal{A}$, then $\mathcal{A}_{\mathfrak{p}} = \mathbb{Z}_{(p)}$ is local ring with maximal ideal $\mathfrak{p}_{\mathfrak{p}}$ generated by image of \mathfrak{p} . $\text{Spec}(\mathbb{Z}_{(p)}) \cong \{\mathfrak{q} \in \text{Spec}(\mathbb{Z}) \mid \mathfrak{q} \subseteq \mathfrak{p}\} = \{(0), (p)\}$

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 3.21. 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 3.22. $\Omega \subseteq \mathbb{C}$ open \mathcal{A} is the set of holomorphic germs $f : \Omega \longrightarrow \mathbb{C}$. Fix $p \in \Omega$. and set $\mathfrak{p} = \{f \in \mathcal{A} \mid f(p) = 0\}$. 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. \square

Example 3.23. $\mathcal{A} = \mathbb{C}[x, y], \mathfrak{p} = (y)$

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

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 $\mathbb{C}(x)$.

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

$$\text{Spec}(\mathcal{A}_{\mathfrak{p}}) \cong \{\mathfrak{q} \in \text{Spec}(\mathcal{A}) \mid \mathfrak{q} \subseteq (x, y)\}$$

Then

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

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

localization of module

Definition 3.24. $S \subseteq \mathcal{A}$ 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 3.25. $S^{-1}\mathcal{A} \otimes_{\mathcal{A}} M \cong S^{-1}M$, 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. □

Moreover, we can also define the localization of morphisms,

Definition 3.26. Given $f : M \longrightarrow N$ a morphism of \mathcal{A} -module. S^{-1} . We define

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

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

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

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

e.g. $\mathfrak{p} \in \text{Spec}(\mathcal{A})$, 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 $M_{\mathfrak{p}}, \forall \mathfrak{p} \in \text{Spec}(\mathcal{A})$

3.3 Lecture 9: Localization of Modules

$S \subseteq \mathcal{A}$ then we can define $S^{-1}\mathcal{A}$. Also we define **localization of modules**: $S^{-1}M \cong S^{-1}\mathcal{A} \otimes_{\mathcal{A}} M$. The localization of module defines a functor $S^{-1}: f: M \rightarrow N$, induces a morphism of $S^{-1}\mathcal{A}$ -modules $S^{-1}f: S^{-1}M \rightarrow S^{-1}N$ 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 $\text{Ker}(S^{-1}g) \supseteq \text{Im}(S^{-1}f)$. For the converse inclusion, consider an element $\frac{x}{s} \in \text{Ker}(S^{-1}g) | x \in Ms \in S$, $S^{-1}g(\frac{x}{s}) = \frac{g(x)}{s} = \frac{0}{1}$, $\implies \exists t \in S$ s.t. $g(tx) = tg(x) = 0$. $\text{Im}(f) = \text{Ker}(g) \implies \exists y: f(y) = tx$. Then we check that $\frac{x}{s} = (S^{-1}f)(\frac{y}{st}) = \frac{f(y)}{st} = \frac{tx}{st} = \frac{x}{s}$, which concludes the proof. \square

Corollary 3.27. $S^{-1}\mathcal{A}$ is flat \mathcal{A} -module.

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

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

is exact because it is just

$$0 \rightarrow S^{-1}M' \rightarrow S^{-1}M$$

\square

Lemma 3.28. S^{-1} commutes with:

- finite sums
- finite intersections
- Kernel
- quotients

◊◊◊◊◊◊◊◊◊◊1

Local Properties

M is an \mathcal{A} -module

Lemma 3.29. *Being zero is a local property i.e. the followings are equivalent:*

- (a) $M = 0$
- (b) $M_{\mathfrak{p}} = 0 \forall \mathfrak{p} \text{ primes}$
- (c) $M_{\mathfrak{m}} = 0 \forall \mathfrak{m} \text{ maximal}$

Claim 1

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

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

Calim2:

\mathfrak{m} maximal $x \in M$ Then $x \notin \text{Ker}(M \longrightarrow M_{\mathfrak{m}})$ (absent)

Proof. $x \in \text{Ker}(M \longrightarrow M_{\mathfrak{m}}) \implies \exists s \in \mathcal{A} - \mathfrak{m} : sx = 0$
 $\text{Ann}(x) \not\subseteq \mathfrak{m}$ □

The claim 2 means if $x \notin \text{Ker}(M \longrightarrow M_{\mathfrak{m}}) \implies M_{\mathfrak{m}} \neq 0$

Proof. (of Lemma 3.29). It suffices to prove that (c) \implies (a) Let $0 \neq x \in M \implies \text{Ann}(x) \neq (1) \implies \exists \text{maximal ideal } \mathfrak{m} \supseteq \text{Ann}(x)$ It suffices to show that □

Injectivity/Surjectivity are local M is an \mathcal{A} -module, then the following are equivalent.

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. (a) \iff (b): Suppose $N \hookrightarrow P$, want $N \otimes M \hookrightarrow P \otimes M \iff (N \otimes M)_{\mathfrak{m}} = (N_{\mathfrak{m}} \otimes_{\mathcal{A}_{\mathfrak{m}}} M_{\mathfrak{m}}) \hookrightarrow P_{\mathfrak{m}} \otimes_{\mathcal{A}_{\mathfrak{m}}} M_{\mathfrak{m}} (P \otimes M)_{\mathfrak{m}} \forall \mathfrak{m}$
 $\iff N_{\mathfrak{m}} \hookrightarrow P_{\mathfrak{m}} \forall \mathfrak{m}$
 $\iff N \hookrightarrow P$ as usual. □

Definition 3.30. (Lemma)

- (a) \mathcal{A} satisfies the **ascending chain condition on ideals** (All the sequence $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$ stabilizes $\exists n_0$ s.t. $\mathfrak{a}_n = \mathfrak{a}_{n_0} \forall n \geq 0$)
- (b) Every ideal of \mathcal{A} is finitely generated.
- (c) $\{\text{ideals in } \mathcal{A}\}$ 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. $\forall \mathfrak{b} \in S \implies \mathfrak{b} \not\supset \mathfrak{a}$

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

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

(a) \implies (c)

Let $\emptyset \neq S \subseteq \{\text{ideals in } \mathcal{A}\}$. If S violates the maximal property, then we can find $\mathfrak{a}_1, \mathfrak{a}_2, \dots \in S$ s.t. $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \implies \text{ACC fails.}$

(c) \implies (a), If ACC fails, $\exists \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$ Take $S := \{\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3 \dots\}$. Then S violates Maximal property.

(b) \implies (a), Let $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$ 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 $\dots\dots\dots 3$ □

Definition 3.31. (Lemma)

M is an \mathcal{A} -module. The followings are equivalent:

- (a) M ACC on submodules
- (b) Every submodule of M is finitely generated
- (c) M has the property of Maximal on submodules

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

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

Lemma 3.32. Let $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ be a short exact sequence of \mathcal{A} -modules. Then M is Noetherian \iff both M', M'' Noetherian

Proof. \Leftarrow , Use ACC. Let $N_1 \subseteq N_2 \subseteq \dots$ be submodules of M . Want to show that $\exists n_0 : (n \geq n_0) N_n = N_{n_0}$. Consider $N_j'' := \text{Image of } N_j \text{ in } M''$. $N_1'' \subseteq N_2'' \subseteq \dots$. 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 $N_i = N_j$. \square

Theorem 3.33. (Hilbert basis theorem) \mathcal{A} Noetherian $\implies \mathcal{A}[X]$ is Noetherian.

Corollary 3.34. \mathcal{A} Noetherian $\implies \mathcal{A}[x_1, \dots, x_n]$ Noetherian $\mathcal{A}[x_1, \dots, x_n]/\mathfrak{a}$ Noetherian $\forall \mathfrak{a} \subseteq \mathcal{A}[x_1, \dots, x_n]$

Proof. 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 $\mathfrak{a} : ax^n + \dots \in \mathcal{L}$. Then \mathcal{A} Noetherian $\implies \mathcal{L} = (t_1, \dots, t_r), t_i \in \mathcal{L} \exists f_1, \dots, f_r \in \mathfrak{a} : f_j = t_j x^{n_j} + \dots$
 $N := \max(n_1, \dots, n_r)$ 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. \square

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.

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

Because \mathfrak{a} is Noetherian, \mathfrak{a}' is finitely generated.

Let $f \in \mathfrak{a}$ with $f = ax^n + \dots$, where $n \geq (n_1, \dots, n_r)$.

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

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 $n, n-1, \dots, N$, $\implies \mathfrak{a} \subseteq (f_1, \dots, f_r) + M_N \subseteq \mathfrak{a}$, then the equality holds and \mathfrak{a} is finitely generated. \square

Applications:

- $\mathcal{A}[x_1, \dots, x_r]/\mathfrak{a}$ 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 $S \subseteq \mathbb{C}[x_1, \dots, x_d] =: \mathcal{A}$. $V(S) = \{X \in \mathbb{C}^d : f(X) = 0 \forall f \in S\}$. 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 $S \subseteq \mathbb{C}[x_1, \dots, x_d]$ 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 $\iff \mathfrak{a} = (f_1, \dots, f_r)$ \square

Non-Example:

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

Lemma 4.2. \mathcal{A} Noetherian \implies any homomorphic image of \mathcal{A} is Noetherian:

Proof. The image if of the form \mathcal{A}/\mathfrak{a} for some $\mathfrak{a} \subseteq \mathcal{A}$. $0 \longrightarrow \mathfrak{a} \longrightarrow \mathcal{A} \longrightarrow \mathcal{A}/\mathfrak{a} \longrightarrow 0$. Because there is a one to one inclusion preserving correspondence between the $\{\text{ideals in } \mathcal{A}\}$ and $\{\text{ideals in } \mathcal{A}/\mathfrak{a}\}$. 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 $\{\text{ideals in } \mathcal{A}\}$ and $\{\text{ideals in } S^{-1}\mathcal{A}\}$. 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. $\mathcal{A}[x_1, \dots, x_n]$ is an \mathcal{A} -algebra, with the obvious choice of f .

Example 4.6.

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

$$\begin{aligned}\mathbb{Z} &\longrightarrow \mathcal{B} \\ n &\longmapsto n \cdot 1_{\mathcal{B}}\end{aligned}$$

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 if there exists $x_1, \dots, x_n \in \mathcal{B}$ s.t. \mathcal{B} is generated by $f(\mathcal{A}), x_1, \dots, x_n$. 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

$$\begin{array}{ccc}\mathcal{B} & \longrightarrow & \mathcal{C} \\ \uparrow & \nearrow & \\ \mathcal{A} & & \end{array}$$

Now we come back to the proof of the statement

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

$$\iff \exists n \geq 0 \quad \exists h : \mathcal{A}[x_1, \dots, x_n] \longrightarrow \mathcal{B}, h \text{ surjective}$$

then we have the derivation: \mathcal{A} Noetherian $\implies \mathcal{A}[x_1, \dots, x_n]$ Noetherian, it surjectively maps to \mathcal{B} , \mathcal{B} is a homomorphism image of a Noetherian ring, then we have \mathcal{B} is Noetherian. \square

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.**

| $\mathcal{B}$                        | <i>finite</i> | <i>finitely generated</i> |
|--------------------------------------|---------------|---------------------------|
| $\mathbb{Z}$                         | $T$           | $T$                       |
| $\frac{1}{2}\mathbb{Z}$              | $T$           | $N/A$                     |
| $\mathbb{Z}\left[\frac{1}{2}\right]$ | $F$           | $T$                       |
| $\mathbb{Q}$                         | $F$           | $F$                       |

**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  $\iff \mathbb{L}/\mathbb{K}$  is a finite field extension.

**Corollary 4.13.** The maximal ideal of  $\mathcal{A} = \mathbb{C}[x_1, \dots, x_d]$  are all of the form  $\mathfrak{m}_X = (x_1 - X_1, \dots, x_d - X_d)$  for some  $X \in \mathbb{C}^d$ .

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

$$\begin{array}{c} \mathbb{C} \longrightarrow \mathbb{C}[x_1, \dots, x_d] = \mathcal{A} \xrightarrow{q} \mathbb{L} = \mathcal{A}/\mathfrak{m} \\ \searrow \quad \quad \quad \nearrow j \\ \quad \quad \quad \mathbb{C} \end{array}$$

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

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

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

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

*Proof.*  $\mathbb{K} = \mathbb{C}, \mathbb{L} = \mathbb{C}(x_1, \dots, x_d)$ , then  $\mathbb{L}/\mathbb{K}$  NOT finite (by thm)  $\implies \mathbb{L}$  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  $f_1, \dots, f_n \in \mathbb{K}(x_1, \dots, x_d)$ , each  $f_i = \frac{g_i}{h_i} \in \mathbb{C}[x_1, \dots, x_d]$ . Set  $u := 1 + x_1 h_1 \cdot \dots \cdot h_n \implies 1/u \notin \mathbb{K}[f_1, \dots, f_n]$  because denominator is coprime to the denominators of the  $f_j$ .  $\square$

Then we come back to the proof of the theorem (about field extensions)





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

*Proof.* (a) “ $\implies$ ” Assume  $S$  maximal algebraic independent. 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  $s_1, \dots, s_n \in S$  and a nontrivial polynomial relation between  $s_1, \dots, s_n$ . This relation must involve  $\alpha$ . Then  $\exists m \geq 1, p_0, \dots, p_m \in F[X_1, \dots, X_n]$  s.t.  $\alpha^m p_m(s_1, \dots, s_n) + \dots + \alpha p_1(s_1, \dots, s_n) + p_0(s_1, \dots, s_n) = 0$  with  $p_m \neq 0 \implies [F(\alpha, s_1, \dots, s_n) : F(s_1, \dots, s_n)] \leq m \implies \alpha$  is algebraic over  $F(S)$ . “ $\impliedby$ ”, 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  $\alpha$  is algebraic over  $F(S)$ , by assumption.  $\exists m \geq 1$

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

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

□

**Example 4.17.**

$$\text{tr.deg}(\overline{\mathbb{Q}}/\mathbb{Q}) = 0$$

$$\text{tr.deg}(\mathbb{C}/\mathbb{Q}) = \infty$$

$$\text{tr.deg}(F(t_1, \dots, t_n)/F) = n$$

If  $E/F(t_1, \dots, t_n)$  is algebraic, then  $\text{tr.deg}(E/F)$  is  $n$

$$\text{tr.deg}(F/F) = 0 \iff (E/F) \text{ is algebraic.}$$

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,  $L = \langle x_1, \dots, x_n \rangle_{K\text{-alg}}$ .  $r := \text{tr.deg}(L/K)$ . Conclusion  $\iff r = 0$ . Suppose not. Then  $r \geq 1$ . By part (f) of the Theorem 4.16 that after relabeling,  $\{x_1, \dots, x_r\}$  is a transcendence basis of  $L/K$ . Each  $x_{r+1}, \dots, x_n$  is algebraic over  $K(x_1, \dots, x_r) =: M \implies L/M$  is finite.  $\underbrace{\phantom{L/M \text{ is finite}}}_{\text{by (f) of Thm 4.16}}$

**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)  $C = \langle y_1, \dots, y_m \rangle_{\mathcal{B}\text{-mod}}$  and  $C = \langle x_1, \dots, x_n \rangle_{\mathcal{A}\text{-alg}}$  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  $\implies$  (Hilbert basis theorem)  $\mathcal{B}_0$  : Noetherian,  $\mathcal{C} = \{\text{polynomials in } \{x_j\} \text{ with coefficients in } \mathcal{A}\}$  and by substitution if equals  $\{\text{linear combinations of } y_i \text{ with coefficients in } \mathcal{B}_0\} \implies \mathcal{C}$  is a finite  $\mathcal{B}_0$ -module.  $\implies \mathcal{C}$  is a Noetherian,  $\mathcal{B}_0$ -module.  $\implies$  the  $\mathcal{B}_0$ -submodule  $\mathcal{B} \subseteq \mathcal{C}$  is finitely generated.  $\implies \mathcal{B}$  is finitely generated  $\mathcal{A}$ -algebra  $\square$

$\square$

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

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

For the converse inclusion recall that  $r(\mathfrak{a}) = \cap_{\mathfrak{p} \ni \mathfrak{a}, \text{prime}} \mathfrak{p}$ . 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  $0 \neq \bar{f} \in \mathcal{A}/\mathfrak{p}$ .  $\implies (\mathcal{A}/\mathfrak{p})_{\bar{f}} = (\mathcal{A}/\mathfrak{p})_{[\frac{1}{\bar{f}}]} \neq 0$ . Choose a maximal ideal  $\mathfrak{m} \subseteq (\mathcal{A}/\mathfrak{p})_{\bar{f}} =: \mathcal{B}$ . Set  $L := \mathcal{B}/\mathfrak{m}$  a field,  $L$  is finitely generated  $K$ -algebra.  $\implies L/K$  is finite  $\implies L = K$  because  $\overline{K} = K$ . Set  $X = (X_1, \dots, X_d)$ ,  $X_j = \text{image of } t_j \text{ in } L$ . Check that  $f(X) \neq 0, X \in V(\mathfrak{a}) \implies f \notin I(V(\mathfrak{a}))$ .  $\square$

## Primary Decomposition

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

$\mathcal{A}$  any ring.

**Definition 4.19.** ?????????????

llllllllllll2

**Definition 4.20.** An ideal  $\mathfrak{a} \subseteq \mathcal{A}$  is **decomposable** if we may write  $\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$ , We call this a **primary decomposition**.

**Proposition 4.21.**  $\mathcal{A}$  is Noetherian,  $\implies$  every  $\mathfrak{a} \subseteq \mathcal{A}$  is decomposable.

recall the ideal of induction in general. **Induction:**  $S \subseteq \mathbb{N}$

(I)  $S$  has a minimal element.

and **Noetherian Induction**  $\mathcal{A}$  a Noetherian ring

$$(II) \quad iiii3$$

**Lemma 4.22.**  *$\mathcal{A}$  is Noetherian,  $\mathfrak{a} \subseteq \mathcal{A}$  is an ideal.  $\implies \mathfrak{a}$  decomposable:*

$$\iff xy \in \mathfrak{q} \implies x \in \mathfrak{q} \text{ or } y^n \in \mathfrak{q} \text{ for some } n$$

**Claim1:**  $\mathcal{A}$  Noetherian. Then irresucible  $\implies$  primary.

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  $Ann(y^n)$ . These ideals goes up as  $n$  increases  $\implies, Ann(y^n) = Ann(y^{n+1})$  for some  $n$  because  $\mathcal{A}$  is Noetherian. Then we know,  $xy = 0, x \in Ann(y), (x) \subseteq Ann(y)$ .

Assuming the subclaim, (since  $(0)$  is irreducible) deduce that either  $Ann(y) = (0) \implies x \in (0)$  or  $(y^n) = (0) \implies y^n = 0$ . Now we turn to prove the subclaim: Let  $z \in Ann(y) \cap (y^n)$ . Then  $z = y^nt, t \in \mathcal{A}$  and  $zy = 0 \implies ty^{n+1} = 0 \implies t \in Ann(y^{n+1}) = Ann(y^n) \implies z = ty^n = 0$ . This finishes the proof of subclaim thus also the proof of Claim1.

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

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

show if  $\mathfrak{a}$  has the property that **all strictly larger ideals  $\mathfrak{b} \supsetneq \mathfrak{a}$  belongs to  $S$**  Then  $\mathfrak{a} \in S$ . If not, then  $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}, \mathfrak{b} \supsetneq \mathfrak{a} \implies \mathfrak{b}, \mathfrak{c} \in S$ . conclude as before.  $\square$

Basics on primary ideals:

**Lemma 4.23.** *Let  $\mathfrak{q}$  primary. Then  $\mathfrak{p} := \text{rad}(\mathfrak{q})$  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  $n$ .  $x^n \notin \mathfrak{q} \implies (y^n)^m \in \mathfrak{q}$  for some  $m \implies y \in \mathfrak{p}$ .  $\square$

**Definition 4.24.** *If  $\mathfrak{q}$  is primary with radical  $\mathfrak{p}$ , we call  $\mathfrak{q}$   **$\mathfrak{p}$ -primary**.*

**Lemma 4.25.** *If  $\mathfrak{q}_1, \dots, \mathfrak{q}_n$ ,  $\mathfrak{p}$ -primary, then  $\mathfrak{q} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$  is  $\mathfrak{p}$ -primary.*

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

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

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  $\mathfrak{m} = \text{rad}(\mathfrak{q})$ , then  $\mathfrak{q}$  is primary.

*Proof.* Then  $\mathfrak{m}/\mathfrak{q} = \text{Nil}(\mathcal{A}/\mathfrak{q})$  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 (belong to  $\text{Nil}(\mathcal{A}/\mathfrak{q}) = \mathfrak{m}/\mathfrak{q}$ ) In other words, want if  $x \in \mathcal{A}/\mathfrak{q}, x \notin \mathfrak{m}/\mathfrak{q}$ , then  $x$  not a zero divisor. Because  $x \in \mathcal{A}/\mathfrak{q} \implies \exists n, x^n \notin \mathfrak{m}/\mathfrak{q} \implies \mathcal{A}/\mathfrak{q}$  is local ring with unique prime  $\mathfrak{m}/\mathfrak{q} \implies x$  is a unit.  $\square$

**Lemma 4.26.**  $\mathfrak{m}$  maximal,  $\implies \mathfrak{m}^n$  is  $\mathfrak{m}$ -primary  $\forall n$

**Example 4.27.**  $\mathfrak{m} = (X, Y) \subseteq K[X, Y] \implies \mathfrak{m}^n$  is primary.

**Example 4.28.**  $\mathfrak{q} = (X^2, Y) \subseteq K[X, Y]$  is  $\mathfrak{m}$ -primary.

**Example 4.29.**  $\mathfrak{a} = \prod_{j=1}^J (X - z_j)^{n_j} \subseteq \mathbb{C}[X]$  for some distinct  $z_1, \dots, z_J \in \mathbb{C}$ .  
Then  $\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_J, \mathfrak{q}_j = ((X - z_j)^{n_j}) \mathfrak{p}_j = \text{rad}(\mathfrak{q}_j) = (X - z_j)$

**Example 4.30.**  $\mathfrak{q}_1 = (X, Y)^2 = (X^2, XY, Y^2) \subseteq K[X, Y], \mathfrak{p} = (X, Y).$   
 $\mathfrak{q}_2 = (Y) \implies \mathfrak{p}_2 = (Y)$   
 $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 = (XY, Y^2)$

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

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

**Definition 4.31.** If we can't do (a) or (b), we call the resulting decomposition **minimal**. Let  $\mathfrak{a}$  ideal, we define  $\text{Ass}(\mathfrak{a}) := \{\text{prime ideals of the form } \text{rad}(\mathfrak{a} : x) \text{ for some } x \in \mathcal{A}\}$  to be **the set of associated ideals of  $\mathfrak{a}$** . (recall  $y \in (\mathfrak{a} : x) \iff y \text{ maps } x \text{ into } \mathfrak{a} \iff yx \in \mathfrak{a}$ )

**Theorem 4.32.** Let  $\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$  be a minimal primary decomposition. Then  $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\} = \text{Ass}(\mathfrak{a})$ . In particular, the set  $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$  is independent of the choice of minimal primary decomposition.

**Lemma 4.33.** Let  $\mathfrak{q}$   $\mathfrak{p}$ -primary,  $x \in \mathcal{A}$ .

$$\begin{aligned} x \in \mathfrak{q} &\implies (\mathfrak{q} : x) = (1) \\ x \notin \mathfrak{q} &\implies (\mathfrak{q} : x) \text{ is } \mathfrak{p}\text{-primary.} \\ x \notin \mathfrak{p} &\implies (\mathfrak{q} : x) = \mathfrak{q} \end{aligned}$$

We first show that the lemma leads to the theorem.

*Proof.*  $\{\mathfrak{p}_j\} \supseteq \text{Ass}(\mathfrak{a})$ . Let  $x \in \mathcal{A}$  s.t.  $\text{rad}(\mathfrak{a} : x) = \mathfrak{p}$  is prime. want  $\mathfrak{p} = \text{some } \mathfrak{p} + j$ .  $\text{rad}(\mathfrak{a} : x) = \cap \text{rad}(\mathfrak{q}_j : x) = \cap_{x \notin \mathfrak{q}_j} \mathfrak{p}_j \implies \mathfrak{p} = \text{some } \mathfrak{q}_j$   $\lll\lll\lll\lll\lll\lll 1$   $\square$