

# Commutative Algebra notes

arnaucube

2026

## Abstract

Notes taken while studying Commutative Algebra, mostly from Atiyah & MacDonald book [1] and Reid's book [2]. For the exercises, I follow the assignments listed at [3].

Usually while reading books and papers I take handwritten notes in a notebook, this document contains some of them re-written to *LaTeX*.

The proofs may slightly differ from the ones from the books, since I try to extend them for a deeper understanding.

## Contents

<b>1</b>	<b>Ideals</b>	<b>2</b>
1.1	Definitions . . . . .	2
1.2	$\mathbb{Z}$ and $K[X]$ , two Principal Ideal Domains . . . . .	3
1.3	Zorn's lemma and Jacobson radicals . . . . .	4
<b>2</b>	<b>Modules</b>	<b>5</b>
2.1	Modules concepts . . . . .	5
2.2	Cayley-Hamilton theorem, Nakayama lemma, and corollaries . . . . .	5
2.3	Sequences . . . . .	10
<b>3</b>	<b>Noetherian rings (and modules)</b>	<b>12</b>
3.1	Noetherian rings and modules . . . . .	13
3.2	Hilbert basis . . . . .	15
<b>4</b>	<b>Finite ring extensions and Noether normalization</b>	<b>16</b>
4.1	A-algebras and integral domains . . . . .	16
4.2	Noether normalization . . . . .	20
4.3	Weak Nullstellensatz . . . . .	22
<b>5</b>	<b>Nullstellensatz</b>	<b>23</b>

<b>6 Exercises</b>	<b>25</b>
6.1 Exercises Chapter 1 . . . . .	25
6.2 Exercises Chapter 2 . . . . .	29
6.3 Exercises Chapter 3 . . . . .	30
6.4 Exercises Chapter 4 . . . . .	32

# 1 Ideals

## 1.1 Definitions

**Definition** (ideal).  $I \subset R$  ( $R$  ring) such that  $0 \in I$  and  $\forall x \in I, r \in R, xr, rx \in I$ .

ie.  $I$  absorbs products in  $R$ .

**Definition** (prime ideal). if  $a, b \in R$  with  $ab \in P$  and  $P \neq R$  ( $P$  a prime ideal), implies  $a \in P$  or  $b \in P$ .

**Definition** (principal ideal). generated by a single element,  $(a)$ .

$(a)$ : principal ideal, the set of all multiples  $xa$  with  $x \in R$ .

**Definition** (maximal ideal).  $\mathfrak{m} \subset A$  ( $A$  ring) with  $\mathfrak{m} \neq A$  and there is no ideal  $I$  strictly between  $\mathfrak{m}$  and  $A$ . ie. if  $\mathfrak{m}$  maximal and  $\mathfrak{m} \subseteq I \subseteq A$ , either  $\mathfrak{m} = I$  or  $I = A$ .

**Definition** (unit).  $x \in A$  such that  $xy = 1$  for some  $y \in A$ . ie. element *which divides 1*.

**Definition** (zerodivisor).  $x \in A$  such that  $\exists 0 \neq y \in A$  such that  $xy = 0 \in A$ . ie.  $x$  *divides 0*.

If a ring does not have zerodivisors is an integral domain.

**Definition** (prime spectrum -  $\text{Spec}(A)$ ). set of prime ideals of  $A$ . ie.

$$\text{Spec}(A) = \{P \mid P \subset A \text{ is a prime ideal}\}$$

**Definition** (integral domain). Ring in which the product of any two nonzero elements is nonzero.

ie. no zerodivisors.

ie.  $\forall 0 \neq a, 0 \neq b \in A, ab \neq 0 \in A$ .

Every field is an integral domain, not the converse.

**Definition** (principal ideal domain - PID). integral domain in which every ideal is principal. ie.  $\forall I \subset R, \exists a \in I$  such that  $I = (a) = \{ra \mid r \in R\}$ .

**Definition** (nilpotent).  $a \in A$  such that  $a^n = 0$  for some  $n > 0$ .

**Definition** (nilrad  $A$ ). set of all nilpotent elements of  $A$ ; is an ideal of  $A$ .  
if  $\text{nilrad} A = 0 \implies A$  has no nonzero nilpotents.

$$\text{nilrad} A = \bigcap_{P \in \text{Spec}(A)} P$$

**Definition** (idempotent).  $e \in A$  such that  $e^2 = e$ .

**Definition** (radical of an ideal).

$$\text{rad}I = \{f \in A \mid f^n \in I \text{ for some } n\}$$

$\text{rad}I$  is an ideal.

$$\text{nilrad}A = \text{rad}0$$

$$\text{rad}I = \bigcap_{\substack{P \in \text{Spec}(A) \\ P \supset I}} P$$

**Definition** (local ring). A *local ring* has a unique maximal ideal.

Notation: local ring  $A$ , its maximal ideal  $\mathfrak{m}$ , residue field  $K = A/\mathfrak{m}$ :

$$A \supset \mathfrak{m} \text{ or } (A, \mathfrak{m}) \text{ or } (A, \mathfrak{m}, K)$$

## 1.2 $\mathbb{Z}$ and $K[X]$ , two Principal Ideal Domains

**Lemma** .  $\mathbb{Z}$  is a PID.

*Proof.* Let  $I$  a nonzero ideal of  $\mathbb{Z}$ .

Since  $I \neq \{0\}$ , there is at least one nonzero integer in  $I$ . Choose the smallest element of  $I$ , namely  $d$ .

Observe that  $(d) \subseteq I$ , since  $d \in I$ . Then, every multiple  $nd \in I$ , since  $I$  is an ideal.

Take  $a \in I$ . By the Euclidean division algorithm in  $\mathbb{Z}$ ,  $a = qd + r$ , with  $q, r \in \mathbb{Z}$  and  $0 \leq r < d$ .

Then  $r = a - qd \in I$ , but  $d$  was chosen to be the smallest positive element of  $I$ , so the only possibility is  $r = 0$ .

Hence,  $a = qd$ , so  $a \in (d)$ , giving  $I \subseteq (d)$ .

Since we had  $(d) \subseteq I$  and now we got  $I \subseteq (d)$ , we have  $I = (d)$ , so every ideal of  $\mathbb{Z}$  is principal. Thus  $\mathbb{Z}$  is a Principal Ideal Domain(PID).  $\square$

**Lemma** .  $K[X]$  is a PID.

*Proof.* This proof follows very similarly to the previous proof.

Let  $K$  be a field,  $K[X]$  a polynomial ring.

Take  $\{0\} \neq I \subseteq K[X]$ .

Since  $I \neq \{0\}$ , there is at least one non-zero polynomial in  $I$ .

Let  $p(X) \in I$  be of minimal degree among nonzero elements of  $I$ .

Observe that  $(p(X)) \subseteq I$ , because  $p(X) \in I$  and  $I$  is an ideal.

Let  $f(X) \in I$ . By Euclidean division algorithm in  $K[X]$ ,  $\exists q, r \in K[X]$  such that  $f(X) = q(X) \cdot p(X) + r(X)$  with either  $r(X) = 0$  or  $\deg(r) < \deg(p)$ .

Since  $f, p \in I$ , then  $r(X) = f(X) - q(X) \cdot p(X) \in I$

If  $r(X) \neq 0$ , then  $\deg(r) < \deg(p)$ , which contradicts the minimality of  $\deg(p)$  in  $I$ .

Therefore,  $r(X) = 0$ , thus  $f(X) = q(X) \cdot p(X)$ , hence  $f(X) \in (p(X))$ . Henceforth,  $I \subseteq (p(X))$ .

Then, since  $(p(X)) \subseteq I$  and  $I \subseteq (p(X))$ , we have that  $I = (p(X))$ .  
So every ideal of  $K[X]$  is principal; thus  $K[X]$  is a PID. □

### 1.3 Zorn's lemma and Jacobson radicals

Let  $\Sigma$  be a partially ordered set. Given subset  $S \subset \Sigma$ , an *upper bound* of  $S$  is an element  $u \in \Sigma$  such that  $s < u \forall s \in S$ .

A *maximal element* of  $\Sigma$ , is  $m \in \Sigma$  such that  $m < s$  does not hold for any  $s \in \Sigma$ .

A subset  $S \subset \Sigma$  is *totally ordered* if for every pair  $s_1, s_2 \in S$ , either  $s_1 \leq s_2$  or  $s_2 \leq s_1$ .

**Lemma R.1.7** (Zorn's lemma). Suppose  $\Sigma$  a nonempty partially ordered set (ie. we are given a relation  $x \leq y$  on  $\Sigma$ ), and that any totally ordered subset  $S \subset \Sigma$  has an upper bound in  $\Sigma$ .

Then  $\Sigma$  has a maximal element.

**Theorem AM.1.3.** Every ring  $A \neq 0$  has at least one maximal ideal.

*Proof.* By Zorn's lemma R.1.7. □

**Corollary AM.1.4.** if  $I \neq (1)$  an ideal of  $A$ ,  $\exists$  a maximal ideal of  $A$  containing  $I$ .

**Corollary AM.1.5.** Every non-unit of  $A$  is contained in a maximal ideal.

**Definition** (Jacobson radical). The *Jacobson radical* of a ring  $A$  is the intersection of all the maximal ideals of  $A$ .

Denoted  $Jac(A)$ .

$Jac(A)$  is an ideal of  $A$ .

**Proposition AM.1.9.**  $x \in Jac(A)$  iff  $(1 - xy)$  is a unit in  $A$ ,  $\forall y \in A$ .

*Proof.* Suppose  $1 - xy$  not a unit.

By AM.1.5,  $1 - xy \in \mathfrak{m}$  for  $\mathfrak{m}$  some maximal ideal.

But  $x \in Jac(A) \subseteq \mathfrak{m}$ , since  $Jac(A)$  is the intersection of all maximal ideals of  $A$ .

Hence  $xy \in \mathfrak{m}$ , and therefore  $1 \in \mathfrak{m}$ , which is absurd, thus  $1 - xy$  is a unit.

Conversely:

Suppose  $x \notin \mathfrak{m}$  for some maximal ideal  $\mathfrak{m}$ .

Then  $\mathfrak{m}$  and  $x$  generate the unit ideal  $(1)$ , so that we have  $u + xy = 1$  for some  $u \in \mathfrak{m}$  and some  $y \in A$ .

Hence  $1 - xy \in \mathfrak{m}$ , and is therefore not a unit. □

## 2 Modules

### 2.1 Modules concepts

Let  $A$  be a ring. An  $A$ -module is an Abelian group  $M$  with a multiplication map

$$\begin{aligned} A \times M &\longrightarrow M \\ (f, m) &\longmapsto fm \end{aligned}$$

satisfying  $\forall f, g \in A, m, n \in M$ .

- i.  $f(m \pm n) = fm \pm fn$
- ii.  $(f \pm g)m = fm \pm gm$
- iii.  $(fg)m = f(gm)$
- iv.  $1_A m = m$

Let  $\psi : M \longrightarrow M$  an  $A$ -linear endomorphism of  $M$ .  
 $A[\psi] \subset \text{End}M$  is the subring generated by  $A$  and the action of  $\psi$ .

- since  $\psi$  is  $A$ -linear,  $A[\psi]$  is a commutative ring.
- $M$  is a module over  $A[\psi]$ , so  $\psi$  becomes multiplication by a ring element.

### 2.2 Cayley-Hamilton theorem, Nakayama lemma, and corollaries

**Proposition AM.2.4.** (Cayley-Hamilton Theorem) Let  $M$  a finitely generated  $A$ -module. Let  $\mathfrak{a}$  an ideal of  $A$ , let  $\psi$  an  $A$ -module endomorphism of  $M$  such that  $\psi(M) \subseteq \mathfrak{a}M$ .

Then  $\psi$  satisfies

$$\psi^n + a_1\psi^{n-1} + \dots + a_{n-1}\psi + a_n = 0$$

with  $a_i \in \mathfrak{a}$ .

*Proof.* Since  $M$  finitely generated, let  $\{x_1, \dots, x_n\}$  be generators of  $M$ .

By hypothesis,  $\psi(M) \subseteq \mathfrak{a}M$ ; so for any generator  $x_i$ , its image  $\psi(x_i) \in \mathfrak{a}M$ .

Any element in  $\mathfrak{a}M$  is a linear combination of the generators with coefficients in the ideal  $\mathfrak{a}$ , thus

$$\psi(x_i) = \sum_{j=1}^n a_{ij}x_j$$

with  $a_{ij} \in \mathfrak{a}$ .

Thus, for a module with  $n$  generators, we have  $n$  different  $\psi(x_i)$  equations:

$$\left. \begin{array}{l} \psi(x_1) = a_{1,1}x_1 + a_{1,2}x_2 + \dots + a_{1,n}x_n \\ \psi(x_2) = a_{2,1}x_1 + a_{2,2}x_2 + \dots + a_{2,n}x_n \\ \dots \\ \psi(x_n) = a_{n,1}x_1 + a_{n,2}x_2 + \dots + a_{n,n}x_n \end{array} \right\} \begin{array}{l} n \text{ elements } \psi(x_i) \in \mathfrak{a}M \text{ which} \\ \text{are linear combinations of the} \\ n \text{ generators of } M \end{array}$$

Next step: rearrange in order to use matrix algebra.

Observe that each row equals 0, and rearranging the elements at each row we get

$$\left. \begin{array}{l} \psi(x_1) - (a_{1,1}x_1 + a_{1,2}x_2 + \dots + a_{1,n}x_n) = 0 \\ \psi(x_2) - (a_{2,1}x_1 + a_{2,2}x_2 + \dots + a_{2,n}x_n) = 0 \\ \dots \\ \psi(x_n) - (a_{n,1}x_1 + a_{n,2}x_2 + \dots + a_{n,n}x_n) = 0 \end{array} \right\}$$

Then, group the  $x_i$  terms together; as example, take the row  $i = 1$ :

$$(\psi - a_{1,1})x_1 - a_{1,2}x_2 - \dots - a_{1,n}x_n = 0$$

$$\left. \begin{array}{l} (\psi - a_{1,1})x_1 - a_{1,2}x_2 - \dots - a_{1,n}x_n = 0 \\ -a_{2,1}x_1 + (\psi - a_{2,2})x_2 - \dots - a_{2,n}x_n = 0 \\ \dots \\ -a_{n,1}x_1 - a_{n,2}x_2 - \dots + (\psi - a_{n,n})x_n = 0 \end{array} \right\}$$

So,  $\forall i \in [n]$ , as a matrix:

$$\begin{pmatrix} \psi - a_{1,1} & -a_{1,2} & \dots & -a_{1,n} \\ -a_{2,1} & \psi - a_{2,2} & \dots & -a_{2,n} \\ \vdots & & & \\ -a_{n,1} & -a_{n,2} & \dots & \psi - a_{n,n} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Denote the previous matrix by  $\Phi$ . Let  $m$  denote the vector  $(x_1, x_2, \dots, x_n)^T$  (ie. the vector of generators of the  $A$ -module  $M$ ).

Then we can write the previous equality as

$$\Phi \cdot m = 0 \tag{1}$$

We know that

$$\text{adj}(\Phi)\Phi = \det(\Phi)I \tag{2}$$

(aka. *fundamental identity for the adjugate matrix*).

So if at (1) we multiply both sides by  $\text{adj}(\Phi)$ ,

$$\begin{aligned} \text{adj}(\Phi) \cdot \Phi \cdot m &= 0 \\ (\text{recall from (2): } \text{adj}(\Phi)\Phi &= \det(\Phi) \cdot I) \\ &= \det(\Phi) \cdot I \cdot m = 0 \end{aligned}$$

Thus,

$$\begin{aligned}
& \det(\Phi) \cdot I \cdot m = 0 : \\
& \begin{pmatrix} \det(\Phi) & 0 & \dots & 0 \\ 0 & \det(\Phi) & \dots & 0 \\ \vdots & & & \\ 0 & 0 & \dots & \det(\Phi) \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \\
\Rightarrow & \det(\Phi) \cdot x_i = 0 \quad \forall i \in [n] \tag{3}
\end{aligned}$$

ie.  $\det(\Phi)$  is an *annihilator* of the generators  $x_i$  of  $M$ , thus is an annihilator of the entire module  $M$ .

So, we're interested into calculating the  $\det(\Phi)$ .

By the Leibniz formula,

$$\det(A) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^n a_{i, \sigma(i)}$$

thus,

$$\det(\Phi) = \underbrace{(\psi - a_{11})(\psi - a_{22}) \dots (\psi - a_{nn})}_{\text{diagonal of } \Phi, \text{ leading term of the determinant}} - \dots$$

The *determinant trick* is that the terms that go after the "leading term of the determinant", will belong to  $\mathfrak{a}$  and their combinations with  $\psi$  will not be bigger than  $\psi^n$ . Furthermore, when expanding it

- highest power is  $1 \cdot \psi^n$
- coefficient of  $\psi^{n-1}$  is  $-(\underbrace{a_{11} + a_{22} + \dots + a_{nn}}_{a_1})$ ,  
where, since each  $a_{ii} \in \mathfrak{a}$ ,  $a_1 \in \mathfrak{a}$
- the rest of coefficients of  $\psi^k$  are also elements in  $\mathfrak{a}$

Therefore we have

$$\det(\Phi) = \psi^n + a_1 \psi^{n-1} + a_2 \psi^{n-2} + \dots + a_{n-1} \psi + a_n$$

with  $a_i \in \mathfrak{a}$ .

Now, notice that we had  $\det(\Phi) \cdot x_i = 0 \quad \forall i \in [n]$ .

The matrix  $\Phi$  is the *characteristic matrix*,  $xI - A$ , viewed as an operator. Then,

$$\det(\Phi) = \det(xI - A) = p(x)$$

where  $p(x)$  is the *characteristic polynomial*.

If a linear transformation turns every basis vector  $(x_i)$  into zero, then that transformation is the zero transformation. So in our case,  $\det(\Phi)$  is the zero transformation, thus  $\det(\Phi) = 0$ . Therefore,

$$\psi^n + a_1\psi^{n-1} + a_2\psi^{n-2} + \dots + a_{n-1}\psi + a_n = 0$$

□

**Corollary AM.2.5.** Let  $M$  a fingen  $A$ -module, let  $\mathfrak{a}$  an ideal of  $A$  such that  $\mathfrak{a}M = M$ .

Then,  $\exists x \equiv 1 \pmod{\mathfrak{a}}$  such that  $xM = 0$ .

*Proof.* take  $\psi = \text{identity}$ . Then in Cayley-Hamilton (AM.2.4):

$$\begin{aligned} \psi^n + a_1\psi^{n-1} + a_2\psi^{n-2} + \dots + a_{n-1}\psi + a_n &= 0 \\ \implies id_M + a_1id_M + a_2id_M + \dots + a_{n-1}id_M + a_n &= 0 \\ \implies (1 + a_1 + \dots + a_n)id_M &= 0 \end{aligned}$$

apply it to  $m \in M$ , where since  $id_M(m) = m$  (by definition of the identity), we then have

$$(1 + a_1 + \dots + a_n) \cdot m = 0$$

with  $a_i \in \mathfrak{a}$ .

part i.  $xM = 0$ :

Thus the scalar  $x = (1 + a_1 + \dots + a_n)$  annihilates every  $m \in M$ , ie. the entire module  $M$ .

part ii.  $x \equiv 1 \pmod{\mathfrak{a}}$ :

$x \equiv 1 \pmod{\mathfrak{a}} \iff (x - 1) \in \mathfrak{a}$   
then from  $x = (1 + \underbrace{a_1 + \dots + a_n}_b) \in \mathfrak{a}$ , set  $b = a_1 + \dots + a_n$ ,

so that  $x = (1 + b) \in \mathfrak{a}$ .

Then  $x - 1 = (1 + b) - 1 = b \in \mathfrak{a}$   
so  $x - 1 \in \mathfrak{a}$ , thus  $x \equiv 1 \pmod{\mathfrak{a}}$  as stated.

□

**Proposition AM.2.6** (Nakayama's lemma). Let  $M$  a fingen  $A$ -module, let  $\mathfrak{a}$  an ideal of  $A$  such that  $\mathfrak{a} \subseteq \text{Jac}(A)$ .

Then  $\mathfrak{a}M = M$  implies  $M = 0$ .

*Proof.* By AM.2.5: since  $\mathfrak{a}M = M$ , we have  $xM = 0$  for some  $x \equiv 1 \pmod{\text{Jac}(A)}$ . (notice that at AM.2.5 is  $\pmod{\mathfrak{a}}$  but here we use  $\pmod{\text{Jac}(A)}$ ), since we have  $\mathfrak{a} \subseteq \text{Jac}(A)$ .



(recall AM.1.9:  $x \in \text{Jac}(A)$  iff  $(1 - xy)$  is a unit in  $A$ ,  $\forall y \in A$ ).  
 By AM.1.9,  $x$  is a unit in  $A$  (thus  $x^{-1} \cdot x = 1$ ).

$$\text{Hence } M = x^{-1} \cdot \underbrace{x \cdot M}_{=0 \text{ (by AM.2.5)}} = 0.$$

Thus, if  $\mathfrak{a}M = M$  then  $M = 0$ . □

**Corollary AM.2.7.** Let  $M$  a fingen  $A$ -module, let  $N \subseteq M$  a submodule of  $M$ , let  $\mathfrak{a} \subseteq \text{Jac}(A)$  an ideal.

Then  $M = \mathfrak{a}M + N \xRightarrow{\text{implies}} M = N$ .

*Proof.* The idea is to apply Nakayama (AM.2.6) to  $M/N$ .

Since  $M$  fingen  $\implies M/N$  is fingen and an  $A$ -module.

Since  $\mathfrak{a} \subseteq \text{Jac}(A) \implies$  Nakayama applies to  $M/N$  too.

By definition,

$$\mathfrak{a}M = \left\{ \sum a_i \cdot m_i \mid a_i \in \mathfrak{a}, m_i \in M \right\}$$

where  $m_i$  are the generators of  $M$ .

Then, for  $M/N$ ,

$$\mathfrak{a}\left(\frac{M}{N}\right) = \left\{ \sum a_i \cdot (m_i + N) \mid a_i \in \mathfrak{a}, m_i \in M \right\}$$

observe that  $a_i(m_i + N) = a_i m_i + N$ , thus

$$\sum_i a_i \cdot (m_i + N) = \underbrace{\left( \sum_i a_i \cdot m_i \right)}_{\in \mathfrak{a}M} + N \in \mathfrak{a}M + N$$

Hence,

$$\mathfrak{a}\left(\frac{M}{N}\right) = \{x + N \mid x \in \mathfrak{a}M\} = \mathfrak{a}M + N \tag{4}$$

By definition, if we take  $\frac{\mathfrak{a}M + N}{N}$ , then

$$\frac{\mathfrak{a}M + N}{N} = \{y + N \mid y \in \mathfrak{a}M + N\} = \mathfrak{a}M + N$$

thus every  $y \in \mathfrak{a}M + N$  can be written as

$$y = x + n, \text{ with } x \in \mathfrak{a}M, n \in N$$

which comes from (4).

Thus,  $y + N = (x + n) + N = x + N$ , since  $n \in N$  is zero in the quotient.

Hence, every element of  $\frac{\mathfrak{a}M + N}{N}$  has the form

$$\frac{\mathfrak{a}M + N}{N} = \{x + N \mid x \in \mathfrak{a}M\}$$

as in (4).

Thus

$$\mathfrak{a}\left(\frac{M}{N}\right) = \mathfrak{a}M + N = \frac{\mathfrak{a}M + N}{N} \quad (5)$$

By the Collorary assumption,  $M = \mathfrak{a}M + N$ ; quotient it by  $N$ :

$$\frac{M}{N} = \frac{\mathfrak{a}M + N}{N} \quad (6)$$

So, from (5) and (6):

$$\mathfrak{a}\left(\frac{M}{N}\right) = \mathfrak{a}M + N = \frac{\mathfrak{a}M + N}{N} = \frac{M}{N}$$

thus,  $\mathfrak{a}\left(\frac{M}{N}\right) = \frac{M}{N}$ .

By Nakayama's lemma AM.2.6, if  $\mathfrak{a}\left(\frac{M}{N}\right) = \frac{M}{N} \implies \frac{M}{N} = 0$

Note that

$$\frac{M}{N} = \{m + N \mid m \in M\}$$

(the zero element in  $\frac{M}{N}$  is the coset  $N = 0 + N$ )

Then,  $\frac{M}{N} = 0$  means that the quotient has exactly one element, the zero coset  $N$ .

Thus, every coset  $m + N$  equals the zero coset  $N$ , so  $m - 0 \in N \implies m \in N$ .

Hence every  $m \in M$  lies in  $N$ , ie.  $\forall m \in M, m \in N$ .

So  $M \subseteq N$ . But notice that by the Corollary, we had  $N \subseteq M$ , therefore  $M = N$ .

Thus, if  $M = \mathfrak{a}M + N \implies M = N$ .  $\square$

**Proposition AM.2.8.** Let  $x_i \forall i \in [n]$  be elements of  $M$  whose images  $\frac{M}{mM}$  from a basis of this vector space. Then the  $x_i$  generate  $M$ .

*Proof.* Let  $N$  submodule  $M$ , generated by the  $x_i$ .

Then the composite map  $N \longrightarrow M \longrightarrow \frac{M}{mM}$  maps  $N$  onto  $\frac{M}{mM}$ , hence  $N + \mathfrak{a}M = M$ , which by AM.2.7 implies  $N = M$ .  $\square$

## 2.3 Sequences

**Definition R.2.9.a** (Exact Sequence). Let a sequence of homomorphisms

$$L \xrightarrow{\alpha} M \xrightarrow{\beta} N$$

It is *exact* at  $M$  if  $im(\alpha) = ker(\beta)$ .

ie.  $\beta \circ \alpha = 0$  and  $\alpha$  maps surjectively to  $ker(\beta)$ .

**Definition R.2.9.b** (Short Exact Sequence (s.e.s.)).

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$$

is exact  $\iff L \subset M$  and  $N = M/L$ .

Properties:

- $\alpha$  injective
- $\beta$  surjective
- $\alpha : L \implies \ker \beta$
- $\beta$  induces  $M/\alpha(L) \longrightarrow N$

**Proposition R.2.10** (Split exact sequence). For the previous s.e.s., 3 equivalent conditions:

- i.  $\exists$  isomorphism  $M \cong L \oplus N$ , with

$$\begin{aligned}\alpha : m &\longmapsto (m, 0) \\ \beta : (m, n) &\longmapsto n\end{aligned}$$

- ii.  $\exists$  a *section* of  $\beta$ , that is, a map  $s : N \longrightarrow M$  such that  $\beta \circ s = id_N$

- iii.  $\exists$  a *retraction* of  $\alpha$ , that is, a map  $r : M \longrightarrow L$  such that  $r \circ \alpha = id_L$

If all i, ii, iii are satisfied, it is a split exact sequence.

*Proof.* Intuitively, when a s.e.s. *splits* it means that the middle module  $M$  is the direct sum of the other (outer) two modules, ie.  $M = L \oplus N$ .

- (i to ii, iii) if  $M \cong L \oplus N$  such that  $\alpha : m \longmapsto (m, 0)$ ,  $\beta : s(m, n) \longmapsto n$ , we can define the maps

for ii:

$$\begin{aligned}s : N &\longrightarrow L \oplus N \\ s(n) &\longmapsto (0, n)\end{aligned}$$

Then  $\beta(s(n)) = \beta(0, n)$ , so  $\beta \circ s = id_N$ .

for iii:

$$\begin{aligned}r : L \oplus N &\longrightarrow L \\ r(m, n) &\longmapsto m\end{aligned}$$

Then  $r(\alpha(m)) = r(m, 0)$ , so  $r \circ \alpha = id_L$ .

- (ii to i) assume  $s : N \longrightarrow M$  such that  $\beta \circ s = id_N$

Want to show  $M \cong im(\alpha) \oplus im(s)$ .

$\forall m \in M$ , consider  $m - s(\beta(m))$ , apply  $\beta$  to it:

$$\beta(m - s(\beta(m))) = \beta(m) - (\beta \circ s)(\beta(m)) = \beta(m) - \beta(m) = 0$$

Since  $\ker(\beta) = im(\alpha)$ ,  $\exists ! l \in L$  such that  $\alpha(l) = m - s(\beta(m))$ .

Thus  $m = \alpha(l) + s(\beta(m))$ .

Now, suppose  $x \in \text{im}(\alpha) \cap \text{im}(s)$ , then  $x = \alpha(l) = s(n)$ , apply  $\beta$  to it:  
 $\beta(\alpha(l)) = \beta(s(n)) \implies 0 = n$ .

If  $n = 0$ , then  $s(n) = 0$ , so the intersection is  $\{0\}$ .

Define

$$\begin{aligned}\phi : L \oplus N &\longrightarrow M \\ \phi(l, n) &\longmapsto \alpha(l) + s(n)\end{aligned}$$

This isomorphism satisfies the required conditions.

(iii to i) similar to the previous one.

Overview:

$$0 \longrightarrow L \xrightarrow[r]{\alpha} M \xleftarrow[s]{\beta} N \longrightarrow 0$$

$$\begin{aligned}\alpha : l &\longmapsto (l, 0) \\ r : (m, n) &\longmapsto m \\ \alpha \circ r &= \text{id}_L \\ \beta : (l, n) &\longmapsto n \\ s : n &\longmapsto (0, n) \\ \beta \circ s &= \text{id}_N\end{aligned}$$

□

### 3 Noetherian rings (and modules)

**Definition** (Ascending Chain Condition). A partially ordered set  $\Sigma$  has the *ascending chain condition* (a.c.c.) if every chain

$$s_1 \leq s_2 \leq \dots \leq s_k \leq \dots$$

eventually breaks off, that is,  $s_k = s_{k+1} = \dots$  for some  $k$ .

$\implies \Sigma$  has the a.c.c. iff every non-empty subset  $S \subset \Sigma$  has a maximal element.

if  $\neq S \subset \Sigma$  does not have a maximal element, choose  $s_1 \in S$ , and for each  $s_k$ , an element  $s_{k+1}$  with  $s_k < s_{k+1}$ , thus contradicting the a.c.c.

### 3.1 Noetherian rings and modules

**Definition R.3.2** (Noetherian ring). Let  $A$  a ring; 3 equivalent conditions:

- i. the set  $\Sigma$  of ideals of  $A$  has the a.c.c.; in other words, every increasing chain of ideals

$$I_1 \subset I_2 \subset \dots \subset I_k \subset \dots$$

eventually stops, that is  $I_k = I_{k+1} = \dots$  for some  $k$ .

- ii. every nonempty set  $S$  of ideals has a maximal element
- iii. every ideal  $I \subset A$  is finitely generated

If these conditions hold, then  $A$  is *Noetherian*.

*Proof.* TODO □

**Definition R.3.4.D** (Noetherian modules). An  $A$ -module  $M$  is Noetherian if the submodules of  $M$  have the a.c.c., that is, any increasing chain

$$M_1 \subset M_2 \subset \dots \subset M_k \subset \dots$$

of submodules eventually stops.

As in with rings, it is equivalent to say that

- i. any nonempty set of submodules of  $M$  has a maximal element
- ii. every submodule of  $M$  is finite

**Proposition R.3.4.P.** Let  $0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$  be a s.e.s. (split exact sequence, R.2.10).

Then,  $M$  is Noetherian  $\iff L$  and  $N$  are Noetherian.

*Proof.*  $\implies$ : trivial, since ascending chains of submodules in  $L$  and  $N$  correspond one-to-one to certain chains in  $M$ .

$\impliedby$ : suppose  $M_1 \subset M_2 \subset \dots \subset M_k \subset \dots$  is an increasing chain of submodules of  $M$ .

Then identifying  $\alpha(L)$  with  $L$  and taking intersection gives a chain

$$L \cap M_1 \subset L \cap M_2 \subset \dots \subset L \cap M_k \subset \dots$$

of submodules of  $L$ , and applying  $\beta$  gives a chain

$$\beta(M_1) \subset \beta(M_2) \subset \dots \beta(M_k) \subset \dots$$

of submodules of  $N$ .

Each of these two chains eventually stop, by the assumption on  $L$  and  $N$ , so that we only need to prove the following lemma which completes the proof. □

**Lemma R.3.4.L.** for submodules  $M_1 \subset M_2 \subset M$ ,

$$L \cap M_1 = L \cap M_2 \text{ and } \beta(M_1) = \beta(M_2) \implies M_1 = M_2$$

*Proof.* if  $m \in M_2$ , then  $\beta(m) \in \beta(M_1) = \beta(M_2)$ , so that there is an  $n \in M_1$  such that  $\beta(m) = \beta(n)$ .

Then  $\beta(m - n) = 0$ , so that

$$m - n \in M_2 \cap \ker(\beta) = M_1 \cap \ker(\beta)$$

Hence  $m \in M_1$ , thus  $M_1 = M_2$ .  $\square$

**Corollary R.3.5** (Properties of Noetherian modules). i. if  $\forall i \in [r]$ ,  $M_i$  are Noetherian modules, then  $\bigoplus_{i=1}^r M_i$  is Noetherian.

- ii. if  $A$  a Noetherian ring, then an  $A$ -module  $M$  is Noetherian iff it is finite over  $A$ .
- iii. if  $A$  a Noetherian ring,  $M$  a finite module, then any submodule  $N \subset M$  is again finite.
- iv. if  $A$  a Noetherian ring, and  $\psi : A \longrightarrow B$  a ring homomorphism such that  $B$  is a finite  $A$ -module, then  $B$  is a Noetherian ring.

*Proof.* i. a direct sum  $M_1 \oplus M_2$  is a particular case of an exact sequence.

Then, Proposition R.3.4.P proves this statement when  $r = 2$ . The case  $r > 2$  follows by induction.

- ii. if  $M$  finite, then  $\exists$  surjective homomorphism

$$A^r \longrightarrow M \longrightarrow 0$$

for some  $r$ , so that  $M$  is a quotient

$$M \cong A^r / N$$

for some submodule  $N \subset A^r$ .

$A^r$  is a Noetherian module by i., so  $M$  is Noetherian due Proposition R.3.4.P.

Conversely,  $M$  Noetherian implies  $M$  finite.

item as in previous implications:

$M$  finite and  $A$  Noetherian  $\implies M$  is Noetherian,

$\implies$  since  $N \subseteq M$ , then  $N$  is Noetherian too

$\implies$  which implies that  $N$  is a finite  $A$ -module.

- iii.  $B$  is Noetherian as an  $A$ -module; but ideals of  $B$  are submodules of  $B$  as an  $A$ -submodule, so that  $B$  is a Noetherian ring.  $\square$

### 3.2 Hilbert basis

**Theorem R.3.6** (Hilbert basis theorem). If  $A$  a Noetherian ring, then so is the polynomial ring  $A[x]$ .

*Proof.* Prove that any ideal  $I \subset A[x]$  is finitely generated.

Define auxiliary sets  $J_n \subset A$  by

$$J_n = \{a \in A \mid \exists f \in I \text{ s.t. } f = ax^n + b_{n-1}x^{n-1} + \dots + b_0\}$$

ie.  $J_n$  is the set of leading coefficients of  $I$  of degree  $n$ .

$J_n$  is an ideal, since  $I$  is an ideal.

$J_n \subset J_{n+1}$ , since for  $f \in I$  also  $xf \in I$ .

Therefore  $J_1 \subset J_2 \subset \dots \subset J_k \subset \dots$  is an increasing chain of ideals.

Using the assumption that  $A$  is Noetherian, deduce that  $J_n = J_{n+1}$  for some  $n$ .

For each  $m \leq n$ ,  $J_m \subset A$  is finitely generated, ie.

$$J_m = (a_{m,1}, \dots, a_{m,r_m})$$

By definition of  $J_m$ , for each  $a_{m,j}$  with  $1 \leq j \leq r_m$ ,

$\exists$  a polynomial  $f_{m,j} \in I$  of degree  $m$  having the leading coefficient  $a_{m,j}$ .

$$\implies \{f_{m,j}\}_{m < n; 1 \leq j \leq r_m}$$

the set of elements of  $I$ .

Claim: this finite set  $(\{f_{m,j}\})$  generates  $I$ .

$\forall f \in I$ , if  $\deg f = m$ , then its leading coefficient is  $a \in J_m$ ,

hence if  $m \geq n$ , then  $a \in J_m = J_n$ , so that

$$a = \sum b_i a_{n,i} \text{ with } b_i \in A$$

and

$$f - \sum b_i X^{m-n} \cdot f_{n,i}$$

has degree  $< m$ .

Similarly, if  $m \leq n$ , then  $a \in J_m$ , so that

$$a = \sum b_i a_{m,i} \text{ with } b_i \in A$$

and

$$f - \sum b_i f_{m,i}$$

has degree  $< m$ .

By induction on  $m$ ,  $f$  can be written as a linear combination of finitely many elements.

Thus, any ideal of  $A[x]$  is finitely generated.  $\square$

**Corollary R.3.6.C.** if  $A$  a Noetherian ring, and  $\psi : A \longrightarrow B$  a ring homomorphism such that  $B$  is a fingen extension ring of  $\psi(A)$ , then  $B$  is Noetherian.

In particular, any fingen algebra over  $\mathbb{Z}$  or over a field  $K$  is Noetherian.

*Proof.* the assumption is that  $B$  is a quotient of a polynomial ring,

$$B \cong A[x_1, \dots, x_n]/I$$

for some ideal  $I$ .

By the Hilbert basis theorem R.3.6 and induction,  
 $A$  being Noetherian implies that  $A[x_1, \dots, x_n]$  is Noetherian.

And by Corollary R.3.5(iv),  
 $A[x_1, \dots, x_n]$  being Noetherian implies that  $A[x_1, \dots, x_n]/I$  is Noetherian.  $\square$

## 4 Finite ring extensions and Noether normalization

### 4.1 A-algebras and integral domains

**Definition** ( $A$ -algebra). An  $A$ -algebra is a ring  $B$  with a ring homomorphism  $\psi : A \longrightarrow B$ .

$B$  is an  $A$ -module with multiplication defined by  $\psi(a) \cdot b$  ( $a \in A, b \in B$ ).

When  $A \subset B$ ,  $B$  is an extenaion ring of  $A$ ; denoted  $\psi(A) = A' \subset B$ .

**Definition R.4.1.** Let  $B$  be an  $A$ -algebra.

- i.  $B$  is a *finite*  $A$ -algebra (*finite over*  $A$ ) if it is finite as an  $A$ -module.
- ii.  $y \in B$  is *integral over*  $A$  if  $\exists$  a monic polynomial

$$f(Y) = Y^n + a_{n-1}Y^{n-1} + \dots + a_0 \in A'[Y]$$

such that  $f(y) = 0$  :

$$f(y) = y^n + a_{n-1}y^{n-1} + \dots + a_0 = 0$$

The algebra  $B$  is *integral over*  $A$  if  $\forall b \in B$  is integral.

**Proposition R.4.2.** Let  $\psi : A \longrightarrow B$  be an  $A$ -algebra, and  $y \in B$ . Three equivalent conditions:

- i.  $y$  is integral over  $A$
- ii. subring  $A'[y] \subset B$  generated by  $A' = \psi(A)$  and  $y$  is finite over  $A$



iii.  $\exists$  an  $A$ -subalgebra  $C \subset B$  such that  $A'[y] \subset C$  and  $C$  is finite over  $A$

Notes:  $A'$  is the image of  $A$  in  $B$ , ie.  $A' = \psi(A)$ .  
 $A'[y]$  is the smallest subring of  $B$  containing both coefficients from  $A$  and the element  $y$ .

*Proof.* .

(i to ii): since  $y$  integral over  $A \implies$  by R.4.1 (ii),  $y$  satisfies

$$f(y) = y^n + a_{n-1}y^{n-1} + \dots + a_0 = 0$$

So any power  $y^k$  ( $k \geq n$ ) can be expressed in terms of  $\{1, y, y^2, \dots, y^{n-1}\}$ .

Thus the set  $\{1, y, y^2, \dots, y^{n-1}\}$  spans  $A'[y]$  as an  $A$ -module.

(iii to i): since  $A'[y] \subset C \implies y \in C$

since  $C$  finite over  $A$ ,  $C$  has finite generators  $\{c_1, \dots, c_n\}$  such that  $C = A \cdot c_1 + A \cdot c_2 + \dots + A \cdot c_n$

Thus  $y \cdot c_i \in C$ ,

$$y \cdot c_i = \sum_{j=1}^n a_{ij}c_j$$

with  $a_{ij} \in A$ .

By the Cayley-Hamilton theorem (AM.2.4),

$$y^n + a_{n-1}y^{n-1} + \dots + a_1y + a_0 = 0$$

Therefore,  $y$  is integral (by R.4.1 (ii)).

□

**Proposition R.4.3** (Tower Laws). Let  $B$  be an  $A$ -algebra.

- a. Transitivity of finiteness: if  $A \subset B \subset C$  are extension rings such that  $C$  is a finite  $B$ -algebra and  $B$  a finite  $A$ -algebra, then  $C$  is finite over  $A$ .
- b. Finiteness of generated algebras: if  $y_1, \dots, y_m \in B$  are integral over  $A$ , then  $A[y_1, \dots, y_m]$  is finite over  $A$ .  
In particular, every  $f \in A[y_1, \dots, y_m]$  is integral over  $A$ .
- c. Transitivity of integrality: if  $A \subset B \subset C$  with  $C$  integral over  $B$ , and  $B$  integral over  $A$ , then  $C$  is integral over  $A$ .
- d. Integral closure as a subring: the subset

$$\tilde{A} = \{y \in B \mid y \text{ is integral over } A\} \subset B$$

is a subring of  $B$ .

Moreover, if  $y \in B$  is integral over  $\tilde{A}$  then  $y \in \tilde{A}$ , so that  $\tilde{\tilde{A}} = \tilde{A}$ .

*Proof.* .

- a. if  $\{\beta_1, \dots, \beta_n\}$  generate  $B$  as an  $A$ -module and  $\{\gamma_1, \dots, \gamma_n\}$  generate  $C$  as an  $B$ -module,  
then the set of products  $\{\beta_i \gamma_j\}$  generates  $C$  as an  $A$ -module.

Since there are  $n \times m$  generators (ie. finite),  $C$  is finite over  $A$ .

- b. proof by induction:

base case: if  $y_1$  integral over  $A \implies$  it satisfies a monic polynomial.

Thus  $A[y_1]$  is generated as an  $A$ -module by  $\{1, y_1, y_1^2, \dots, y_1^{n-1}\}$ , making it a finite  $A$ -algebra.

inductive step: let  $R_k = A[y_1, \dots, y_k]$ . Assume  $R_k$  is finite over  $A$ .

Since  $y_{k+1}$  is integral over  $A \implies$  it is also integral over  $R_k$ .

Thus  $R_{k+1} = R_k[y_{k+1}]$  is finite over  $R_k$ .

Applying part (a) (transitivity of finiteness), if  $R_{k+1}$  is finite over  $R_k$  and  $R_k$  finite over  $A$ , then  $R_{k+1}$  is finite over  $A$ .

Consequence: since any  $f \in A[y_1, \dots, y_m]$  belongs to a finite  $A$ -algebra,  $f$  must be integral over  $A$  (since an element is integral iff it is contained in a finite extension).

- c. let  $x \in C$ , since  $x$  integral over  $B$ , it satisfies:

$$x^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0 = 0, \quad b_i \in B$$

Let  $B'' = A[b_0, b_1, \dots, b_{n-1}]$ . Since each  $b_i \in B$  and  $B$  is integral over  $A \implies$  each  $b_i$  is integral over  $A$ .

Since all  $b_i$  are integral over  $B' \implies B'[x]$  is a finite  $B'$ -algebra.

By part (a) (transitivity of finiteness),  $B'[x]$  is a finite  $A$ -algebra.

Therefore,  $x$  is integral over  $A$ .

- d. I. subring:

let  $x, y \in \tilde{A}$ . Want to show  $x + y, xy \in \tilde{A}$ :

by part (b), the algebra  $A[x, y]$  is finite over  $A$ .

Since  $x + y, xy \in A[x, y]$ , they are integral over  $A$ .

Thus  $x + y, xy \in \tilde{A}$ , since  $\tilde{A} = \{b \in B \mid b \text{ integral over } A\}$ .

- II. idempotence

let  $z \in B$  be integral over  $\tilde{A}$

we have a chain  $A \subseteq \tilde{A} \subseteq \tilde{A}[x]$ .

By definition,  $\tilde{A}$  is integral over  $A$ , and  $z$  is integral over  $\tilde{A}$

thus by part (c),  $z$  is integral over  $A$ .

Therefore,  $z \in \tilde{A}$ .

□

**Lemma 4.3.Aux** (Integrality implies finiteness). If  $y$  integral over  $A$  then  $A[y]$  is finite over  $A$ .

This extends on point (b) from the previous proposition R.4.3.

*Proof.* Suppose  $y$  is integral over  $A$ . By definition  $\exists f \in A[T]$ , with  $f$  monic, such that  $f(y) = 0$ .

Let  $\deg(f) = d$ , so that for  $f(y) = 0$  we have

$$y^d + a_{d-1}y^{d-1} + \dots + a_1y + a_0 = 0 \quad a_i \in A$$

Since it is monic (leading coefficient is 1), we can rearrange it to isolate the highest power:

$$y^d = -(a_{d-1}y^{d-1} + \dots + a_1y + a_0) \quad (7)$$

Thus  $y^d$  can be written using lower powers of  $y$  with coefficients in  $A$ .

Consider any element  $p \in A[y]$ ,  $p = c_my^m + c_{m-1}y^{m-1} + \dots + c_0$ .  
if  $m < d$ , leave it as it is.

if  $m \geq d$ , use the monic equation (7) to replace  $y^d$  with lower powers.

Repeating this process, can reduce any power of  $y$  down to a linear combination of  $\{1, y, y^2, \dots, y^{d-1}\}$ .

Thus every element in  $A[y]$  can be expressed as

$$\lambda_{d-1}y^{d-1} + \dots + \lambda_2y^2 + \lambda_1y + \lambda_0 \cdot 1 \quad \lambda_i \in A$$

Henceforth, the set  $\{1, y, y^2, \dots, y^{d-1}\}$  generates  $A[y]$  as a finite  $A$ -module. □

**Definition 4.4** (Integral closure). Given the ring  $\tilde{A}$  from R.4.3.(d), ie.  $\tilde{A} = \{y \in B \mid y \text{ integral over } A\} \subset B$ ,  $\tilde{A}$  is the *integral closure* of  $A$  in  $B$ .

If  $A = \tilde{A}$ , then  $A$  is *integrally closed* in  $B$ .

An integral domain  $A$  is *normal* if it is *integrally closed in its field of fractions*, that is if

$$A = \tilde{A} \subset K = \text{Frac}(A)$$

For any integral domain  $A$ , the integral closure of  $A$  in its field of fractions  $K = \text{Frac}(A)$  is also called the *normalization* of  $A$ .

## 4.2 Noether normalization

**Definition 4.6** (Algebraically independent).  $y_1, \dots, y_n \in A$  are *algebraically independent* over  $K$  if the natural surjection  $K[Y_1, \dots, Y_n] \longrightarrow K[y_1, \dots, y_n]$  is an isomorphism.

$\implies \nexists F(y_1, \dots, y_n) = 0$  ( $F$  nonzero) with coefficients in  $K$ .

Recall: a  $K$ -algebra  $A$  is *fingen* over  $K$  if  $A = K[y_1, \dots, y_n]$  for some finite set  $y_1, \dots, y_n$ .

**Lemma R.4.6.L.** Let  $A = K[y_1, \dots, y_n]$  and  $0 \neq F \in K[Y_1, \dots, Y_n]$  such that  $F(y_1, \dots, y_n) = 0$ .

Then  $\exists y_1^*, \dots, y_{n-1}^* \in A$  such that  $y_n$  is integral over

$$A^* = K[y_1^*, \dots, y_{n-1}^*] \quad \text{and} \quad A = A^*[y_n]$$

*Proof.* Set  $y_i^* = y_i - y_n^{r_i}$  for  $i \in [n-1]$  and  $r_1, \dots, r_{n-1} \geq 1 \in \mathbb{Z}$ .

(ie.  $y_i = y_i^* + y_n^{r_i}$ )

Define  $G \in A$  by

$$G(y_1^*, \dots, y_{n-1}^*, y_n) = F(y_i^* + y_n^{r_i}, y_n) = 0$$

viewed as a relation for  $y_n$  over  $K[y_1^*, \dots, y_{n-1}^*]$ .

Since  $F$  is a polynomial in  $y_1, \dots, y_{n-1}^*$ , can write it as a sum of monomials

$$F = \sum_m a_m y^m = \sum_m a_m \prod y_i^{m_i}$$

where  $m = (m_1, \dots, m_n)$  and each  $a_m \neq 0$ .

Therefore,

$$G = \sum a_m \prod (y_i^* + y_n^{r_i})^{m_i}$$

which when expanding out, each summand  $a_m \prod (y_i^* + y_n^{r_i})^{m_i}$  has a unique term of highest order in  $y_n$ , namely  $a_m y_n^{(\sum r_i m_i)}$ .

Suppose we can arrange so that

$$m \neq m' \implies \sum r_i m_i \neq \sum r_i m'_i$$

Then  $\max\{\sum r_i m_i \mid m \text{ s.t. } a_m \neq 0\}$  is achieved in only one summand, so that there is no cancellation; thus the highest order term in  $G$  is  $a_m y_n^{(\sum r_i m_i)}$  (ie.  $a_m$  times a pure power of  $y_n$ ).  $\square$

**Theorem R.4.6** (Noether normalization lemma). Let  $K$  a field,  $A$  a fingen  $K$ -algebra.

Then  $\exists z_1, \dots, z_m \in A$  such that

- i.  $z_1, \dots, z_m$  are algebraically independent over  $K$
- ii.  $A$  is finite over  $B = K[z_1, \dots, z_m]$

That is, a fingen extension  $K \subset A$  can be written as a composite

$$K \subset B = K[z_1, \dots, z_m] \subset A$$

where  $K \subset B$  is a polynomial extension, and  $B \subset A$  is finite.

*Proof.* Let  $y_1, \dots, y_n$  be generators of  $A = K[y_1, \dots, y_n]$ .

if  $n = 0$ , nothing to prove since  $A$  is generated by 0 elements  $\implies A = K$ , and  $K$  is finite.

if  $n > 0$  we have two cases:

- $y_1, \dots, y_n$  are algebraically independent over  $K$ , then by definition 4.6  $A \cong K[y_1, \dots, y_n]$ , so that  $A$  is a finite module over itself, with  $m = n$ .
- $y_1, \dots, y_n$  are algebraically dependent over  $K$ ,

$$\exists 0 \neq f \in K[y_1, \dots, y_n] \text{ s.th } f(y_1, \dots, y_n) = 0$$

Want  $f$  to be *monic*, so that  $y_n$  is integral over new defined variables  $y_1^*, \dots, y_{n-1}^*$ . In other words, want some polynomial like

$$y_n^d + a_{d-1}y_n^{d-1} + \dots + a_1y_n + a_0 = 0 \quad a_i \in K[y_1^*, \dots, y_{n-1}^*]$$

ie. monic, so that by definition (R.4.1),  $y_n$  is integral over  $K[y_1^*, \dots, y_{n-1}^*]$ .

$\longrightarrow$  Change variables so that  $f$  becomes monic in one of the variables ( $y_n$ ); this allows to express one generator ( $y_n$ ) as an integral element over the others.

Following from Lemma R.4.6.L, define the new variables  $y_1^*, \dots, y_{n-1}^* \in A$  such that  $y_n$  is integral over

$$A^* = K[y_1^*, \dots, y_{n-1}^*], \text{ and } A = A^*[y_n]$$

Setting  $y_i^* = y_i - y_n^{r_i}$ , so that  $y_i = y_i^* + y_n^{r_i} \forall i \in [n-1]$ ,  $r_1, \dots, r_{n-1} \geq 1 \in \mathbb{Z}$ . Use those new variables at  $f(y_1, \dots, y_n) = 0$ :

$$f(y_1^* + y_n^{r_1}, y_2^* + y_n^{r_2}, \dots, y_{n-1}^* + y_n^{r_{n-1}}, y_n) = 0$$

Then the highest power of  $y_n$  in each term of  $f$  will look like  $y_n^{(\sum a_i r_i)}$ , and with  $r_i$  growing fast enough we ensure that each monomial in  $f$  produces a unique power of  $y_n$ .

Then we have  $c \cdot y_n^D + (\text{terms with lower powers of } y_n) = 0$  with  $c \in K \setminus \{0\}$ . So that dividing by  $c$  we get the shape  $y_n^D + \dots = 0$ , thus  $y_n$  is integral over  $A^* = K[y_1^*, \dots, y_{n-1}^*]$ .

Induction:

Since  $y_n$  integral over  $A^* \implies A = A^*[y_n]$  is finite over  $A^* = K[y_1^*, \dots, y_{n-1}^*]$  (by 4.3.Aux).

By inductive hypothesis on  $A^*$ ,  $\exists z_1, \dots, z_m \in A^*$  algebraically independent over  $K$  and with  $A^*$  finite over  $B = K[z_1, \dots, z_m]$ .

Therefore, each step of  $B \subset A^* \subset A^*[y_n] = A$  is finite, and  $A$  is finite over  $B$  as required.  $\square$

**Example .**  $A = K[X, Y]/(XY - 1)$ .  $Y$  is algebraic over  $K[X]$ , but not integral over  $K[Y]$ .

This corresponds to the fact that the hyperbola  $XY = 1$  has the line  $X = 0$  as an asymptotic line (so that its projection to the  $X$ -axis misses a root over  $X = 0$ ).

Take  $X' = X - \epsilon Y$  as the element of  $A$  instead of  $X$ ; then the relation becomes  $(X' + \epsilon Y)Y = 1$ , monic in  $Y$  if  $\epsilon \neq 0$ .

This corresponds geometrically to tilting the hyperbola a little before projecting, so that no longer has a vertical asymptotic line.

### 4.3 Weak Nullstellensatz

**Proposition R.4.9.** let  $A \subset B$  be an integral extension of integral domain, then  $A$  is a field  $\iff B$  is a field.

*Proof.*  $\implies$ :

let  $0 \neq x \in B$ , then  $\exists x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0 \quad a_i \in A$ , monic.

Since  $A$  is a field,  $\exists$  inverse, observe that:

$$\begin{aligned} x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 &= 0 \\ x(x^{n-1} + a_{n-1}x^{n-2} + \dots + a_1) &= -a_0 \\ -a_0^{-1}(x^{n-1} + a_{n-1}x^{n-2} + \dots + a_1) &= x^{-1} \in B \end{aligned}$$

thus there exists inverse in  $B$ , so  $B$  is a field too.

$\impliedby$ :

if  $B$  is a field and  $0 \neq x \in A$ , then  $x^{-1} \in B$ , so  $x^{-1}$  is integral over  $A$ .

So there is a relation of the form

$$(x^{-1})^n + a_{n-1}(x^{-1})^{n-1} + \dots + a_0 = 0$$

Therefore

$$\begin{aligned} (x^{-1})^n + a_{n-1}(x^{-1})^{n-1} + \dots + a_0 &= 0 \\ (x^{-1})^n &= -a_{n-1}(x^{-1})^{n-1} - \dots - a_0 \\ x^{-n} &= -a_{n-1}x^{-n+1} - \dots - a_0 \quad (\text{mult by } x^{n-1}) \\ x^{-n+(n-1)} &= -a_{n-1}x^{-n+1+(n-1)} - \dots - a_0x^{n-1} \\ x^{-1} &= -a_{n-1} - \dots - a_0x^{n-1} \in A \end{aligned}$$

thus there exists inverse in  $A$ , so  $A$  is a field too.  $\square$

**Theorem R.4.10** (Weak Nullstellensatz - Zariski's lemma). let  $k$  a field,  $K$  a  $k$ -algebra which

1. is finitely generated as a  $k$ -algebra
2. is a field

Then  $K$  is algebraic over  $k$ , so that  $k \subset K$  is a finite field extension. That is,  $[K : k] < \infty$ .

*Proof.*  $K = k[z_1, \dots, z_m]$  a field; want to show that  $K$  is algebraic over  $k$ .

Since  $K$  is a finitely generated  $k$ -algebra, by Noether normalization lemma (R.4.6),  $\exists z_1, \dots, z_m \in K$  such that

- are algebraically independent
- $K$  is integral over the polynomial ring  $A = k[z_1, \dots, z_m]$  (which by 4.3.Aux is finite)

Now we're at the situation of R.4.9:

$A \subset K$  is integral,  $K$  is a field  $\implies$  therefore  $A$  is a field.

Since  $z_1, \dots, z_m \in K$  are algebraically independent,

$\implies A = k[z_1, \dots, z_m]$  is a polynomial ring in  $m$  indeterminates, and this is a field only if  $m = 0$

(since in  $k[z_1]$  the element  $z_1$  is not invertible, since  $1/z_1$  is a rational function, not a polynomial).

So  $A = k$ ; which by Noether normalization we saw that  $K$  is integral over  $A = k$ , and by 4.3.Aux that it is finite, thus  $K$  is finite over  $k$ , ie.  $[K : k] < \infty$ , and  $K$  is algebraic over  $k$ .  $\square$

## 5 Exercises

For the exercises, I follow the assignments listed at [3].

The exercises that start with **R** are the ones from the book [2], and the ones starting with **AM** are the ones from the book [1].

### 5.1 Exercises Chapter 1

**Exercise R.1.1.** Ring  $A$  and ideals  $I, J$  such that  $I \cup J$  is not an ideal. What's the smallest ideal containing  $I$  and  $J$ ?

*Proof.* Take ring  $A = \mathbb{Z}$ . Set  $I = 2\mathbb{Z}$ ,  $J = 3\mathbb{Z}$ .

$I, J$  are ideals of  $A (= \mathbb{Z})$ . And  $I \cup J = 2\mathbb{Z} \cup 3\mathbb{Z}$ .

Observe that for  $2 \in I, 3 \in J \implies 2, 3 \in I \cup J$ , but  $2 + 3 = 5 \notin I \cup J$ .

Thus  $I \cup J$  is not closed under addition; thus is not an ideal.

Smallest ideal of  $\mathbb{Z} (= A)$  containing  $I$  and  $J$  is their sum:

$$I + J = \{a + b \mid a \in I, b \in J\}$$

$\gcd(2, 3) = 1$ , so  $I + J = \mathbb{Z}$ .

Therefore, smallest ideal containing  $I$  and  $J$  is the whole ring  $\mathbb{Z}$ .  $\square$

**Exercise R.1.5.** let  $\psi : A \longrightarrow B$  a ring homomorphism. Prove that  $\psi^{-1}$  takes prime ideals of  $B$  to prime ideals of  $A$ .

In particular if  $A \subset B$  and  $P$  a prime ideal of  $B$ , then  $A \cap P$  is a prime ideal of  $A$ .

*Proof.* (Recall: prime ideal is if  $a, b \in R$  and  $a \cdot b \in P$  (with  $R \neq P$ ), implies  $a \in P$  or  $b \in P$ ).

Let

$$\psi^{-1}(P) = \{a \in A \mid \psi(a) \in P\} = A \cap P$$

The claim is that  $\psi^{-1}(P)$  is prime ideal of  $A$ .

- i. show that  $\psi^{-1}(P)$  is an ideal of  $A$ :  
 $0_A \in \psi^{-1}(P)$ , since  $\psi(0_A) = 0_B \in P$  (since every ideal contains 0).  
 If  $a, b \in \psi^{-1}(P)$ , then  $\psi(a), \psi(b) \in P$ , so

$$\psi(a - b) = \psi(a) - \psi(b) \in P$$

hence  $a - b \in \psi^{-1}(P)$ .

If  $a \in \psi^{-1}(P)$  and  $r \in A$ , then  $\psi(ra) = \psi(r)\psi(a) \in P$ , since  $P$  is an ideal.  
 Thus  $ra \in \psi^{-1}(P)$ .

$\implies$  so  $\psi^{-1}$  is an ideal of  $A$ .

- ii. show that  $\psi^{-1}(P)$  is prime:  
 $\psi^{-1}(P) \neq A$ , since if  $\psi^{-1}(P) = A$ , then  $1_A \in \psi^{-1}(P)$ , so  $\psi(1_A) = 1_B \in P$ , which would mean that  $P = B$ , a contradiction since  $P$  is prime ideal of  $B$ .



Take  $a, b \in A$  with  $ab \in \psi^{-1}(P)$ ; then  $\psi(ab) \in P$ , and since  $\psi$  is a ring homomorphism,  $\psi(ab) = \psi(a)\psi(b)$ .

Since  $P$  prime ideal, then  $\psi(a)\psi(b) \in P$  implies either  $\psi(a) \in P$  or  $\psi(b) \in P$ . Thus  $a \in \psi^{-1}(P)$  or  $b \in \psi^{-1}(P)$ .

Hence  $\psi^{-1}(P) (= A \cap P)$  is a prime ideal of  $A$ .

□

**Exercise R.1.6.** prove or give a counter example:

- the intersection of two prime ideals is prime
- the ideal  $P_1 + P_2$  generated by 2 prime ideals  $P_1, P_2$  is prime
- if  $\psi : A \longrightarrow B$  ring homomorphism, then  $\psi^{-1}$  takes maximal ideals of  $B$  to maximal ideals of  $A$
- the map  $\psi^{-1}$  of Proposition 1.2 takes maximal ideals of  $A/I$  to maximal ideals of  $A$

*Proof.* a. let  $I = 2\mathbb{Z} = (2)$ ,  $J = 3\mathbb{Z} = (3)$  be ideals of  $\mathbb{Z}$ , both prime.

Then  $I \cap J = (2) \cap (3) = (6)$ .

The ideal  $(6)$  is not prime in  $\mathbb{Z}$ , since  $2 \cdot 3 \in (6)$ , but  $2 \notin (6)$  and  $3 \notin (6)$ .

Thus the intersection of two primes can not be prime.

- $P_1 = (2)$ ,  $P_2 = (3)$ , both prime.

Then,

$$P_1 + P_2 = (2) + (3) = \{a + b | a \in P_1, b \in P_2\}$$

$\longrightarrow$  in a principal ideal domain (like  $\mathbb{Z}$ ), the sum of two principal ideals is again principal, and given by  $(m) + (n) = (gcd(m, n))$ .

(recall: principal= generated by a single element)

So,  $P_1 + P_2 = (2) + (3) = (gcd(2, 3)) = (1) = \mathbb{Z}$ .

The whole ring is not a prime ideal (by the definition of the prime ideal), so  $P_1 + P_2$  is not a prime ideal.

Henceforth, the sum of two prime ideals is not necessarily prime.

- let  $A = \mathbb{Z}$ ,  $B = \mathbb{Q}$ ,  $\psi : A \longrightarrow B$ .

Since  $\mathbb{Q}$  is a field, its only maximal ideal is  $(0)$ .

Then

$$\begin{aligned} \psi^{-1}((0)) &= (0) \subset \mathbb{Z} \\ \text{ie. } \psi^{-1}(m_B) &= (m_B) \subset A \end{aligned}$$

But  $(0)$  is not maximal in  $\mathbb{Z}$ , because  $\mathbb{Z}/(0) \cong \mathbb{Z}$  is not a field.

Thus the preimages of maximal ideals under arbitrary ring homomorphisms need not be maximal.

d.  $\psi : A \longrightarrow A/I$  quotient homomorphism,  $I \subseteq A$  an ideal.

Let  $M$  a maximal ideal of  $A/I$ , then  $\frac{(A/I)}{M}$  is a field (Proposition 1.3).

By the isomorphism theorems,

$$\frac{(A/I)}{M} \cong \frac{A}{\psi^{-1}(M)}$$

Since  $\frac{(A/I)}{M}$  is a field, the quotient  $\frac{A}{\psi^{-1}(M)}$  is a field, so  $\psi^{-1}(M)$  is a maximal ideal of  $A$ .

$\implies$  under  $\psi$ , preimages of maximal ideals are maximal.

□

**Exercise R.1.12.a.** if  $I, J$  ideals and  $P$  prime ideal, prove that

$$IJ \subseteq P \iff I \cap J \subseteq P \iff I \text{ or } J \subseteq P$$

*Proof.* assume  $I \subseteq P$  (for  $J \subseteq P$  will be the same, symmetric), take  $x \in IJ$ , then

$$x = \sum_{k=1}^n a_k b_k$$

with  $a_k \in I$ ,  $b_k \in J$ .

Each  $a_k \in I \subseteq P$ . Since  $P$  an ideal,

$$\sum_{k=1}^n a_k b_k \in P$$

thus  $x \in P$ , hence  $IJ \subseteq P$ .

So  $I \subseteq P$  or  $J \subseteq P \implies IJ \subseteq P$ .

Conversely,

assume  $P$  prime and  $IJ \subseteq P$ .

Suppose by contradiction that  $I \not\subseteq P$  and  $J \not\subseteq P$ .

- since  $I \not\subseteq P$ ,  $\exists a \in I$  with  $a \notin P$

- since  $J \not\subseteq P$ ,  $\exists b \in J$  with  $b \notin P$

Since  $a \in I$ ,  $b \in J$ ,  $ab \in IJ \subseteq P$ , but  $P$  is prime, so  $ab \in P$  implies that  $a \in P$  or  $b \in P$ . This contradicts  $a, b$  being taken outside of  $P$ .

Thus  $I \not\subseteq P$  and  $J \not\subseteq P$  are false.

So both directions are proven, hence

$$IJ \subseteq P \implies I \subseteq P \text{ or } J \subseteq P$$

□

**Exercise R.1.18.** Use Zorn's lemma to prove that any prime ideal  $P$  contains a minimal prime ideal.

*Proof.* Let  $P$  prime ideal of  $R$ .

$$S = \{Q \subseteq R \mid Q \text{ a prime ideal AND } Q \subseteq P\}$$

Goal: show that  $S$  has a minimal element, the minimal ideal contained in  $P$ .

$P \subset S$ , so  $S$  is nonempty.

Let  $C \subseteq S$  be a chain (= totally ordered subset) with respect to inclusion.

Define

$$Q_C = \bigcap_{Q \in C} Q$$

Clearly  $Q_C \subseteq P$ , since each  $Q \in C$  is  $Q \subseteq P$ .

Since  $C$  is ordered by inclusion, it is a decreasing chain of prime ideals.

Intersection of a decreasing chain of prime ideals is again a prime ideal:

- if  $ab \in Q_C$ , then  $ab \in Q \forall Q \in C$
- since  $Q$  prime,  $\forall Q \in C$  either  $a \in Q$  or  $b \in Q$

If there were some  $Q_1, Q_2 \in C$  with  $a \in Q_1$  and  $b \notin Q_2$ , then by total ordering, either  $Q_1 \subseteq Q_2$  or  $Q_2 \subseteq Q_1$ .

In either case: contradiction, since the smaller one would have to contain the element that was assumed to be excluded.

Thus  $\forall Q \in C$  the same element  $a, b$  must lie in all  $Q$ .  $\implies$  lies in the intersection of them,  $Q_C$ .

Henceforth,  $Q_C$  is a prime ideal and lies in  $S$ , and its a lower bound of  $C$  in  $S$ .

Now,  $S$  is nonempty, and every chain in  $S$  has a lower bound in  $S$  (its intersection).

Therefore,  $S$  has a minimal element  $P_{min}$ .

By construction,  $P_{min}$  is a prime ideal  $P_{min} \subseteq P$ , and by minimality there are no strictly smaller prime ideals inside  $P$ .

So  $P_{min}$  is a minimal prime ideal, contained in  $P$ . □

**Exercise R.1.10.**

*Proof.* □

**Exercise R.1.11.**

*Proof.* □

**Exercise R.1.4.**

*Proof.* □

## 5.2 Exercises Chapter 2

**Exercise R.2.9.**  $0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$  is a s.e.s. of  $A$ -modules. Prove that if  $N, L$  are finite over  $A$ , then  $M$  is finite over  $A$ .

*Proof.* Denote the generators of  $L$  and  $N$  respectively as

$$\begin{aligned} \{l_1, \dots, l_k\} &\subseteq L \\ \{n_1, \dots, n_p\} &\subseteq N \end{aligned}$$

By s.e.s. definition,

-  $\alpha$  is injective (one-to-one), so

$$\forall l_i \in L, \exists x_i \in M \text{ s.th. } \alpha(l_i) = x_i$$

-  $\beta$  is surjective (onto), so

$$\forall n_j \in N, \exists y_j \in M \text{ s.th. } \beta(y_j) = n_j$$

We will show that  $\{x_1, \dots, x_k, y_1, \dots, y_p\}$  generate  $M$ , and thus  $M$  is finite:  
Let  $m \in M$ , then  $\beta(m) \in N$ , and

$$\beta(m) = \sum_{j=1}^p a_j n_j \quad \text{with } a_j \in A$$

Take  $m' \in M$ , with  $m' = \sum a_j y_j$ , then

$$\beta(m') = \sum a_j \beta(y_j) = \sum a_j n_j = \beta(m)$$

Then, since  $\beta(m) = \beta(m') \implies \beta(m - m') = 0$ , thus

$$(m - m') \in \ker(\beta)$$

By *exactness* property, since  $\alpha : L \longrightarrow \ker(\beta)$ , we have  $\ker(\beta) = \text{im}(\alpha)$ .

Therefore,  $\exists l \in L$  such that  $\alpha(l) = m - m'$ .

Since  $\{l_i\}_k$  generate  $L$ ,

$$l = \sum_{i=1}^k b_i l_i$$

thus

$$m - m' = \alpha(l) = \alpha\left(\underbrace{\sum_{i=1}^k b_i l_i}_l\right) = \sum_{i=1}^k b_i \underbrace{\alpha(l_i)}_{x_i} = \sum_{i=1}^k b_i x_i$$

Rearrange,

$$m = m' + \sum_{i=1}^k b_i x_i = \sum_{j=1}^p a_j y_j + \sum_{i=1}^k b_i x_i \quad \forall m \in M$$

So,  $L$  provides  $k$  generators for the kernel part of  $M$ ,  $N$  provides  $p$  "lifts" for the quotient part of  $M$ ; thus  $M$  is generated by  $k + p$  elements.  
Thus  $M$  is finitely generated over  $A$ . □

### 5.3 Exercises Chapter 3

**Exercise R.3.2.**  $K$  a field,  $A \supset K$  a ring which is finite dimensional as a  $K$ -vector space. Prove that  $A$  is Noetherian and Artinian.

*Proof.*  $\dim(A) = n < \infty$ , so every ideal  $\mathfrak{a}$  of  $A$  is a  $K$ -subspace of  $A$ , because if  $x \in \mathfrak{a}$  and  $c \in K$ , then  $c \cdot x \in \mathfrak{a}$ .

1. Noetherian:

let  $I_1 \subseteq I_2 \subseteq \dots$  be an ascending chain of ideals in  $A$ .

Since each  $I_i$  is a subspace, we have

$$\dim_K(I_1) \leq \dim_K(I_2) \leq \dots \leq n$$

where at some  $i = m$  we have  $\dim_K(I_m) = \dim_K(I_{m+1})$ ; then since  $I_m \subseteq I_{m+1}$ , we have  $I_m = I_{m+1}$ . So  $A$  is Noetherian.

2. Artinian:

Similarly, if  $I_1 \supseteq I_2 \supseteq \dots$  a descending chain of ideals in  $A$ .

then

$$n \geq \dim_K(I_1) \geq \dim_K(I_2) \geq \dots \geq 0$$

where at some  $i = m$  we have  $\dim_K(I_m) = \dim_K(I_{m+1})$ ; then since  $I_m \supseteq I_{m+1}$ , we have  $I_m = I_{m+1}$ . So  $A$  is Artinian.

□

**Exercise R.3.5.** Let  $0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$  an exact sequence. Let  $M_1, M_2 \subseteq M$  be submodules of  $M$ .

Prove if the following holds or not:

$$\beta(M_1) = \beta(M_2) \text{ and } \alpha^{-1}(M_1) = \alpha^{-1}(M_2) \implies M_1 = M_2$$

*Proof.* Counterexample showing that it does not hold:

Let  $K$  a field,  $M = K \oplus K$ ,  $L = K$ ,  $N = K$ .

Set, for  $l \in L$ ,  $(m_1, m_2) \in M$ ,

$$\alpha : l \longmapsto (l, 0)$$

$$\beta : (m_1, m_2) \longmapsto m_2$$

So we have

$$0 \longrightarrow K \xrightarrow{\alpha} K^2 \xrightarrow{\beta} K \longrightarrow 0$$

Then,

$$M_1 = \{(x, x) \mid x \in K\} \sim (\text{diagonal line})$$

$$M_2 = \{(0, x) \mid x \in K\} \sim (\text{y-axis})$$

(Geometric interpretation:  $M_1$ ,  $M_2$  are the *diagonal line* and *y-axis* respectively; and  $\alpha$ ,  $\beta$  capture information about the *vertical* components (x-axis,

y-axis respectively), but not about the *diagonal* way a submodule is embedded in  $M$ ).

Then,

$$\begin{aligned}\beta(M_1) &= \{x \mid x \in K\} = K \\ \beta(M_2) &= \{x \mid x \in K\} = K\end{aligned}$$

thus,  $\beta(M_1) = \beta(M_2)$ .

For  $M_1$ ,  $(l, 0) \in M$  iff  $l = 0$ , thus  $\alpha^{-1}(M_1) = \{0\}$ ,  
for  $M_2$ ,  $(l, 0) \in M$  iff  $l = 0$ , thus  $\alpha^{-1}(M_2) = \{0\}$ ,  
thus  $\alpha^{-1}(M_1) = \alpha^{-1}(M_2)$ .

So we've seen that

$$\begin{aligned}\beta(M_1) &= \beta(M_2) \\ \alpha^{-1}(M_1) &= \alpha^{-1}(M_2)\end{aligned}$$

while having  $M_1 \neq M_2$ . □

**Exercise R.3.3.** Let  $A$  a ring,  $I_1, \dots, I_k$  ideals such that each  $A/I_i$  is a Noetherian ring. Prove that  $\bigoplus A/I_i$  is a Noetherian  $A$ -module, and deduce that if  $\bigcap I_i = 0$  then  $A$  is also Noetherian.

*Proof.* i. by Corollary R.3.5 (i), if  $M_i$  Noetherian modules, then  $\bigoplus M_i$  is Noetherian.  $\implies$  thus  $\bigoplus A/I_i$  is Noetherian.

ii. Take the canonical homomorphism

$$\phi : A \longrightarrow \bigoplus_{i=1}^n A/I_i$$

by  $\phi(a) = (a + I_1, a + I_2, \dots, a + I_n)$ .

$\phi$  is injective:  $\ker(\phi) = \{a \in A \mid a \in I_i \forall i\}$ .

Since we're given  $\bigcap I_i = 0$ , then  $\ker(\phi) = \bigcap I_i$ , and  $\phi$  is injective.

Thus,  $\phi$  is the isomorphism  $A \cong \text{im}(\phi)$ , where  $\text{im}(\phi)$  is an  $A$ -submodule of  $\bigoplus A/I_i$ .

We know that any submodule of a Noetherian module is Noetherian, thus, since

- $A/I_i$  is Noetherian by hypothesis of the exercise
- $A \cong \text{im}(\phi)$
- $\text{im}(\phi)$  is an  $A$ -submodule of  $\bigoplus A/I_i$

then,  $A$  is Noetherian. □

**Exercise R.3.4.** Prove that if  $A$  is a Noetherian ring and  $M$  a finite  $A$ -module, then there exists an exact sequence  $A^q \xrightarrow{\alpha} A^p \xrightarrow{\beta} M \rightarrow 0$ . That is,  $M$  has a presentation as an  $A$ -module in terms of finitely many generators and relations.

*Proof.* since  $M$  fingen  $\implies$  generators  $\{m_1, \dots, m_2\} \subseteq M$  span  $M$ .

Let  $\beta$  be a surjective  $A$ -linear map, which forms a free  $A$ -module of rank  $p$  onto  $M$ :

$$\begin{aligned} \beta : A^p &\longrightarrow M \\ (a_1, \dots, a_p) &\longmapsto \sum_{i=1}^p a_i m_i \end{aligned}$$

Let  $K = \ker(\beta)$ . By the 1st Isomorphism Theorem,

$$M \cong A^p / K$$

Since  $A$  is a Noetherian ring, then every free  $A$ -module of finite rank (eg.  $A^p$ ) is a Noetherian module.

Every submodule of a Noetherian module is fingen.

$\implies$  since  $K \subseteq A^p$ ,  $\implies K (= \ker(\beta))$  is fingen.

Since  $K$  fingen, let  $\{k_1, \dots, k_q\}$  be generators of  $K$ .

Define  $\psi : A^q \longrightarrow K$ .

Compose it with the inclusion map  $i : K \longrightarrow A^p$ ,

$$\alpha = i \circ \psi : A^q \longrightarrow A^p$$

So we have the whole sequence  $A^q \xrightarrow{\alpha} A^p \xrightarrow{\beta} M \rightarrow 0$ , where

- $\beta$  is surjective
- $\text{im}(\alpha) = \ker(\beta)$

so that it is a exact sequence, thus,  $M$  has a finite presentation.  $\square$

## 5.4 Exercises Chapter 4

**Exercise R.4.1.a.**  $k[X^2] \subset k[X]$  is a finite extension, hence integral. Find the integral dependence relation for any  $f \in k[X]$ .

*Proof.*  $\forall f(X) \in k[X]$  can be uniquely decomposed into its even and odd parts:

$$f(X) = p(X^2) + X \cdot q(X^2)$$

with  $p(X^2), q(X^2) \in k[X^2]$ , and

$p(X^2)$ : sum of all terms with even exponents

$q(X^2)$ : sum of all terms with odd exponents, and then factoring out  $X$ .

(Observation: this is used in FRI cryptographic protocol

[https://github.com/arnaucube/math/blob/master/notes\\_fri\\_stir.pdf](https://github.com/arnaucube/math/blob/master/notes_fri_stir.pdf))

Rearrange it

$$\begin{aligned}
f(X) - p(X^2) &= X \cdot q(X^2), \quad \text{square:} \\
(f(X) - p(X^2))^2 &= X^2 \cdot q(X^2)^2 \\
f(X)^2 - 2p(X^2)f(X) + p(X^2)^2 &= X^2 \cdot q(X^2)^2 \\
f(X)^2 - \underbrace{[2p(X^2)]}_{a_1} f(X) + \underbrace{[p(X^2)^2 - X^2 \cdot q(X^2)^2]}_{a_0} &= 0
\end{aligned}$$

Denote the last polynomial as  $P(T) \in k[X^2]$ , where  $f(X)$  is a root of  $P(T)$ .

The integral dependence relation for any  $f \in k[X]$  is given by the monic polynomial from R.4.1.ii, in this case  $T^2 + a_1T + a_0 = 0$  with  $a_i \in k[X^2]$ .

We have that

$$\begin{aligned}
a_1 &= -2p(X^2) \\
a_0 &= p(X^2)^2 - X^2q(X^2)^2
\end{aligned}$$

So for example, for  $f(X) = X^3 + X^2 + X + 1$ :

$$\begin{aligned}
f(X) &= (X^2 + 1) + X(X^2 + 1) \\
(f(X) - (X^2 + 1))^2 &= X^2(X^2 + 1)^2 \\
(f(X) - p(X))^2 &= X^2(q(X))^2
\end{aligned}$$

□

**Exercise R.4.5.** Let  $A = k[X, Y]/(Y^2 - X^2 - X^3)$ . Prove that the normalization of  $A$  is  $k[t]$  where  $t = Y/X$ .

*Proof.*  $A = k[X, Y]/(Y^2 - X^2 - X^3)$ , express  $X$  and  $Y$  in terms of  $t$ :

Since  $t = Y/X$  then  $Y = tX$ , and combined with  $Y^2 = X^2 + X^3$ , then

$$\begin{aligned}
(tX)^2 &= X^2 + X^3 \\
t^2X^2 &= X^2 + X^3, \quad \text{assuming } X \neq 0 : \\
t^2 &= 1 + X, \quad \text{thus} \\
X &= t^2 - 1 \in k[X]
\end{aligned}$$

Then,  $Y = tX = t(t^2 - 1) = t^3 - t \in k[X]$ .

Hence  $X, Y \in k[X]$ .

Therefore,  $k[X, Y]/(Y^2 - X^2 - X^3) \subseteq k[t]$ .

By R.4.6 (Noether normalization lemma), to show that  $k[t]$  is the *normalization*, must show that  $k[t]$  is *integral* over  $A$ .

From  $X = t^2 - 1 \implies t^2 - 1 - X = 0 \implies t^2 - (1 + X) = 0$ .

$(1 + X) \in A$ , so  $t$  satisfies the monic polynomial

$$P(T) = T^2 - (1 + X) \in A[T]$$



Thus  $t$  is integral over  $A$ .

Since  $k[t]$  is generated by  $t$  over  $k$ , and  $k \subset A$ , then the entire ring  $k[t]$  is integral over  $A$ .

Since  $k[t]$  is a polynomial ring over a field, which is a UFD, it is integrally closed (since all UFD are integrally closed).

$\text{Frac} A = k(X, Y)$ , since  $X = t^2 - 1$ ,  $Y = t^3 - t \implies k(X, Y) \subseteq k(t)$   
and  $t = Y/X \in k(X, Y)$ , thus  $k(X, Y) = k(t)$ .

Since  $k[t]$  is integrally closed and is the integral closure of  $A$  in its fraction field  $k(t)$ , we conclude that the normalization of  $A$  is  $k[t]$ .  $\square$

**Exercise R.4.9.**  $k$  a field,  $A = k[X, Y, Z]/(X^2 - Y^3 - 1, XZ - 1)$ , find  $\alpha, \beta \in k$  such that  $A$  is integral over  $B = k[X + \alpha Y + \beta Z]$ , and write a set of generators of  $A$  as a  $B$ -module.

*Proof.* (want to find a linear combination of the coordinates such that the original variables satisfy monic polynomials over the new ring  $B$ )

The relations defining  $A$  are

$$\begin{aligned} X^2 - Y^3 - 1 = 0 &\implies Y^3 = X^2 - 1 \quad (*) \\ XZ - 1 = 0 &\implies Z = 1/X = X^{-1} \end{aligned}$$

Thus  $A$  can be denoted as  $A = k[X, Y, X^{-1}]/(Y^3 - X^2 - 1)$ .

Now,  $Y$  is integral over  $k[X]$ , since  $Y^3 - (X^2 - 1) = 0$  is monic in  $Y$  with coefficients in  $k[X]$ .

$Z$  is not integral over  $k[X]$ , since  $Z = 1/X$  and  $X$  is not a unit in  $k[X]$ .

Choose  $\alpha, \beta \in k$  such that  $X$  (and thus  $Z$ ) becomes integral over  $B$ :

set  $\alpha = 0$ ,  $\beta = 1 \implies B = k[X + \alpha Y + \beta Z] = k[X + Z]$ .

Let  $w = X + Z$ ; since  $XZ = 1$ , we have

$$w = X + \frac{1}{X} \implies Xw = X^2 + 1 \implies X^2 - wX + 1 = 0 \quad (**)$$

which is monic with coefficients in  $k[w]$ , thus  $X$  is integral over  $B$ .

Since  $Z = w - X$ ,  $Z$  is also integral.

Generators of  $A$  as a  $B$ -module:

we have  $B = k[w]$  with  $w = X + Z$ .

From  $(**)$  we have  $X^2 - wX + 1 = 0$ , so  $X^2 = wX - 1$ .

Thus any polynomial in  $X$  can be reduced to a linear form  $b_1X + b_0$  with  $b_i \in k[w]$ . Hence it's partial basis is  $\{1, X\}$ .

Fitting  $X^2$  into  $(*)$ ,

$$\begin{aligned} X^2 - Y^3 - 1 &= 0 \\ Y^3 &= X^2 - 1 \\ Y^3 &= wX - 2 \end{aligned}$$

thus any power of  $Y$  higher than 2 can be reduced (eg.  $Y^4 = Y(wX - 2) = w(XY) - 2Y$ ).

So its partial basis is  $\{1, Y, Y^2\}$ .

For  $Z$ , since  $XZ = 1$  and  $w = X + Z \implies Z = w - X$ , thus  $Z$  is a  $B$ -linear combination of  $\{1, X\}$ .

Combining the previous partial basis, the generators are

$$\{1, X\} \times \{1, Y, Y^2\} = \{1, Y, Y^2, X, XY, XY^2\}$$

□

## References

- [1] M. F. Atiyah and I. G. MacDonald. Introduction to Commutative Algebra, 1969.
- [2] Miles Reid. Undergraduate Commutative Algebra, 1995.
- [3] Steven Kleiman. Commutative Algebra - MIT OpenCourseWare, 2008. <https://ocw.mit.edu/courses/18-705-commutative-algebra-fall-2008/>.