

# MATH 502 Notes

Jiantong Liu

October 26, 2023

Throughout the notes, we assume a ring  $R$  has a multiplicative identity and is commutative.

## 0 NOETHERIAN, ARTINIAN, AND LOCALIZATION

**Proposition 0.1.** Let  $R$  be a (commutative) ring, and let  $M$  be an  $A$ -module, then the following are equivalent:

- (i) Given an infinite increasing chain of submodules of  $M$

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq M_{n+1} \subseteq \cdots$$

then there exists some  $N \in \mathbb{N}$  such that  $M_N = M_{N+1} = \cdots$ , i.e., for all  $n \geq N$ ,  $M_n = M_{n+1}$ .

- (ii) Every non-empty family of submodules has a maximal element.

- (iii) Every submodule of  $M$  is finitely-generated.

*Proof.* (i)  $\Rightarrow$  (ii): This is a direct result of Zorn's lemma.

(ii)  $\Rightarrow$  (i): Obvious.

(i), (ii)  $\Rightarrow$  (iii): Take any submodule  $N$  of  $M$  and take  $x_1 \in N$ . If  $(x_1) \neq N$ , then there exists  $x_2 \in N \setminus (x_1)$ , so  $(x_1, x_2) \subseteq N$ , now we proceed inductively, but by the given property we know this stops in finite number of steps, hence we have  $N = (x_1, \dots, x_n)$  for some  $n \in \mathbb{N}$ , thus  $N$  is finitely-generated.

(iii)  $\Rightarrow$  (i): Note that the property implies  $M$  is finitely-generated, but that means the chain of submodules must be finite.  $\square$

**Definition 0.2** (Noetherian Module). If any of the conditions in [Proposition 0.1](#) holds, then  $M$  is said to be a Noetherian module. Alternatively, we say  $M$  satisfies the ascending chain condition.

**Proposition 0.3.** Let  $R$  be a (commutative) ring, and let  $M$  be an  $A$ -module, then the following are equivalent:

- (i) Given an infinite decreasing chain of submodules of  $M$

$$M_1 \supseteq M_2 \supseteq \cdots \supseteq M_n \supseteq M_{n+1} \supseteq \cdots$$

then there exists some  $N \in \mathbb{N}$  such that  $M_N = M_{N+1} = \cdots$ , i.e., for all  $n \geq N$ ,  $M_n = M_{n+1}$ .

- (ii) Every non-empty family of submodules has a minimal element.

*Proof.* Again, Zorn's lemma.  $\square$

**Definition 0.4** (Artinian Module). If any of the conditions in [Proposition 0.3](#) holds, then  $M$  is said to be a Artinian module. Alternatively, we say  $M$  satisfies the descending chain condition.

**Example 0.5.** •  $\mathbb{Z}$  is Noetherian.

- $\mathbb{Q}/\mathbb{Z}$  is not Noetherian.

- Let  $p$  be a prime. Let  $\mathbb{Z}(p^\infty)$  be the union of chains (as direct limits)

$$\left\langle \frac{\bar{1}}{p} \right\rangle \subseteq \left\langle \frac{\bar{1}}{p^2} \right\rangle \subseteq \cdots \subseteq \left\langle \frac{\bar{1}}{p^n} \right\rangle \subseteq \cdots$$

then there is an embedding  $\mathbb{Z}(p^\infty) \subseteq \mathbb{Q}/\mathbb{Z}$ , where  $\bar{a}$  is the image of  $a$  in  $\mathbb{Q}/\mathbb{Z}$ . With this construction,  $\mathbb{Z}(p^\infty)$  is Artinian.

**Exercise 0.6.** Show that  $\mathbb{Q}/\mathbb{Z} \cong \bigoplus_p \mathbb{Z}(p^\infty)$  where  $p$  traverses through all the primes.

**Proposition 0.7.** Let  $N$  be a submodule of  $M$ . Suppose  $M$  satisfies ascending (respectively, descending) chain condition, then  $N$  and  $M/N$  also satisfy ascending (respectively, descending) chain condition. If, for some submodule  $N$  of  $M$ , we know  $N$  and  $M/N$  satisfy ascending (respectively, descending) chain condition, then  $M$  also satisfies ascending (respectively, descending) chain condition.

*Proof.* Suppose  $M$  satisfies ascending (respectively, descending) chain condition, and let  $N$  be a submodule of  $M$ . Let  $\{N_i\}$  be an increasing (respectively, decreasing) sequence of submodules of  $N$ , then they can be regarded as submodules of  $M$ , therefore by the Noetherian (respectively, Artinian) condition, we know  $N$  satisfies ascending (respectively, descending) chain condition. Now let  $\bar{M} = M/N$ , and take  $\{\bar{M}_i\}$  be an increasing (respectively, decreasing) sequence of submodules of  $\bar{M}$ . Let  $\pi : M \rightarrow M/N$  be the quotient map, then the preimages give an increasing (respectively, decreasing) sequence  $\{M_i\}$  of submodules of  $M$ , where  $M_i = \pi^{-1}(\bar{M}_i)$ , but by the Noetherian (respectively, Artinian) condition, we know the sequence stops in finite steps, therefore the original sequence stops in finite steps as well, hence  $\bar{M}$  satisfies the ascending (respectively, descending) chain condition.

Suppose a submodule  $N$  of  $M$  is such that  $N$  and  $M/N$  both satisfy ascending chain condition. Take a submodule  $T$  of  $M$ , then we have a short exact sequence

$$0 \longrightarrow T \cap N \hookrightarrow T \longrightarrow T/(T \cap N) \longrightarrow 0$$

Now  $T \cap N$  is finitely-generated as  $N$  is finitely-generated, therefore we have an embedding  $T/(T \cap N) \hookrightarrow M/N$ , thus  $T/(T \cap N)$  is finitely-generated, therefore  $T$  is also finitely-generated by a vector space argument.

Suppose we have a decreasing sequence  $\{M_n\}$  of  $M$ , then we have a decreasing sequence  $\{N \cap M_n\}$ . Let  $\bar{M} = M/N$ , then  $\bar{M}_n := (M_n + N)/N$  defines a decreasing sequence of submodules in  $\bar{M}$ , but  $N$  satisfies the descending chain condition, so the sequence  $\{N \cap M_n\}$  stops in finite number of steps, say  $n_0$ . Moreover, the sequence of  $\bar{M}_n$ 's also stops in finite number of steps, so by definition the sequence of  $(M_n + N)/N$  stops in finite number of steps, say  $m_0$ , but by the isomorphism theorem this shows that the sequence of  $M_n/(N \cap M_n)$  stops in  $m_0$  steps. Therefore, whenever  $n \geq m_0, n_0$ , then  $N \cap M_n = N \cap M_{n+1}$ , hence  $M_n = M_{n+1} = \cdots$  for such  $n$ .  $\square$

**Remark 0.8.** The final argument should also work in the Noetherian case.

**Definition 0.9** (Simple Module). An  $A$ -module  $M$  is simple if the submodules of  $M$  are either 0 or  $M$ .

**Exercise 0.10.** Let  $A$  be a commutative ring, and  $M$  is an  $A$ -module, then  $M$  is simple if and only if  $M \cong A/\mathfrak{m}$  for some maximal ideal  $\mathfrak{m}$  of  $A$ .

**Definition 0.11** (Jordan-Hölder Chain). Let  $A$  be a commutative ring and  $M$  be an  $A$ -module. We say  $M$  has a Jordan-Hölder chain if there exists a decreasing chain of submodules  $\{M_i\}$  such that

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_{n-1} \supsetneq M_n = 0$$

such that  $M_i/M_{i+1}$  is simple. In such a situation, we know  $n$  is the length of the Jordan-Hölder chain, and such  $n$  is unique. We say  $M$  is a module of finite length, and the length is  $\ell_A(M) = n$ .

**Exercise 0.12.** Let  $A$  be a commutative ring, and let  $M$  be an  $A$ -module, then  $M$  is of finite length if and only if  $M$  is both Noetherian and Artinian.

**Theorem 0.13.** Let  $A$  be a commutative ring, then  $A$  is Artinian if and only if  $A$  is Noetherian and every prime ideal of  $A$  is maximal.

*Proof.* ( $\Leftarrow$ ):

**Lemma 0.14.** Let  $A$  be Noetherian, then every ideal of  $A$  contains a product of prime ideals.

*Subproof.* Suppose, towards contradiction, that there exists some ideal  $I$  of  $A$  that does not contain a product of prime ideals. Let  $\mathcal{J}$  be the set of such ideals of  $A$ , then  $\mathcal{J} \neq \emptyset$ , and we can take a maximal element of  $\mathcal{J}$ , namely  $J$ .<sup>1</sup> By definition,  $J$  is not prime, therefore there exists  $a, b \in A$  such that  $a \notin J$  and  $b \notin J$ , but  $ab \in J$ . Now  $J \subsetneq J + Aa$  and  $J \subsetneq J + Ab$ , therefore  $J + Aa, J + Ab \notin \mathcal{J}$ , therefore  $J + Aa$  and  $J + Ab$  both contain product of prime ideals. But now  $(J + Aa)(J + Ab)$  should also contain products of prime ideals, but by distribution this is just  $J^2 + Ja + Jb + Aab$ , which is contained in  $J$  because every term is contained in  $J$ , so  $J$  contains a product of prime ideals as well, contradiction. ■

In particular,  $(0)$  contains a product of prime ideals, in particular  $(0)$  equals to this product, but every prime ideal is maximal, therefore  $(0) = \mathfrak{m}_1 \cdots \mathfrak{m}_n$  becomes the product of maximal ideals (which may not necessarily be distinct), hence we have a descending chain of ideals

$$A \supseteq \mathfrak{m}_1 \supseteq \mathfrak{m}_1 \mathfrak{m}_2 \supseteq \cdots \supseteq \mathfrak{m}_1 \cdots \mathfrak{m}_n = (0),$$

and in particular  $(\mathfrak{m}_1 \cdots \mathfrak{m}_{i-1})/(\mathfrak{m}_1 \cdots \mathfrak{m}_i)$  is a finite-dimensional since  $A$  is Noetherian, and it has a natural structure as a  $A/\mathfrak{m}_i$ -vector space. From the short exact sequence

$$0 \longrightarrow \mathfrak{m}_1 \cdots \mathfrak{m}_i \longrightarrow \mathfrak{m}_1 \cdots \mathfrak{m}_{i-1} \longrightarrow (\mathfrak{m}_1 \cdots \mathfrak{m}_{i-1})/(\mathfrak{m}_1 \cdots \mathfrak{m}_i) \longrightarrow 0$$

we know the two sides of the sequence are Artinian, hence the central term is Artinian. Proceeding inductively, we know that  $\mathfrak{m}_1$  is Artinian, and  $R/\mathfrak{m}_1$  would also be Artinian, hence  $A$  is Artinian.

( $\Rightarrow$ ): Now suppose  $A$  is Artinian, and we want to show that every prime ideal is maximal, and  $(0)$  is a product of maximal ideals. The result then follows from the argument above.

**Lemma 0.15.** Every Artinian domain is a field.

*Subproof.* Let  $0 \neq a \in A$ , then consider the chain

$$(a) \supseteq (a^2) \supseteq \cdots \supseteq (a^n) \supseteq \cdots$$

and by the Artinian property, for some large enough  $n$  the descending chain stops. Hence, we have  $a^n = \lambda a^{n+1}$  for some large enough  $n$  and some  $\lambda \in A$ . Hence,  $a^n(1 - \lambda a) = 0$ , by the cancellation property of a domain, since  $a \neq 0$ , we must have  $\lambda a = 1$ , therefore  $a$  is a unit, as desired. ■

**Corollary 0.16.** Let  $A$  be Artinian, then every prime ideal of  $A$  is maximal.

Finally, it suffices to show that  $(0) = \mathfrak{m}_1 \cdots \mathfrak{m}_n$ . Let  $\mathfrak{J}$  be the set of finite products of maximal ideals, then  $\mathfrak{J}$  has a minimal element, and it suffices to show that this element is  $(0)$ . Suppose not, let  $I \neq (0)$  be a minimal element of  $\mathfrak{J}$ . For any two ideals  $\alpha, \beta$  of  $A$ , let  $(\alpha : \beta) = \{a \in A \mid a\beta \subseteq \alpha\}$ . Note that this has a natural structure as an ideal of  $A$ . Let  $J = ((0) : I)$ , and suppose  $J = A$ , then  $I = 0$ , contradiction, so  $J \neq A$  is a proper ideal of  $A$ , now consider  $A/J$  which is Artinian, then let  $\mathfrak{G}$  be the set of all non-zero ideals of  $A/J$ , so  $\mathfrak{G}$  has a minimal element as well, call it  $\bar{H}$ . Let  $H = \pi^{-1}(\bar{H})$  where  $\pi : A \rightarrow A/J$ , so we have  $J \subsetneq H$ , thus let  $P = (J : H)$ .

**Claim 0.17.**  $P$  is a prime ideal.

*Subproof.* Given  $c, d \notin P$ , we want to show that  $cd \notin P$ . Indeed, consider  $J \subsetneq J + cH \subseteq H$ , then since  $H$  is minimal, then  $J + cH = H$ , and similarly we have that  $J + dH = H$ . Therefore, we have that  $J + cdH = J + c(dH + J) = J + cH = H$ , hence we know  $cd \notin P$ , as desired. ■

Now  $P = (J : H)$  and  $J = (0 : I)$ , the by definition we have  $PHI = (0)$ . Since  $P$  is a prime ideal, then  $P$  is maximal, and now

$$(0 : PI) \supseteq H \supsetneq J = (0 : I)$$

Therefore  $PI \subsetneq I$ , where  $I$  is a minimal element, contradiction, hence  $(0)$  is a product of maximal ideals. □

<sup>1</sup>The existence of this maximal element is the result of Zorn's lemma and ACC condition.

**Definition 0.18** (Short Exact Sequence). Consider the sequence

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} T \longrightarrow 0$$

This is called a short exact sequence if  $\ker(f) = 0$ ,  $\operatorname{im}(g) = T$ , and  $\ker(g) = \operatorname{im}(f)$ . In particular, one slot of the sequence is said to be exact if the kernel of the previous map equals to the image of the subsequent map.

**Definition 0.19** (Flat Module). Let  $M$  be an  $A$ -module, then we say  $M$  is a flat  $A$ -module if for every short exact sequence

$$0 \longrightarrow N_1 \longrightarrow N_2 \longrightarrow N_3 \longrightarrow 0$$

the tensored sequence

$$0 \longrightarrow M \otimes_A N_1 \longrightarrow M \otimes_A N_2 \longrightarrow M \otimes_A N_3 \longrightarrow 0$$

remains exact.

**Remark 0.20.** Recall that the properties of modules have the following implications: free  $\Rightarrow$  projective  $\Rightarrow$  flat  $\Rightarrow$  torsion-free, and in the case of finitely-generated modules, torsion-free  $\Rightarrow$  free.

**Remark 0.21.** We already know that the tensor functor is right exact, namely given the short exact sequence above, then

$$M \otimes_A N_1 \longrightarrow M \otimes_A N_2 \longrightarrow M \otimes_A N_3 \longrightarrow 0$$

is exact.

**Exercise 0.22.** Let  $M$  be an  $A$ -module, and if there exists a short exact sequence of  $A$ -modules

$$0 \longrightarrow N_1 \longrightarrow N_2 \longrightarrow N_3 \longrightarrow 0$$

where  $N_1$  and  $N_2$  are finitely-generated as  $A$ -modules, and such that tensoring  $M$  preserves the short exact sequence, then  $M$  is flat.

**Definition 0.23** (Multiplicatively Closed Subset). Let  $A$  be a commutative ring and  $M$  be an  $A$ -module. Let  $S \subseteq A$  be a subset. We say  $S$  is a multiplicatively closed subset of  $A$  if  $1 \in S$ ,  $0 \notin S$ , and whenever  $s_1, s_2 \in S$ , then  $s_1 s_2 \in S$ .

**Definition 0.24** (Localization). Let  $S \subseteq A$  be a multiplicatively closed subset, and let  $M$  be an  $A$ -module, then  $S^{-1}M = (M \times S)/\sim$ , where  $\sim$  is an equivalence relation defined by the following:  $(m_1, s_1) \sim (m_2, s_2)$  if and only if there exists  $t \in S$  such that  $t(m_1 s_2 - m_2 s_1) = 0$ .  $S^{-1}M$  is said to be the localization of  $M$  at  $S$ .

Given  $(m, s) \in M \times S$ , we write  $\overline{(m, s)}$  to be the equivalence class in  $S^{-1}M$  represented by  $(m, s)$ .

**Exercise 0.25.** Similarly, one can define the localization  $S^{-1}A$  of  $A$  at  $S$ . In fact,  $S^{-1}A$  inherits a ring structure from  $A$ , namely

- $\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}$ ,
- $\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}$ ,
- $\frac{1}{s} \cdot \frac{s}{1} = \frac{1}{1} = 1$ .

**Remark 0.26.** Note that a ring structure does not guarantee every element to have a multiplicative inverse. The localization of  $A$  at  $S$  ensures that every element of  $S$  now becomes invertible in the new ring  $S^{-1}A$ . In particular, this induces a ring homomorphism

$$\begin{aligned} f : A &\rightarrow S^{-1}A \\ a &\mapsto \frac{a}{1} \end{aligned}$$

This homomorphism is injective if  $A$  is a domain.

**Remark 0.27.** Let  $I$  be an ideal of  $A$ .

- Consider the ring homomorphism  $f : A \rightarrow S^{-1}A$  above, then

$$S^{-1}I = IS^{-1}A = f(I)S^{-1}A.$$

In particular,  $f^{-1}(IS^{-1}A) \supseteq I$ .

- If  $I \cap S \neq \emptyset$ , then  $IS^{-1}A = S^{-1}A$ .
- If  $P$  is a prime ideal of  $A$  such that  $P \cap S = \emptyset$ , then  $f^{-1}(PS^{-1}A) = P$ .
- Let  $M$  be an  $A$ -module, then if  $N \subseteq M$  is a submodule, then  $S^{-1}N \subseteq S^{-1}M$ . That is, given an exact sequence

$$0 \longrightarrow N \longrightarrow M$$

then we obtain an exact sequence

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

Indeed, given  $0 \rightarrow N \xrightarrow{f} M$ , say we have it sending  $\frac{n}{1} \mapsto \frac{f(n)}{1} = 0$ , then there exists  $s \in S$  such that  $sf(n) = 0$ , so  $f(sn) = 0$ , therefore  $sn = 0$  by injection, hence  $\frac{n}{1} = 0$  in  $S^{-1}N$  as well.

**Exercise 0.28.** The localization functor is exact.

**Lemma 0.29.** Let  $A$  be a commutative ring and  $S$  be a multiplicatively closed subset of  $A$ , then  $S^{-1}A \otimes_A M \cong S^{-1}M$ .

*Proof.* We define

$$\begin{aligned} \varphi : S^{-1}A \otimes_A M &\rightarrow S^{-1}M \\ \frac{a}{s} \otimes m &\mapsto \frac{am}{s}. \end{aligned}$$

For any  $\frac{m}{s} \in S^{-1}M$ , we have  $\varphi\left(\frac{1}{s} \otimes m\right) = \frac{m}{s}$ , so the map is onto. Now suppose  $\varphi\left(\sum_{i=1}^n \frac{a_i}{s_i} \otimes m_i\right) = 0$  (since this is a finite sum), then  $\varphi\left(\sum_{i=1}^n \frac{a_i}{s_i} \otimes m_i\right) = \sum_{i=1}^n \frac{a_i m_i}{s_i} = 0$ . We make  $s = s_1 \cdots s_n$ , so

$$\frac{a_i}{s_i} \otimes m_i = \frac{a_i s_1 \cdots s_{i-1} s_{i+1} \cdots s_n}{s} \otimes m_i =: \frac{b_i}{s} \otimes m_i,$$

then  $\sum_{i=1}^n \frac{a_i}{s_i} \otimes m_i = \sum_{i=1}^n \frac{b_i}{s} \otimes m_i$ , therefore

$$\varphi\left(\sum_{i=1}^n \frac{a_i}{s_i} \otimes m_i\right) = \varphi\left(\sum_{i=1}^n \frac{b_i}{s} \otimes m_i\right) = \frac{\sum_{i=1}^n b_i m_i}{s} = 0,$$

so there exists  $t \in S$  such that  $t \sum_{i=1}^n b_i m_i = 0$ , now

$$\begin{aligned} \sum_{i=1}^n \frac{a_i}{s_i} \otimes m_i &= \sum_{i=1}^n \frac{b_i}{s} \otimes m_i \\ &= \sum_{i=1}^n \frac{1}{s} \otimes b_i m_i \\ &= \frac{1}{s} \otimes \sum_{i=1}^n b_i m_i \end{aligned}$$

$$\begin{aligned}
 &= \frac{t}{ts} \otimes \sum_{i=1}^n b_i m_i \\
 &= \frac{1}{ts} \otimes t \sum_{i=1}^n b_i m_i \\
 &= \frac{1}{ts} \otimes 0 \\
 &= 0.
 \end{aligned}$$

□

**Proposition 0.30.** The map  $A \rightarrow S^{-1}A$  is  $A$ -flat, i.e.,  $S^{-1}A$  is a flat  $A$ -module.

*Proof.* Consider

$$0 \longrightarrow N \longrightarrow M \longrightarrow T \longrightarrow 0$$

By [Lemma 0.29](#) (since the isomorphism is functorial), it suffices to show the exactness of

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

and this follows from [Exercise 0.28](#). □

**Definition 0.31** (Quasi-local, Local). Let  $A$  be a commutative ring. We say  $A$  is quasi-local if  $A$  has exactly one maximal ideal. In particular, if  $A$  is also Noetherian, then we say  $A$  is a local ring.

**Definition 0.32** (Localization). Let  $A$  be a commutative ring and  $\mathfrak{p}$  be a prime ideal of  $A$ . Note that  $S = A \setminus \mathfrak{p}$  is a multiplicatively closed subset, then we write  $S^{-1}A = A_{\mathfrak{p}}$  (in general, we have  $S^{-1}M = M_{\mathfrak{p}}$ , where  $M \otimes_A A_{\mathfrak{p}} \cong M_{\mathfrak{p}}$ ) to denote the localization of  $A$  away from the prime ideal  $\mathfrak{p}$ .

**Exercise 0.33.**  $A_{\mathfrak{p}}$  is quasi-local with unique maximal ideal  $\mathfrak{p}A_{\mathfrak{p}}$ .

**Remark 0.34.** Take  $x \in M$ , then the following are equivalent:

- $x = 0$ ;
- $\frac{x}{1} = 0$  in  $M_{\mathfrak{m}}$  for any maximal ideal  $\mathfrak{m}$  of  $A$ ;
- $\frac{x}{1} = 0$  in  $M_{\mathfrak{p}}$  for any prime ideal  $\mathfrak{p}$  of  $A$ .

*Proof.* We will prove the first two are equivalent. The  $(\Rightarrow)$  direction is obvious. Conversely, let  $I = \{a \in A \mid ax = 0\}$  to be the annihilator of  $x$  in  $A$ . Suppose, towards contradiction, that  $I \neq A$ , then  $I$  is contained in some maximal ideal  $\mathfrak{m}$  of  $A$ , then consider  $M_{\mathfrak{m}}$ . Since  $\frac{x}{1} = 0$  in  $M_{\mathfrak{m}}$ , then there exists  $t \in A \setminus \mathfrak{m}$  such that  $tx = 0$ , but  $I \subseteq \mathfrak{m}$  and  $t \notin \mathfrak{m}$ , then we reach a contradiction, hence  $I = A$ , and obviously we are done. □

**Exercise 0.35.** 1. Given the sequence

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$$

the following are equivalent:

- the sequence is exact;
- the sequence

$$0 \longrightarrow M_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}}} N_{\mathfrak{m}} \xrightarrow{g_{\mathfrak{m}}} T_{\mathfrak{m}} \longrightarrow 0$$

is exact for all maximal ideals  $\mathfrak{m}$  of  $A$ ;

- the sequence

$$0 \longrightarrow M_{\mathfrak{p}} \xrightarrow{f_{\mathfrak{p}}} N_{\mathfrak{p}} \xrightarrow{g_{\mathfrak{p}}} T_{\mathfrak{p}} \longrightarrow 0$$

is exact for all prime ideals  $\mathfrak{p}$  of  $A$ .

To see this, apply [Remark 0.34](#).

2. Let  $A$  be a commutative ring and  $M$  be an  $A$ -module, then the following are equivalent:

- $M$  is  $A$ -flat;
- $M_{\mathfrak{m}}$  is  $A_{\mathfrak{m}}$ -flat for all maximal ideals  $\mathfrak{m}$  of  $A$ ;
- $M_{\mathfrak{p}}$  is  $A_{\mathfrak{p}}$ -flat for all prime ideals  $\mathfrak{p}$  of  $A$ ;

Hence, exactness is a local property.

**Exercise 0.36.** Let  $A$  be a commutative ring, then  $A$  is Artinian if and only if  $A$  as an  $A$ -module is of finite length, i.e.,  $\ell_A(A) < \infty$ . Indeed, note that  $(0) = \mathfrak{m}_1 \cdots \mathfrak{m}_n$ , and write down the Jordan-Hölder series.

## 1 PRIMARY DECOMPOSITION THEOREM

Throughout [Section 1](#), the commutative ring  $A$  is always Noetherian. In [Section 1.1](#),  $M$  is a finitely-generated  $A$ -module; in [Section 1.2](#), we drop this assumption.

## 1.1 FINITELY-GENERATED CASE

**Definition 1.1** (Coprimary). We say  $M$  is a coprimary module if for all  $a \in A$ , the left multiplication  $m_a : M \rightarrow M$  is either injective or nilpotent (i.e., there exists  $n > 0$  such that  $a^n M = 0$ ).

**Remark 1.2.** (i) If  $M$  is coprimary, then  $N$  is coprimary for all  $N \subseteq M$ .

(ii) If  $M$  is coprimary, let  $P = \{a \in A \mid a : M \rightarrow M \text{ is nilpotent}\}$ , then  $P$  is a prime ideal of  $A$ .

*Proof.* For  $a, b \notin P$ ,  $a, b : M \rightarrow M$  are injective maps, so  $ab : M \rightarrow M$  is injective, hence  $ab \notin P$ . □

Hence, we usually say  $M$  is  $P$ -coprimary.

(iii) Let  $M$  be  $P$ -coprimary, then there exists an injection (as  $M$ -linear map)  $A/P \hookrightarrow M$ .

*Proof.* Take any  $x \neq 0$  in  $M$ , then consider

$$\begin{aligned} a_x : A &\rightarrow M \\ 1 &\mapsto x \end{aligned}$$

Let  $I = \ker(a_x)$ , then we have

$$\begin{aligned} A/I &\hookrightarrow M \\ \bar{1} &\mapsto x \end{aligned}$$

Now  $I \subseteq P$  since  $I$  already kills  $x$ . Since  $A$  is Noetherian,  $P$  is finitely-generated, thus consider  $P = (a_1, \dots, a_r)$ , then  $a_i^{t_i} \cdot x = 0$  for all  $i$  and some  $t_i$ 's. Let  $t = t_1 + \dots + t_r$ , then  $P^t \cdot x = 0$  by binomial theorem, so  $P^t \subseteq I \subseteq P$ , hence there exists  $j$  such that  $P^j \subseteq I \subsetneq P^{j-1}$ . Take  $y \in P^{j-1} \setminus I$ , so  $\bar{y} \neq 0$  in  $A/P$ , taking the injection into  $M$ , then  $\text{Ann}_A(\bar{y}) = P$ . We now have the composition

$$\begin{aligned} A/P &\hookrightarrow A/I \hookrightarrow M \\ \bar{1} &\mapsto \bar{y} \end{aligned}$$

to be injective. □

(iv) Suppose  $M$  is  $P$ -coprimary, and  $Q$  is a prime ideal such that  $A/Q \hookrightarrow M$ , then  $P = Q$ .

*Proof.* By definition of  $P$ ,  $Q \subseteq P$  is obvious:  $Q$  kills elements in  $M$ , therefore the mapping becomes nilpotent. The other direction is also easy. □

**Definition 1.3** (Primary). Let  $N \subseteq M$  be a submodule. We say  $N$  is a primary submodule of  $M$  if  $M/N$  is coprimary. If  $M/N$  is  $P$ -coprimary, we say  $N$  is  $P$ -primary.

**Remark 1.4.** Let  $\mathfrak{p}$  be a prime ideal of  $A$ . We claim that  $\mathfrak{p}^t$  is  $P$ -primary. Consider

$$m_x : A/\mathfrak{p}^t \rightarrow A/\mathfrak{p}^t$$

then  $x^t = 0$  on  $A/\mathfrak{p}^t$ .

**Example 1.5.** Let  $A = k[X, Y, Z]/(Z^2 - XY)$ , let  $\mathfrak{p} = (x, z)$  where  $x = \text{im}(X)$  and  $z = \text{im}(Z)$ . Now  $A/\mathfrak{p} = k[Y]$ .  $\mathfrak{p}^2$  is not  $P$ -primary. Indeed, note that  $A/\mathfrak{p}^2 = k[X, Y, Z]/(z^2 - xy, x^2, z^2) \cong k[X, Y, Z]/(X^2, XY, Z^2, XZ)$ . Now the mapping given by multiplication by  $y$  on this map is not injective, so  $\mathfrak{p}^2$  is not  $P$ -primary.

In particular, the represented surface is not smooth, since the origin  $(0, 0, 0)$  is a singularity.



**Theorem 1.6** (Primary Decomposition Theorem). By assumption,  $A$  is Noetherian and  $M$  is finitely-generated. Let  $N \subseteq M$  be a submodule, then there exists a decomposition

$$N = \bigcap_{i=1}^r N_i$$

where each  $N_i$  is  $P_i$ -primary, and such that

1. all  $P_i$ 's are distinct, and
2. this decomposition is irredundant, i.e., minimal. In particular, this means removing any of the  $N_i$ 's gives a different intersection, i.e.,  $\bigcap_{j \neq i} N_j \not\subseteq N_i$ .

This is called a primary decomposition of  $N$ . Moreover, the primary decomposition is unique up to permutation of modules, that is, if there exists another primary decomposition, i.e.,  $N = \bigcap_{i=1}^s N'_i$  where  $N'_i$ 's are  $P'_i$ -primary, then  $r = s$  and  $\{N_1, \dots, N_r\} = \{N'_1, \dots, N'_s\}$ .

*Proof.*

**Definition 1.7** (Irreducible). A submodule  $T \subsetneq M$  is called irreducible if  $T \neq T_1 \cap T_2$ , where  $T_1, T_2$  are distinct proper submodules of  $M$ .

**Claim 1.8.** Every submodule  $T$  of  $M$  can be expressed by  $T = T_1 \cap \dots \cap T_l$  where each  $T_i$  is irreducible.

*Subproof.* Suppose, towards contradiction, that there exists some  $T$  for which the claim fails, then the set of all such submodules  $T$  is a non-empty set  $\mathcal{T}$ . Since  $M$  is Noetherian, then  $\mathcal{T}$  has a maximal element  $W$ , therefore  $W$  is not irreducible. By definition,  $W = W_1 \cap W_2$  where  $W_1, W_2$  are distinct proper submodules of  $M$ , so  $W_1 \notin \mathcal{T}$  and  $W_2 \notin \mathcal{T}$ , therefore  $W_1 = T_1 \cap \dots \cap T_r$  for irreducible  $T_i$ 's, and  $W_2 = T'_1 \cap \dots \cap T'_s$  where  $T'_i$  are irreducible. Therefore,  $W$  becomes an intersection of irreducible submodules, a contradiction. ■

**Claim 1.9.** Suppose  $T$  is irreducible in  $M$ , then  $T$  is a primary submodule of  $M$ . That is, we need to show  $\bar{M} := M/T$  is coprimary.

*Subproof.* It suffices to show the following: for all  $a \neq 0$  in  $A$ , the multiplication map  $a : \bar{M} \rightarrow \bar{M}$  is either nilpotent or injective. Note that  $(0)$  in  $\bar{M}$  is irreducible. To see this, we take the ascending chain

$$\ker(a) \subseteq \ker(a^2) \subseteq \ker(a^3) \subseteq \dots$$

and since  $A$  is Noetherian we know  $\ker(a^n) = \ker(a^{n+1}) = \dots$  for some large enough  $n$ , therefore for  $g = a^n$  we know  $\ker(g) = \ker(g^2)$ .

**Claim 1.10.**  $\ker(g) \cap \text{im}(g) = (0)$  in  $\bar{M}$ .

*Subproof of Subclaim.* Let  $x \in \ker(g) \cap \text{im}(g)$ , then  $g(x) = 0$ , and there exists  $y \in \bar{M}$  such that  $x = g(y)$ , so  $0 = g(x) = g^2(y)$ , but that means  $y \in \ker(g^2) = \ker(g)$ , so  $x = 0$ . ■

Therefore,  $(0)$  is irreducible in  $\bar{M}$ , so either  $\ker(g) = (0)$  or  $\ker(g) = \bar{M}$ . If  $\ker(g) = (0)$ , we have  $g$  to be injective, hence multiplication by  $a$  is injective; if  $\ker(g) = \bar{M}$ , we have  $a^n \bar{M} = 0$ , so  $a$  becomes nilpotent. ■

**Claim 1.11.** If  $N_1$  and  $N_2$  are both  $P$ -primary as submodules, then  $N_1 \cap N_2$  is also  $P$ -primary.

*Subproof.* By definition,  $M/N_1$  and  $M/N_2$  are both  $P$ -coprimary, then it is easy to see that  $M/N_1 \oplus M/N_2$  is also  $P$ -coprimary. We know there is an obvious inclusion

$$\begin{aligned} M/(N_1 \cap N_2) &\hookrightarrow M/N_1 \oplus M/N_2 \\ \bar{x} &\mapsto (\bar{x}, \bar{x}) \end{aligned}$$

so  $M/(N_1 \cap N_2)$  is also coprimary by the inclusion, therefore  $N_1 \cap N_2$  is  $P$ -primary. ■

Now by [Claim 1.8](#) we have an irreducible decomposition  $N = N_1 \cap \cdots \cap N_r$  and without loss of generality let it be of the smallest length, that is, the  $N_i$ 's are irreducible modules that are irredundant. By [Claim 1.9](#), we know each of the  $N_i$ 's is primary with respect to some prime ideal. Now for any two  $P$ -primary modules  $N_i$  and  $N_j$ , we know the intersection is still  $P$ -primary according to [Claim 1.11](#), therefore we obtain an irredundant intersection  $N = N'_1 \cap \cdots \cap N'_s$  where each  $N'_i$  is  $P_i$ -primary (where  $P_i$ 's are now distinct!), and this proves the existence.

For the uniqueness, suppose we have  $N = N_1 \cap \cdots \cap N_r$  where  $N_i$  is  $P_i$ -primary, where  $P_i$ 's are distinct, and suppose we have  $N = N'_1 \cap \cdots \cap N'_s$  where  $N'_i$  is  $P'_i$ -primary, where all  $P'_i$  are distinct as well. It is enough to show the following:

**Claim 1.12.** For any prime ideal  $p$  of  $A$ ,  $p \in \{P_1, \dots, P_r\}$  if and only if there exists an injection  $A/p \hookrightarrow M/N$ .

*Subproof.* Let  $p \in \{P_1, \dots, P_r\}$ , without loss of generality denote  $p = P_1$ , then we have an injection  $A/p \hookrightarrow M/N_1$  by [Remark 1.2](#). In  $\bar{M} = M/N$ , we have  $(0) = N_1/N \cap \cdots \cap N_r/N =: \bar{N}_1 \cap \cdots \cap \bar{N}_r$ , therefore  $\bar{N}_2 \cap \cdots \cap \bar{N}_r \hookrightarrow \bar{M}/\bar{N}_1 = M/N_1$ . But  $M/N_1 = \bar{M}/\bar{N}_1$ , so this gives an injection  $\bar{N}_2 \cap \cdots \cap \bar{N}_r \hookrightarrow M/N_1$ , but  $M/N_1$  is  $P_1$ -coprimary, so  $\bar{N}_2 \cap \cdots \cap \bar{N}_r$  is also  $P_1$ -coprimary, therefore  $A/P_1 \hookrightarrow \bar{N}_2 \cap \cdots \cap \bar{N}_r \hookrightarrow \bar{M} = M/N$  by [Remark 1.2](#).

Now suppose  $A/p \hookrightarrow M/N$ , to show  $p \in \{P_1, \dots, P_r\}$ , it suffices to show  $A/p \hookrightarrow M/N_i$  is injective for some  $1 \leq i \leq r$ . We have

$$\begin{array}{c} \varphi_i \\ \curvearrowright \\ A/p \xrightarrow{\varphi} M/N = \bar{M} \xrightarrow{\eta_i} \bar{M}/\bar{N}_i = M/N_i \end{array}$$

and we want to show there exists some injective  $\varphi_i$ . Suppose not, then  $\ker(\varphi_i) \neq 0$  in  $A/p$  for all  $1 \leq i \leq r$ . But  $A/p$  is an integral domain, therefore  $\bigcap_{i=1}^r \ker(\varphi_i) \neq 0$ . Therefore, we have

$$A/p \xrightarrow{\varphi} M/N \xrightarrow{(\eta_1, \dots, \eta_r)} \bigoplus_{i=1}^r M/N_i$$

Thus, the defined composition above is the injection  $(\varphi_1, \dots, \varphi_r)$ . This implies  $\bigcap_{i=1}^r \ker(\varphi_i) = \ker(\varphi_1, \dots, \varphi_r) = 0$ , a contradiction. Thus, there exists some injective  $\varphi_i$ , and therefore  $p \in \{P_1, \dots, P_r\}$ . ■

□

**Definition 1.13** (Zero-divisor). Let  $A$  be Noetherian and  $M$  be a finitely-generated  $A$ -module. We say  $0 \neq a \in A$  is a zero-divisor on  $M$  if there exists  $0 \neq x \in M$  such that  $ax = 0$ . Otherwise, we say  $a$  is a non-zero-divisor on  $M$ .

**Definition 1.14** (Essential prime ideal, Associated prime ideal). Given a primary decomposition  $N = \bigcap_{i=1}^r N_i$ , the corresponding prime ideals  $\{P_1, \dots, P_r\}$  are called the essential prime ideals of  $N$ . In particular, if  $N = (0)$ , we say these are the associated prime ideals of  $M$ , denoted by  $\text{Ass}_A(M) = \{P_1, \dots, P_r\}$ .

**Corollary 1.15.** Let  $A$  be Noetherian and  $M$  be a finitely-generated  $A$ -module, and let  $\text{Ass}_A(M) = \{P_1, \dots, P_r\}$ , then  $\bigcup_{i=1}^r P_i$  is the set of all zero-divisors on  $M$ .

*Proof.* If  $p \in \text{Ass}_A(M)$ , then there exists an injection  $A/p \hookrightarrow M$  mapping  $\bar{1} \mapsto x$  by [Claim 1.12](#). Therefore,  $px = 0$ , so elements of  $p$  are zero-divisors of  $M$ . Let  $a$  be a zero-divisor on  $M$ , i.e., let  $0 \neq x \in M$  be such that  $ax = 0$ . Take the primary decomposition  $(0) = N_1 \cap \cdots \cap N_r$  in  $M$ , where  $N_i$  is  $P_i$ -primary, then there exists  $i$  such that  $x \notin N_i$ . Since  $\bar{x} \neq 0$  in  $M/N_i$ , then  $a : M/N_i \rightarrow M/N_i$  is such that  $a\bar{x} = 0$ , so  $a$  is nilpotent on  $M/N_i$ . Therefore,  $M/N_i$  is  $P_i$ -coprimary, and by definition  $a \in P_i$ . □

**Exercise 1.16.** Let  $\text{Ass}_A(M) = \{P_1, \dots, P_r\}$ , then the set of all nilpotent elements of  $M$  is  $\bigcap_{i=1}^r P_i$ .

**Corollary 1.17.** Suppose  $N \subseteq M$  is a submodule, then

$$\text{Ass}_A(N) \subseteq \text{Ass}_A(M) \subseteq \text{Ass}_A(N) \cup \text{Ass}_A(M/N).$$

*Proof.* The first inclusion is obvious by  $A/p \hookrightarrow N \hookrightarrow M$ . We now show the second inclusion. Let  $p \in \text{Ass}_A(M)$ , and suppose  $p \notin \text{Ass}_A(N)$ , and we have an inclusion  $i : A/p \rightarrow M$ .

**Claim 1.18.**  $i(A/p) \cap N = (0)$ .

*Subproof.* Suppose not, then let  $0 \neq x \in i(A/p) \cap N$ , then  $x \in N$  and  $x \in i(A/p)$ , but  $A/p$  is an integral domain and is  $p$ -coprimary, so  $i(A/p) \cap N$  is  $p$ -coprimary. Therefore, we have

$$A/p \hookrightarrow i(A/p) \cap N \hookrightarrow N$$

and so  $p \in \text{Ass}_A(N)$ , a contradiction. ■

Therefore, we have the composition  $A/p \rightarrow M \rightarrow M/N$  to be injection, thus  $p \in \text{Ass}_A(M/N)$ . □

**Corollary 1.19.** Let  $M$  be finitely-generated, and let  $I = \text{Ann}_A(M)$ , then the essential prime ideals of  $I$  is an associated prime of  $M$ .

*Proof.* Note that the essential prime ideals of  $I$  are just  $\text{Ass}_A(A/I)$ , so if we write  $I = I_1 \cap \cdots \cap I_r$  where  $I_i$  is a  $P_i$ -primary. Therefore, we have  $A/I = \bar{I}_1 \cap \cdots \cap \bar{I}_r$ , where  $\bar{I}_i = I_i/I$ , and  $\bar{I}_i$  is  $P_i$ -primary.

Now let  $M = \langle \alpha_1, \dots, \alpha_n \rangle$  be given by a set of generators, so  $M = \{\sum a_i \alpha_i \mid a_i \in A\}$ , now we look at the map

$$\begin{aligned} \varphi : A &\rightarrow \bigoplus_{i=1}^n M \\ 1 &\mapsto (\alpha_1, \dots, \alpha_n) \end{aligned}$$

then the kernel  $\ker(\varphi) = I$ , so  $\bar{\varphi} : A/I \hookrightarrow \bigoplus_{i=1}^n M$  is an injection. By [Corollary 1.17](#),  $\text{Ass}_A(M_1 \oplus M_2) = \text{Ass}_A(M_1) \cup \text{Ass}_A(M_2)$ , hence we know

$$\text{Ass}(A/I) \subseteq \bigcup_{i=1}^n \text{Ass}_A(M) = \text{Ass}_A(M).$$

□

**Definition 1.20** (Support). The support of  $M$  over  $A$ , denoted  $\text{Supp}_A(M)$ , is the set  $\{P \mid P \text{ prime ideal such that } P \supseteq I = \text{Ann}_A(M)\}$ .

**Theorem 1.21** (Prime Filtration). Let  $M$  be finitely-generated, then we have a descending chain

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_{n-1} \supseteq M_n = (0)$$

of prime ideals such that  $M_i/M_{i+1} \cong A/P_{i+1}$ ,  $0 \leq i \leq n-1$ , where  $P_i$ 's are prime ideals of  $A$ , and  $\text{Ass}_A(M) \subseteq \{P_1, \dots, P_n\}$ .

*Proof.* Note that  $P \in \text{Ass}_A(M)$  if and only if  $i : A/P \hookrightarrow M$ , therefore  $i(A/P)$  satisfies the condition stated in the theorem. Therefore, take  $\mathcal{A} = \{N \subseteq M \mid N \text{ satisfies the condition of the theorem}\}$ . Since  $A$  is Noetherian, we take a maximal element  $T$  of  $\mathcal{A}$ .

**Claim 1.22.**  $T = M$ .

*Subproof.* Suppose, towards contradiction, that  $T \neq M$ , then we have a short exact sequence

$$0 \longrightarrow T \longrightarrow M \longrightarrow M/T \longrightarrow 0$$

such that  $M/T \neq (0)$ .

**Exercise 1.23.** Let  $L$  be a finitely-generated  $A$ -module, then  $L = 0$  if and only if  $\text{Ass}_A(L) = \emptyset$ .

Let  $q \in \text{Ass}_A(M/T)$ , then we have

$$\begin{array}{ccccccc} & & & & A/q & & \\ & & & & \downarrow j & & \\ 0 & \longrightarrow & T & \longrightarrow & M & \xrightarrow{\eta} & M/T \longrightarrow 0 \end{array}$$

and take  $W = \eta^{-1}(j(A/q))$ , so we have a new short exact sequence

$$0 \longrightarrow T \longrightarrow W \longrightarrow j(A/q) \cong A/q \longrightarrow 0$$

Thus,  $W \supsetneq T$  satisfies the condition in the theorem. By the maximality of  $T$ , we have a contradiction. ■

□

**Remark 1.24.** Let  $A$  be Noetherian and  $\mathfrak{m} \subseteq A$  be a maximal ideal, then for any ideal  $I \subseteq A$  such that there exists  $n$  with  $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$ , then  $I$  is  $\mathfrak{m}$ -primary.

*Proof.* Consider the map

$$A/I \xrightarrow{\cdot x^n} A/I$$

for  $x \in \mathfrak{m}$ , then this is the zero map. Therefore, multiplication by  $x$  is nilpotent. Now suppose  $x \notin \mathfrak{m}$ , then we want to show that  $A/I \xrightarrow{\cdot x} A/I$  is injective. Indeed, since  $x \notin \mathfrak{m}$ , then  $\mathfrak{m} + Ax = A$ , hence we have that  $y + ax = 1$  for some  $y \in \mathfrak{m}$  and  $a \in A$ , so  $(y + ax)^n = 1$ ,  $y^n + \mu x = 1$ , but that means the map  $A/I \rightarrow A/I$  is given by multiplication by  $\mu x$ , so  $\bar{\mu}\bar{x} = \bar{1}$  since  $y$  vanishes. That is,  $\bar{x}$  is invertible over  $A/I$ , hence multiplication by  $x$  is an isomorphism. □

**Exercise 1.25.** Let  $A$  be a ring and  $S$  be a multiplicatively closed subset of  $A$ , and let  $M$  be an  $A$ -module, then  $S^{-1}M$  is an  $S^{-1}A$ -module. Let  $T \subseteq S^{-1}M$  be an  $S^{-1}A$ -submodule, then there exists  $N \subseteq M$  such that  $T = S^{-1}N$ .

**Remark 1.26.** Localization functor is fully faithful.

**Remark 1.27.** Let  $A$  be Noetherian and  $S$  be a multiplicatively closed subset of  $A$ .

1. Let  $M$  be  $P$ -coprimary, then
  - if  $S \cap P = \emptyset$ , then  $S^{-1}M$  is  $S^{-1}P$ -coprimary;
  - if  $S \cap P \neq \emptyset$ , then  $S^{-1}M = 0$ .

*Proof.* Indeed, suppose  $S \cap P \neq \emptyset$ , let  $a : M \rightarrow M$  be the multiplication map by  $a$ , so  $a \in P$  gives  $a^n M = 0$  for some  $n$ , and if  $a \notin P$ , then this is injective. Let  $\frac{a}{s} : S^{-1}M \rightarrow S^{-1}M$  be the multiplication map, but  $\frac{a}{s}$  is a unit, so multiplication by  $s$  or  $\frac{1}{s}$  is an isomorphism, hence we can take this to be  $\frac{a}{1}$  with  $s = 1$ . If  $s \in P$ , then  $s^n : M \rightarrow M$  is the zero map, therefore  $s^n : S^{-1}M \rightarrow S^{-1}M$  is also the zero map, so  $s$  is a unit. This only happens if  $S^{-1}M = 0$ . □

2. Let  $N$  be  $P$ -primary, then
  - if  $S \cap P = \emptyset$ , then  $S^{-1}N$  is  $S^{-1}P$ -primary in  $S^{-1}M$ ;
  - if  $S \cap P \neq \emptyset$ , then  $S^{-1}N = S^{-1}M$ .

**Remark 1.28.** Consider the localization  $S^{-1}M$ . Take a submodule  $T$  of  $S^{-1}M$ , then by [Exercise 1.25](#),  $T = S^{-1}N$  for some  $N \subseteq M$ . There is now a primary decomposition on  $N$  given by  $N = N_1 \cap \cdots \cap N_t$  where  $N_i$  is  $P_i$ -primary.

**Exercise 1.29.** Let  $W_1, W_2 \subseteq M$ , then  $S^{-1}(W_1 \cap W_2) = S^{-1}(W_1) \cap S^{-1}(W_2)$  in  $S^{-1}M$ .

**Remark 1.30.** This is true whenever we have a flat ring extension.

Therefore, we have

$$\begin{aligned} T &= S^{-1}N \\ &= S^{-1}N_1 \cap \cdots \cap S^{-1}N_t \\ &= S^{-1}N_{i_1} \cap \cdots \cap S^{-1}N_{i_r} \end{aligned}$$

where  $S^{-1}N_{i_j}$  is  $S^{-1}P_{i_j}$ -primary, and  $P_{i_1}, \dots, P_{i_r}$  are prime ideals for which  $S \cap P_j = \emptyset$ , where  $P_j \in \{P_1, \dots, P_t\}$ .

**Exercise 1.31.** Let  $N$  be  $P$ -primary in  $M$ .

- if  $S \cap P = \emptyset$ , then  $i_M : M \rightarrow S^{-1}M$  and  $i_N : N \rightarrow S^{-1}N$  gives  $i_M^{-1}(S^{-1}N) = N$ ;
- if  $S \cap P \neq \emptyset$ , then  $i_M^{-1}(S^{-1}N) = i_M^{-1}(S^{-1}M) = M$ .

**Corollary 1.32.** Consider a primary decomposition  $N = N_1 \cap \cdots \cap N_t$  where  $N_i$  is  $P_i$ -primary. Suppose we have a different primary decomposition  $N = N'_1 \cap \cdots \cap N'_t$  where  $N'_i$  is also  $P_i$ -primary. Suppose  $P_1$  is a minimal element in  $\{P_1, \dots, P_t\}$ , then  $N_1 = N'_1$ .

*Proof.* Let  $S = A \setminus P_1$ , then  $S^{-1}N = S^{-1}N_1 = S^{-1}N'_1$ . Now consider  $i_M : M \rightarrow S^{-1}M$ , this descends to  $N_1 \rightarrow S^{-1}N_1 = S^{-1}N'_1$  and  $N'_1 \rightarrow S^{-1}N'_1$ , so  $i_M^{-1}(S^{-1}N_1 = S^{-1}N'_1) = N_1 = N'_1$ .  $\square$

Consider flat ring maps (as a ring extension) like  $A \rightarrow A[x]$  and  $A \rightarrow A[x_1, \dots, x_n]$  since as  $A$ -modules they are free, since we have a basis  $\{x_1^{i_1}, \dots, x_n^{i_n}\}$ .

**Lemma 1.33.** Let  $A \rightarrow B$  be a flat map, and let  $M$  be an  $A$ -module. Let  $N_1$  and  $N_2$  be  $A$ -submodules of  $M$ , then  $(N_1 \otimes_A B) \cap (N_2 \otimes_A B) = (N_1 \cap N_2) \otimes_A B$ .

*Proof.* Consider the chain complex

$$\begin{array}{ccccccc} & & 0 & & 0 & & 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & N_1 \cap N_2 & \longrightarrow & N_1 & \longrightarrow & N_1/(N_1 \cap N_2) \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & N_2 & \longrightarrow & M & \longrightarrow & M/N_2 \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & N_2/(N_1 \cap N_2) & \longrightarrow & M/N_1 & \longrightarrow & M/(N_1 + N_2) \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & 0 & & 0 & & 0 \end{array}$$

with exact rows and columns. We tensor this complex by  $- \otimes_A B$ , then since  $B$  is flat we obtain a new chain complex

$$\begin{array}{ccccccc} & & 0 & & 0 & & 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & (N_1 \cap N_2) \otimes_A B & \longrightarrow & N_1 \otimes_A B & \longrightarrow & (N_1/(N_1 \cap N_2)) \otimes_A B \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & N_2 \otimes_A B & \longrightarrow & M \otimes_A B & \longrightarrow & M/N_2 \otimes_A B \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & N_2/(N_1 \cap N_2) \otimes_A B & \longrightarrow & M/N_1 \otimes_A B & \longrightarrow & (M/(N_1 + N_2)) \otimes_A B \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & 0 & & 0 & & 0 \end{array}$$

Via diagram chasing, if  $x \in (N_1 \otimes_A B) \cap (N_2 \otimes_A B)$ , then  $x \in (N_1 \cap N_2) \otimes_A B$ .  $\square$

**Corollary 1.34.** Suppose we have a primary decomposition  $N = N_1 \cap \cdots \cap N_t$  in  $M$ , let  $A \rightarrow A[x]$ , then  $N[x] = N_1[x] \cap \cdots \cap N_t[x]$  in  $M[x]$  where  $N_i[x] = N_i \otimes_A A[x]$ .

*Proof.* We want to show that if  $N_i$  is  $P_i$ -primary, then  $N_i[x]$  is  $P_i[x]$ -primary. Take a short exact sequence

$$0 \longrightarrow P \longrightarrow A \longrightarrow A/p \longrightarrow 0$$

then we tensor it by  $-\otimes_A A[x]$ , then we obtain a new short exact sequence

$$0 \longrightarrow P \otimes_A A[x] \longrightarrow A[x] \longrightarrow A/p \otimes_A A[x] \longrightarrow 0$$

(Note that we are working over the commutative case, so the left tensor and the right tensor are canonically isomorphic.) We have  $B \otimes_A A[x] = B[x]$ , now we have  $A[x] \otimes_A A/p = A[x]/PA[x] = (A/p)[x]$  which is a domain, so  $PA[x]$  is a prime ideal. It now suffices to show that if  $M$  is  $P$ -coprimary, then  $M[x]$  is  $P[x]$ -coprimary. This simplifies to showing that:

- if  $f(x) \in P[x]$ , then the multiplication map  $M[x] \xrightarrow{f(x)} M[x]$  is nilpotent;
- if  $f(x) \notin P[x]$ ,  $M[x] \xrightarrow{f(x)} M[x]$  is an injection.

Note that  $M[x] = \sum_{i \geq 0} m_i x^i$  for some  $m_i$ 's. Since  $P[x]$  is a prime ideal, then  $A[x]/P[x] \cong A/p[x]$ . If  $f(x) \in P[x]$ , we have  $f(x) = p_0 + p_1 x + \cdots + p_t x^t$  for  $p_i$ 's in  $P$ . Consider the multiplication map via  $[f(x)]^p : M[x] \rightarrow M[x]$ , where  $n = n_0 + n_1 + \cdots + n_t$  such that  $p_i^{n_i} M = 0$  by the binomial theorem. Now suppose  $f(x) \notin P[x]$ , then let us write  $f(x) = a_0 + a_1 x + \cdots + a_t x^t$ , and we have two cases:

- if no  $a_i$ 's are in  $P$ , then for all  $i$ , multiplication by  $a_i$  on  $M$  is an injection. If we multiply  $f(x)$  by  $m_0 + m_1 x + \cdots$ , then the constant term would be  $a_0 m_0$ , and for each term to be zero, we must have  $f(x)$  equivalent to zero, hence that means multiplication by  $f(x)$  on  $M[x]$  would be injective as well.
- Now suppose there exists some  $a_i$  that is contained in  $P$ . We can write down  $f(x) = u + v$  where  $u$  has coefficients in  $P$  and  $v$  does not have any coefficients in  $P$ . If possible, let  $f(\alpha) = 0$  for  $\alpha \in M[x]$ , then we have  $u\alpha = -v\alpha$ , and so  $u^2\alpha = v^2\alpha$  since  $u^2\alpha = u(-v\alpha) = v(-u\alpha) = v^2\alpha$ , and by induction we have  $u^n\alpha = (-1)^n v^n\alpha$ . Therefore, for large enough  $n$  such that  $u^n\alpha = 0$ , we know  $v^n\alpha = 0$ , and therefore we have a contradiction since  $v$  does not contain any coefficients in  $P$ .

□

**Remark 1.35.** Remark 1.24 would fail if  $P$  is not a maximal ideal:  $P^2$  may not be  $P$ -primary in this case.

Let  $R$  be a Noetherian ring, we let  $i_P : R \rightarrow R_P$  be the localization away from  $P$ , from  $R$  to the local ring with maximal ideal  $PR_P$ , then we have  $(PR_P)^n = P^n R_P$  to be  $PR_P$ -primary. Therefore, this gives a mapping from  $P^n$  to  $P^n R_P = (PR_P)^n$ . We now denote  $P^{(n)} := i_P^{-1}(P^n R_P)$  to be the  $n$ th symbolic power of  $P$ , then  $P^{(n)}$  is  $P$ -primary. (Indeed, we note that  $P$  is disjoint from  $R \setminus P$ , so given  $M \rightarrow S^{-1}M$  pulling  $S^{-1}P$ -primary module  $S^{-1}N$  back to  $M$  gives a  $P$ -primary module.) In particular,  $P^{(n)} \supseteq P^n$ .<sup>2</sup>

**Exercise 1.36.** 1. • Let  $R$  be Noetherian and  $M$  be finitely-generated. Show that  $\ell_R(M) < \infty$  if and only if  $\text{Ass}_R(M)$  consists of maximal ideals only.

- If  $\ell_A(M) < \infty$ , then  $M$  is a direct sum of coprimary submodules of  $M$ .

Moreover,  $M$  is a direct sum of  $P$ -coprimary submodules where  $P$  runs through  $\text{Ass}_A(M)$ .

2. Now let  $R$  be a Noetherian ring and  $P$  be a prime ideal. Prove that the following are equivalent:

- $P$  is an essential prime ideal of some submodule  $N$  of  $M$ .
- $M_P \neq 0$ .

<sup>2</sup> $P^{(n)}$  is the unique  $P$ -primary component in the primary decomposition of  $P^n$ , and is the smallest  $P$ -primary ideal containing  $P^n$ . Therefore,  $P^{(n)} = P^n$  if and only if  $P^n$  is primary.

- (iii)  $P \supseteq \text{Ann}_R(M)$ .
  - (iv)  $P$  contains some  $Q \in \text{Ass}(M)$ .
3. Let  $R = k[x, y, z]$  for some field  $k$ , and let  $P = (xz - y^2, x^3 - yz, z^2 - x^2y)$ .
- Prove that  $P$  is a prime ideal of  $R$ .
  - Is  $P^2$   $P$ -primary?

*Hint:* consider

$$\begin{aligned} \varphi : k[x, y, z] &\rightarrow k[t] \\ x &\mapsto t^3 \\ y &\mapsto t^4 \\ z &\mapsto t^5 \end{aligned}$$

and show that  $\ker(\varphi) = P$ .

## 1.2 INFINITELY-GENERATED CASE

Now let  $R$  be a Noetherian ring, and  $M$  is not finitely-generated.

**Definition 1.37** (Coprimary).  $M$  is called coprimary if for any  $a \in R$ , we have multiplication map  $a : M \rightarrow M$  to be either injective, or locally nilpotent, i.e., for all  $x \in M$ , there exists  $n_x$  such that  $a^{n_x}x = 0$ .

Therefore, any submodule of  $M$  is coprimary. Now we define the associated primes to be  $\text{Ass}_R(M)$  to be the set of prime ideals in  $R$  such that there exists an injection  $A/p \hookrightarrow M$ , i.e.,  $R/p$  is a cyclic submodule of  $M$ .

**Theorem 1.38.** Let  $R$  and  $M$  be as above. For any  $P \in \text{Ass}_R(M)$ , there exists a  $P$ -primary submodule  $N(P)$  of  $M$  such that  $(0) = \bigcap_{P \in \text{Ass}_R(M)} N(P)$ , which may be infinite.

**Example 1.39.** Let  $A$  and  $B$  be Noetherian rings and  $M$  be a finitely-generated  $A$ -module, and we say have a ring homomorphism  $\varphi : B \rightarrow A$ . Via the pullback over  $\varphi$ , we make  $M$  into a  $B$ -module, but  $M$  may not be finitely-generated as a  $B$ -module. For instance, take  $A = \mathbb{Z}$  and  $B = \mathbb{Z}[x]$ .

**Exercise 1.40.** Let  $\varphi : B \rightarrow A$  be a homomorphism of Noetherian rings. If  $M$  is a finitely-generated  $A$ -module, then via the pullback of  $\varphi$ ,  $M$  is a  $B$ -module. We write it as  ${}_{\varphi}M$ . Prove that  $\text{Ass}_A({}_{\varphi}M) = \varphi^{-1}(\text{Ass}_A(M))$ .

## 2 FILTERED RINGS AND MODULES, COMPLETIONS

**Definition 2.1** (Topological Ring). Let  $R$  be a ring with addition  $\varphi$  and multiplication  $\psi$ . Suppose  $R$  has a topology such that  $\varphi$  and  $\psi$  are continuous, then we say  $R$  is a topological ring with respect to the given topology. That is, the topology respects the algebraic structure.

Similarly, we can define a topological group with respect to multiplication and inverse, and a topological module with respect to addition and scalar multiplication.

**Remark 2.2.** A topological ring  $R$  (respectively, topological group  $G$ , topological module  $M$ ) is Hausdorff if and only if  $(0)$  is closed in  $R$  (respectively,  $(e)$  is closed in  $G$ ,  $(0)$  is closed in  $M$ ).

Let  $M$  be a topological module, consider

$$\begin{aligned}\varphi : M \times M &\rightarrow M \\ (x, y) &\mapsto x - y\end{aligned}$$

then the diagonal is given by  $\varphi^{-1}(0) = \{(x, x) \mid x \in M\} = \Delta_M$ . Now suppose  $(0)$  is closed, which gives  $\Delta_M$  to be closed, hence  $M$  is Hausdorff.

**Definition 2.3** (Pseudo-metric Space). We say  $(X, d)$  is a pseudo-metric space if we have a function  $d : X \times X \rightarrow \mathbb{R}^{\geq 0}$  such that

1.  $d(x, y) + d(y, z) \geq d(x, z)$ ,
2.  $d(x, y) = d(y, x)$ ,
3.  $d(x, x) = 0$ .

This becomes a metric space if  $d(x, y) = 0$  if and only if  $x = y$ .

**Remark 2.4.** A pseudo-metric space is a Hausdorff if and only if it is a metric space.

**Definition 2.5** (Completion). Let  $(X, d)$  be a (pseudo-)metric space, then the completion  $(\hat{X}, \hat{d})$  of  $(X, d)$  is a complete (all Cauchy sequences converge) metric space  $\hat{X}$  with a metric  $\hat{d}$  with a map  $\varphi : X \rightarrow \hat{X}$  such that

1.  $\varphi$  respects both  $d$  and  $\hat{d}$ ,
2.  $\varphi(X)$  is dense in  $\hat{X}$ , and
3. We have

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & \hat{X} \\ & \searrow \psi & \swarrow \theta \\ & Y & \end{array}$$

that is, given any complete metric space  $Y$  and a continuous map  $\psi : X \rightarrow Y$ , there exists a unique map  $\theta : \hat{X} \rightarrow Y$  such that the diagram commutes.

**Remark 2.6.** If  $W \subseteq X$ , then  $\hat{W} \cong \overline{\varphi(W)}$ .

For what we care, a complete space is Hausdorff complete.

**Definition 2.7** (Directed Set). Let  $(I, \leq)$  be a poset, then  $I$  is called a directed set if for all pairs of  $\alpha, \beta \in I$ , there exists  $\gamma \in I$  such that  $\alpha \leq \gamma$  and  $\beta \leq \gamma$ .

**Definition 2.8** (Inverse Limit). We say  $\{X_\alpha\}_{\alpha \in I}$  is an inverse family indexed by  $I$  if for all  $\alpha \leq \beta$ , there exists maps  $\varphi_{\alpha, \beta} : X_\beta \rightarrow X_\alpha$  such that for all  $\alpha \leq \beta \leq \gamma$ , we have a commutative diagram

$$\begin{array}{ccc} X_\gamma & \xrightarrow{\varphi_{\alpha\gamma}} & X_\alpha \\ & \searrow \varphi_{\beta\gamma} & \swarrow \varphi_{\alpha\beta} \\ & X_\beta & \end{array}$$



An inverse limit of  $\{X_\alpha\}_{\alpha \in I}$  is an object  $X$  with maps  $\varphi_\alpha : X \rightarrow X_\alpha$  for all  $\alpha \in I$  such that the diagram

$$\begin{array}{ccc} X & \xrightarrow{\varphi_\alpha} & X_\alpha \\ & \searrow \varphi_\beta & \nearrow \varphi_{\alpha\beta} \\ & X_\beta & \end{array}$$

commutes for all  $\alpha, \beta \in I$ , and for all  $Y$  such that the diagram

$$\begin{array}{ccc} Y & \xrightarrow{\psi_\alpha} & X_\alpha \\ & \searrow \psi_\beta & \nearrow \varphi_{\alpha\beta} \\ & X_\beta & \end{array}$$

commutes for all  $\alpha, \beta \in I$ , then there exists  $f : Y \rightarrow X$  such that

$$\begin{array}{ccc} Y & \xrightarrow{f} & X \\ & \searrow \psi_\alpha & \nearrow \varphi_\alpha \\ & X_\beta & \end{array}$$

commutes for all  $\alpha$ .

**Remark 2.9.** To construct such inverse limits, we take  $\tilde{X} = \prod_{\alpha \in I} X_\alpha$ , then we have an embedding  $X \hookrightarrow \tilde{X}$  where

$$X = \left\{ \prod_{\alpha \in I} X_\alpha \mid \forall \alpha \leq \beta, \varphi_\alpha(X_\beta) = X_\alpha \right\}.$$

We denote the inverse limit to be  $X = \varprojlim X_\alpha$ .

**Exercise 2.10.** Consider  $X_0 \supseteq X_1 \supseteq \cdots \supseteq X_n \supseteq \cdots$ , then the inverse limit  $\varprojlim X_n = \bigcap_{n \geq 0} X_n$ .

**Exercise 2.11.** Let  $A$  be a commutative ring, and consider  $A[x]$  or  $A[x_1, \dots, x_n]$ . Let  $I = (x)$ , or respectively the maximal ideal  $(x_1, \dots, x_n)$ . Then we have a map  $\cdots \rightarrow A[x]/I^{n+1} \rightarrow A[x]/I^n \rightarrow A[x]/I^{n-1} \rightarrow \cdots \rightarrow A[x]/I$ , so  $\varprojlim A[x]/I^n \cong A[[x]]$ .

**Remark 2.12.** By Hilbert's theorem, we know if  $A$  is Noetherian, then so is  $A[x]$ ; similarly, if  $A$  is Noetherian, then so is  $A[[x]]$ .

**Definition 2.13** (Graded Ring). We say a commutative ring  $A$  is graded if  $A$  contains a sequence of  $\{A_n\}_{n \geq 1}$  of subgroups such that

- $A_i \cdot A_j \subseteq A_{i+j}$ ,
- $A = \bigoplus_{i \geq 0} A_i$ .

By definition, this implies  $A_0$  is a subring of  $A$ , and  $A_+ = \bigoplus_{i \geq 1} A_i$  is an ideal, usually called the irrelevant ideal.

**Exercise 2.14.** 1.  $1 \in A_0$ ,

2.  $A$  is Noetherian if and only if  $A_0$  is Noetherian and  $A_+$  is a finitely-generated ideal of  $A$ .

## 2.1 FILTRATIONS OF RINGS AND MODULES

Let  $A$  be a commutative ring, not necessarily Noetherian, and let  $M$  be an  $A$ -module.

**Definition 2.15** (Filtered Ring).  $A$  is called a filtered ring if it admits a filtration  $\{A_n\}_{n \geq 0}$  where  $A_i$ 's form a descending sequence of subgroups of  $A$ .

Since the descending chain satisfies  $A_i \cdot A_j \subseteq A_{i+j}$ , then each  $A_i$  for  $i > 0$  is an ideal of  $A$ . We now write  $A \sim \{A_n\}_{n \geq 0}$ , associating  $A$  with its filtration.

**Definition 2.16** (Filtered Module).  $M$  is called a filtered  $A$ -module if there exists a descending chain of subgroups  $M_0 \supseteq M_1 \supseteq \cdots$  of  $M$  such that  $A_i \cdot M_j \subseteq M_{i+j}$ .

This implies each  $M_j$  is an  $A$ -submodule.

**Example 2.17.** Let  $I$  be an ideal of  $A$ , and let  $A_n = I^n$ . Let  $M$  be an  $A$ -module, with  $M_n = I^n M$ . The associated filtrations are called the  $I$ -adic filtration of  $A$  and of  $M$ .

**Definition 2.18** (Induced Filtration, Image Filtration). Let  $A \sim \{A_n\}$  and  $M \sim \{M_n\}$ . Let  $N \subseteq M$  be a submodule. The induced filtration on  $N$  is given by  $N_n = N \cap M_n$  for all  $n$ .

Let  $f : M \rightarrow T$  be a surjective  $A$ -linear map of modules, then the filtration defined by  $T_n = f(M_n)$  is the image filtration of  $T$ .

**Definition 2.19** (Filtered Map, Strict Morphism). Let  $M \sim \{M_n\}$  and  $N \sim \{N_n\}$  be filtrations. A map  $f : M \rightarrow N$  is called a filtered map if for all  $n$ ,  $f(M_n) \subseteq N_n$ .

If  $f : M \rightarrow N$  is a filtered map, suppose  $f(M)$  has an induced filtration with  $f(M)_n = f(M) \cap N_n$ , as well as an image filtration of  $\{f(M_n)\}$ . We say  $f$  is a strict morphism if for any  $n$ ,  $f(M_n) = f(M) \cap N_n = f(M)_n$ . Note that by definition we have  $f(M_n) \subseteq f(M) \cap N_n$ .

## 2.2 TOPOLOGY AND METRIC ON FILTERED RINGS AND MODULES

**Definition 2.20** (Fundamental System). Let  $A \sim \{A_n\}$  and  $M \sim \{M_n\}$ . We declare  $\{A_n\}$  (respectively,  $\{M_n\}$ ) as a fundamental system of open neighborhoods of  $(0)$  in  $A$  (respectively,  $M$ ). For any  $x \in A$  (respectively,  $x \in M$ ),  $x + A_n$  (respectively,  $x + M_n$ ) form a fundamental system of neighborhoods of  $x$ . This presumption defines a topology on  $A$  corresponding to  $\{A_n\}$  (respectively,  $M$  corresponding to  $\{M_n\}$ ).

**Remark 2.21.**  $A$  is a topological ring and  $M$  is a topological  $A$ -module with respect to this filtration.

**Lemma 2.22.** Let  $M \sim \{M_n\}$  with  $N \subseteq M$ , and let  $\bar{N}$  be the closure of  $N$  in  $M$ , then this is just  $\bigcap_{n \geq 0} N + M_n$ .

*Proof.* Let  $x \in \bar{N}$ , then there exists  $n$  such that  $(x + M_n) \cap N \neq \emptyset$ . Therefore, there exists  $y_n \in M_n$  and  $z \in N$  such that  $x + y_n = z$ , therefore  $x = z - y_n \in N + M_n$  for all  $n$ . Conversely, let  $x \in \bigcap_{n \geq 0} N + M_n$ . When  $x \in N + M_n$ , then we can write  $x = z + y_n$  for  $z \in N$  and  $y_n \in M_n$ . Therefore,  $x - y_n = z$ , so  $(x + M_n) \cap N \neq \emptyset$ .  $\square$

**Corollary 2.23.**  $\overline{(0)} = \bigcap_{n \geq 0} M_n = \bigcap_{n \geq 0} A_n$ . Therefore,  $A$  (respectively,  $M$ ) is Hausdorff if and only if  $\bigcap_{n \geq 0} A_n = 0$  (respectively,  $\bigcap_{n \geq 0} M_n = 0$ ).

**Exercise 2.24.** Let  $f : M \rightarrow N$  be a filtered map, then  $f$  is continuous.

Let  $0 < c < 1$ .

If we assume  $A$  (or  $M$ ) is Hausdorff, i.e.,  $\bigcap_{n \geq 0} A_n = 0$  ( $\bigcap_{n \geq 0} M_n = 0$ ). Denote  $d(x, y) = c^n$ , where  $n$  is the largest integer such that  $x - y \in M_n$ .

If we assume  $A$  (or  $M$ ) is not Hausdorff, i.e.,  $\bigcap_{n \geq 0} A_n \neq 0$  ( $\bigcap_{n \geq 0} M_n \neq 0$ ). We can still define the notion of distance as above, but in addition we need: if  $x - y \in \bigcap_{n \geq 0} M_n$ , then  $d(x, y) = 0$ .

Recall that a sequence  $\{x_n\}$  is Cauchy if for any  $\varepsilon > 0$ , there exists  $N$  such that  $d(x_n, x_m) < \varepsilon$  for all  $n, m \geq N$ . Therefore, given by  $M_n$ , there exists  $N$  such that for all  $s, r \geq N$ , then  $x_r - x_s \in M_N$ . Note that it suffices to have  $x_{N+1} - x_N \in M_N$ , since by telescoping we get what we want over the additive structure of the module. Hence,  $\{x_n\}$  is Cauchy if and only if  $\{x_n - x_{n-1}\} \rightarrow 0$  as  $n \rightarrow \infty$ .

**Exercise 2.25.** Let  $M$  be a complete metric space with respect to  $\{M_n\}$ , then  $\{x_n\} \in M$  has a convergent sum  $\sum_{n \geq 0} x_n$  if and only if  $x_n \rightarrow 0$ .

**Theorem 2.26.** Let  $M \sim \{M_n\}$  be filtered and Hausdorff. Suppose  $M$  is complete with respect to  $\{M_n\}$ . Let  $N$  be a closed submodule of  $M$ , then  $\bar{M} = M/N$  with respect to the image filtration  $\{\bar{M}_n\}$  is also complete (Hausdorff).

*Proof.*  $\bar{M}$  is Hausdorff since  $N = \bar{N} = \bigcap_{n \geq 0} (N + M_n)$ . Consider  $\eta : M \rightarrow \bar{M}$ , then this is Hausdorff and we want to show this is complete. Let  $\{\bar{x}_n\}$  be a Cauchy sequence in  $\bar{M}$ , then  $\bar{x}_{n+1} - \bar{x}_n \in \bar{M}_{i(n)}$  for all  $n \geq N$ , for some  $i(n)$  corresponding to  $n$ . In particular,  $i(n) \rightarrow \infty$  as  $n \rightarrow \infty$ . Let  $x_i$  be the lift of  $\bar{x}_i$  in  $M$ , then we have  $x_{n+1} - x_n = y_n + z_n$  for some  $y_n \in M_{i(n)}$  and  $z_n \in N$ . By telescoping, we have  $x_n - x_1 = \sum_{i=1}^{n-1} y_i + \tilde{z}$  for some  $\tilde{z} \in N$ . But for  $n \rightarrow \infty$ , we have large enough  $i(n) \gg 0$ , therefore the sequence  $\{y_n\}$  satisfies  $y_n \in M_{i(n)}$ , therefore  $y_n \rightarrow 0$  for  $n \rightarrow \infty$ , thus the sequence  $\sum_{n=1}^{\infty} y_n$  converges. Hence, as  $n \rightarrow \infty$ , we have  $\lim_{n \rightarrow \infty} \bar{x}_n = \bar{x}_1 + \sum_{n=1}^{\infty} \bar{y}_n + \tilde{z} = \bar{x}_1 + \bar{y}$ .  $\square$

### 2.3 ( $I$ -ADIC) COMPLETION

**Definition 2.27** (Null Sequence, Completion). A Cauchy sequence  $\{x_n\}$  with  $x_n \rightarrow 0$  is called a null sequence.

Let  $M \sim \{M_n\}$  not necessarily be Hausdorff, then we obtain the completion  $\hat{M}$  of  $M$  with respect to  $\{M_n\}$  (or the metric defined on  $\{M_n\}$ ) by defining  $\hat{M}$  as the set of equivalence classes of all Cauchy sequences in  $M$ , over the submodules generated by null sequences.

**Remark 2.28.** Recall that we define the completion  $\hat{X}$  of a space  $X$  as the equivalence class of sets of all Cauchy sequences over the relation  $x = (x_n) \sim y = (y_n)$  if and only if  $d(x_n, y_n) \rightarrow 0$  as  $n \rightarrow \infty$ . In our case, we have  $\{x_n - y_n\}$  forming a null sequence.

Similarly, we can define the completion  $\hat{A}$  of a ring  $A$  to be the equivalence class of the sets of all Cauchy sequences over the ideal generated by the null sequences.

**Remark 2.29.**  $\hat{M}$  is a topological  $\hat{A}$ -module. In particular, if  $\{a_n\}$ 's define a Cauchy sequence in  $A$  and  $\{m_n\}$ 's define a Cauchy sequence in  $M$ , then  $\{a_n m_n\}$ 's define a Cauchy sequence in  $M$ .

The corresponding mapping is given by

$$\begin{aligned} i : M &\rightarrow \hat{M} \\ x &\mapsto \{x\}, \end{aligned}$$

that is, the image is the constant sequence defined by  $x_n = x$  for all  $n$ . Note that this is not necessarily injective. However,  $i(M)$  is dense in  $\hat{M}$ .

**Remark 2.30.** The completion  $\hat{M}$  of  $M$  satisfies the following property: given any complete space  $T$ , there is  $g : M \rightarrow T$  and  $f : \hat{M} \rightarrow T$  such that  $g = f \circ i$  is a commutative diagram. In particular, if  $\{x_n\}$  is Cauchy in  $M$ , then the image  $g(x_n)$  is Cauchy in  $T$ . If we define  $f(x = (x_n)) = y$ , then  $g(x_n) \rightarrow y$  in  $T$ .

Note that given any  $M_n$  in  $M$ , we have  $\overline{i(M_n)} = \hat{M}_n$ .

**Definition 2.31** (Hausdorffication). The quotient  $M/\ker(i)$  is called the Hausdorffication of  $M$ .

**Remark 2.32.** By Theorem 2.26,  $\hat{M}/\hat{M}_n$  is complete, then there is an induced mapping  $\bar{i}_n : M/M_n \rightarrow \hat{M}/\hat{M}_n$ . Now  $\text{im}(\bar{i}_n)$  is dense in  $\hat{M}/\hat{M}_n$ , then  $\overline{M/M_n} = \hat{M}/\hat{M}_n$ . Recall that  $M_n$  is defined to be open in  $M$  via the fundamental system, now cosets of  $M_n$  are of the form  $x + M_n \cong M_n$  with respect to a homeomorphism, hence  $M \setminus M_n$  is open, so  $M_n$  is also closed in  $M$ . Therefore,  $M/M_n$  is discrete, so  $\overline{(0)}$  is clopen, therefore  $M/M_n$  is complete, therefore  $M/M_n \cong \hat{M}/\hat{M}_n$ , i.e., isomorphic to the completion. In particular,  $i^{-1}(\hat{M}_n) = M_n$  (with  $M \cap \hat{M}_n = M_n$ ).

**Remark 2.33.**  $\bigcap \hat{M}_n = (0)$  and  $\{\hat{M}_n\}$  constitutes a fundamental system of open neighborhoods in  $\hat{M}$ .

**Definition 2.34.** Let  $A \sim \{A_n\}$  and  $M \sim \{M_n\}$ , with  $\bar{A} \sim \{\bar{A}_n\}$  and  $\bar{M} \sim \{\bar{M}_n\}$ . We define  $E_0(A) = A/A_1 \oplus A_1/A_2 \oplus \cdots \oplus A_n/A_{n+1} \oplus \cdots$  as a graded ring, and similarly we can define  $E_0(M)$ . This is called the graded ring (respectively, module) associated to the filtration.

**Remark 2.35.** In particular,  $E_0(M)$  is a graded  $E_0(A)$ -module. We have

$$\begin{aligned} A_i/A_{i+1} \times A_i/A_{j+1} &\rightarrow A_{i+j}/A_{i+j+1} \\ (\bar{\lambda}, \bar{\mu}) &\mapsto \overline{\lambda\mu} \end{aligned}$$

and

$$\begin{aligned} A_i/A_{i+1} \times M_i/M_{j+1} &\rightarrow M_{i+j}/M_{i+j+1} \\ (\bar{\lambda}, \bar{x}) &\mapsto \overline{\lambda x} \end{aligned}$$

We have  $E_0(A) \cong E_0(\hat{A})$  and  $E_0(M) \cong E_0(\hat{M})$  since  $A_i/A_{i+1} \cong \hat{A}_i/\hat{A}_{i+1}$  and  $M_i/M_{i+1} \cong \hat{M}_i/\hat{M}_{i+1}$ .

**Remark 2.36.** Note that  $k[x]$  has transcendental degree 1 over  $k$  and  $k[[x]]$  has infinite transcendental degree over  $k$ , but by Remark 2.35 we know

$$\bigoplus \frac{x^n \cdot k[x]}{x^{n+1} \cdot k[x]} \cong \bigoplus \frac{x^n \cdot k[[x]]}{x^{n+1} \cdot k[[x]]}.$$

**Definition 2.37** (Inverse Limit). Let  $A \sim \{A_n\}$  and  $M \sim \{M_n\}$ , then we can construct the completion of  $A$  (and similarly of  $M$ ) via inverse limit. We denote  $M^* = \varprojlim M/M_n = \{\prod \bar{x}_n : (\bar{x}_n) \in \prod M/M_n, \eta_{n+1}(\bar{x}_{n+1}) = \bar{x}_n \forall n\}$  associated with the directed system

$$\cdots \longrightarrow M/M_{n+1} \xrightarrow[\bar{x}_{n+1} \mapsto \bar{x}_n]{\eta_{n+1}} M/M_n \xrightarrow{\eta_n} M/M_{n-1} \longrightarrow \cdots$$

Therefore this is true if and only if  $x_{n+1} - x_n \in M_n$  for any  $n$ , so we obtain a Cauchy sequence as mentioned previously. Now  $M/M_n$  is discrete hence complete, therefore the associated topology  $\prod M/M_n$  of countable products is complete in the product topology. Therefore, since each  $M/M_n$  is a metric space, then the countable product is still a metric space  $\prod M/M_n$ .

**Exercise 2.38.** Show that  $M^*$  is a closed submodule of  $\prod M/M_n$ . In particular, since  $\prod M/M_n$  is complete, then  $M^*$  is also complete.

**Remark 2.39.** The associated map is

$$\begin{aligned} i : M &\rightarrow M^* \\ x &\mapsto (\bar{x}, \bar{x}, \bar{x}, \dots) \end{aligned}$$

and  $i(M)$  is dense in  $M^*$ . For any  $M_n$ , the image  $i(M_n) = (\bar{0}, \dots, \bar{0}, \bar{x}, \bar{x}, \dots)$  for some  $x \in M_n$  with the first  $n$  coordinates as 0. In general, we have the mapping

$$M^* \xleftarrow{j} \prod M/M_n \xrightarrow{\pi_n} M/M_n$$

and  $\overline{i(M_n)} = (\pi_n j)^{-1}(\bar{0}) = j^{-1} \pi_n^{-1}(\bar{0})$ . For any  $Z_n \in M/M_n$ , the preimage

$$\pi_n^{-1}(Z_n) = M/M_1 \times M/M_{n-1} \times Z_n \times M/M_{n+1} \times \cdots,$$

so

$$j^{-1}(\pi_n^{-1}(0)) = j^{-1}(M/M_1 \times M/M_{n-1} \times \bar{0} \times M/M_{n+1} \times \cdots) = \overline{j(M_n)} = M_n^*.$$

It now follows that  $\bigcap M_n^* = (0)$ .

**Remark 2.40.** We now have the following universal property: for any  $M \rightarrow M^*$  and mapping  $f : M \rightarrow N$  for some complete Hausdorff space  $N$ , then there exists a unique  $g : M^* \rightarrow N$  such that the diagram commutes.

$$\begin{array}{ccc} M & \xrightarrow{\quad} & M^* \\ & \searrow f & \swarrow \exists! g \\ & & N \end{array}$$

Indeed,  $M^*$  is the set of elements  $(\bar{x}_n)$  with  $\eta_{n+1}(\bar{x}_{n+1}) = \bar{x}_n$ , therefore this is the set of elements  $(x_n)$  with  $x_{n+1} - x_n \in M_n$  for all  $n$ , therefore  $\{x_n\}$  is a Cauchy sequence, so for  $y = \varprojlim f(x_n)$ , therefore  $g((\bar{x}_n)) = y$ . Now if  $\{x'_n\}$  is another lift of  $(\bar{x}_n) \in M^*$ , then we can check that  $\{x_n - x'_n\} \rightarrow 0$  for  $n \rightarrow \infty$ , hence  $\varprojlim f(x_n) = \varprojlim f(x'_n)$ , so  $M^* = \bar{M}$ ,  $M_n^* = \bar{M}_n$  and so on.

**Lemma 2.41.** Let  $R = A[x_1, \dots, x_n]$ ,  $I = (x_1, \dots, x_n)$ , then the  $I$ -adic completion is equivalent to the completion with respect to  $I$ -adic filtration corresponding to the topology. i.e., the completion of  $A[x_1, \dots, x_n]$  is  $\hat{A}[[x_1, \dots, x_n]]$ .

**Lemma 2.42.** Say  $A \sim \{A_n\}$ , and suppose  $A$  is Hausdorff, i.e.,  $\bigcap A_n = (0)$ , then if  $E_0(A)$  is a domain, then  $A$  is also a domain.

*Proof.* Suppose not, then we can pick  $x \neq 0$  and  $y \neq 0$  such that  $xy = 0$ , then  $x \in A_n \setminus A_{n+1}$  and  $y \in A_m \setminus A_{m+1}$  for some  $n, m$ , then considering the decomposition of  $E_0(A)$  we have  $\bar{x} \neq 0$  in  $A_n/A_{n+1}$  and  $\bar{y} \neq 0$  in  $A_m/A_{m+1}$ , so  $\bar{y}\bar{x} = \overline{yx} = 0$ , this is a contradiction to the fact that  $E_0(A)$  is a domain, therefore  $A$  is a domain.  $\square$

**Definition 2.43.** Let  $A$  and  $M$  be filtered and Hausdorff, say  $x \in M$  be such that  $x \in M_n \setminus M_{n+1}$  with largest such  $n$ , then we say  $n$  is the filtered degree of  $x$ .

**Theorem 2.44.** Let  $A \sim \{A_n\}$  and  $M \sim \{M_n\}$  and  $N \sim \{N_n\}$ , and  $f : M \rightarrow N$  be a filtered map. Suppose that  $M$  is complete,  $N$  is Hausdorff, and  $E_0(f) : E_0(M) \rightarrow E_0(N)$  is onto, so we can write  $E_0(M) = M/M_1 \oplus M_1/M_2 \oplus \dots \oplus M_n/M_{n+1}$  and  $E_0(N) = N/N_1 \oplus N_1/N_2 \oplus \dots \oplus M_n/M_{n+1}$ , then we have corresponding maps

$$E_0(f)_n : M_n/M_{n+1} \rightarrow N_n/N_{n+1} \\ (\bar{x}) \mapsto \overline{f(x)},$$

then  $f$  is onto,  $N$  is complete, and  $f$  is strict.

*Proof.* Since  $E_0(f)$  is onto, take  $x \in N$  and since  $N$  is Hausdorff, then  $x \in N_n \setminus N_{n+1}$  for some  $n$ . Therefore, the induced mapping  $E_0(f)_n : M_n/M_{n+1} \rightarrow N_n/N_{n+1}$  is onto. Therefore, for  $\bar{x} \in N_n/N_{n+1}$ , we can pick  $y_n \in M_n$  such that  $x - f(y_n) \in N_{n+1}$ . Therefore, on the level of  $E_0(f)_{n+1}$ , we know  $x - f(y_n) \in N_{n+1}/N_{n+2}$ , therefore we can pick  $y_{n+1} \in M_{n+1}$  such that  $x - f(y_n) - f(y_{n+1}) \in N_{n+2}$ . Proceeding inductively, we have a sequence of elements with  $y_{n+t} \in M_{n+t}$  such that  $x - \sum_{k=0}^t f(y_{n+k}) \in N_{n+t+1}$ . Hence, we have a Cauchy sequence in  $M$ , and so this is a Cauchy sequence in  $M_n$ , so  $y_{n+t} \rightarrow 0$  as  $t \rightarrow \infty$ , then  $\sum_t y_{n+t}$  converges, thus the sum  $y \in M_n$ . One can check that  $f(y) = \bar{x}$ , so  $f$  is onto. But that means  $f(M_n) = N_n$ , so  $f$  is strict. We also note that  $f^{-1}(0)$  is a closed submodule of  $M$  since  $N$  is Hausdorff, therefore by [Theorem 2.26](#) we know  $N$  is complete.  $\square$

**Corollary 2.45.** Let  $A$  be complete with respect to the filtration, let  $M$  be Hausdorff. Suppose  $E_0(M)$  is a finitely-generated graded module over  $E_0(A)$ , that is, there exists  $x_1, \dots, x_t$ , where the degree of  $\bar{x}_i$  is  $r_i$ , such that  $E_0(M)$  is a graded module over  $E_0(A)$  generated by  $\bar{x}_1, \dots, \bar{x}_t$ . If this is the case, then  $M$  is generated by  $x_1, \dots, x_t$  over  $A$ .

*Proof.* Denote  $F = \bigoplus_{i=1}^t Ae_i$ , then this induces a mapping

$$\varphi : F \rightarrow M \\ e_i \mapsto x_i$$

defined on the generators. Since this is a finite sum over complete ring  $A$ , then  $F$  is complete. Let  $r_i$  be the degree of  $x_i$ , then this imposes a filtration on  $Ae_i$  as follows:

$$(Ae_i)_j = \begin{cases} 0, & j \leq r_i \\ A_{j-r_i}e_i, & j > r_i \end{cases}$$

We implement this on all  $i$ 's, then the filtered degree of  $e_i$  is just  $r_i$ . Using this filtration, we induce a filtration on  $F$ , then we have a commutative diagram

$$\begin{array}{ccc} E_0(F) & \xrightarrow{E_0(\varphi)} & E_0(M) \\ \parallel & & \parallel \\ E_0\left(\bigoplus_{i=1}^t Ae_i\right) & \xrightarrow{\varphi'} & E_0(M) \end{array}$$

with induced map  $\varphi'$ , where  $\varphi'$  sends  $\bar{\varphi}_i \mapsto \bar{x}_i$  for all  $1 \leq i \leq t$ . Therefore,  $\varphi$  is onto as a  $E_0(A)$ -module map. By [Theorem 2.44](#) we are done.  $\square$

**Corollary 2.46.** Let  $A \sim \{A_n\}$  be complete with respect to filtration, let  $M$  be Hausdorff with filtration  $\{M_n\}$ , and suppose  $E_0(M)$  is Noetherian, then  $M$  is Noetherian as well.

*Proof.* Take submodule  $N \subseteq M$ , define  $N_n = N \cap M_n$ , then we have an induced filtration of  $N$ , therefore  $E_0(N)$  is a submodule of  $E_0(M)$  with  $N_n/N_{n+1} \hookrightarrow M_n/M_{n+1}$  for all  $n$ . Hence,  $N$  is Hausdorff with respect to  $\{N_n\}$ , and  $E_0(N)$  is a finitely-generated  $E_0(A)$ -module, since  $E_0(N)$  is a submodule of  $E_0(M)$ . By [Corollary 2.45](#), this implies  $N$  is finitely-generated and complete.  $\square$

**Corollary 2.47.** Under the same assumptions as in [Corollary 2.46](#), every submodule  $N$  of  $M$  is a closed submodule.

*Proof.* By [Corollary 2.46](#),  $N$  is complete, and every complete subspace of a Hausdorff space is closed, thus  $N$  is closed.  $\square$

**Corollary 2.48.** Let  $(A, \mathfrak{m})$  be quasi-local, i.e.,  $\mathfrak{m}$  is the unique maximal ideal of a commutative ring (not necessarily Noetherian)  $A$ . In addition, suppose  $A$  is complete and Hausdorff with a  $\mathfrak{m}$ -adic filtration, i.e.,  $\bigcap \mathfrak{m}^n = (0)$ . Let  $M$  be an  $A$ -module with respect to the filtration  $\{\mathfrak{m}^n M\}$ , and assume  $M$  is Hausdorff. If  $\dim_{A/\mathfrak{m}}(M/\mathfrak{m}M)$  is finite, and suppose  $\mathfrak{m}$  is a finitely-generated ideal in  $A$ , then  $M$  is a finitely-generated  $A$ -module.

*Proof.* We write down the decomposition

$$E_0(M) = M/\mathfrak{m}M \oplus \frac{\mathfrak{m}M}{\mathfrak{m}^2 M} \oplus \cdots \oplus \frac{\mathfrak{m}^n M}{\mathfrak{m}^{n+1} M} \oplus \cdots$$

and

$$E_0(A) = A/\mathfrak{m} \oplus \frac{\mathfrak{m}}{\mathfrak{m}^2} \oplus \cdots \oplus \frac{\mathfrak{m}^n}{\mathfrak{m}^{n+1}} \oplus \cdots$$

Denote  $\mathfrak{m} = (x_1, \dots, x_n)$  to be the finitely-generated ideal, and since  $A/\mathfrak{m} \cong k$  is a field, then we have a ring homomorphism

$$\begin{aligned} \eta : k[x_1, \dots, x_n] &\rightarrow E_0(A) \\ x_i &\mapsto \bar{x}_i \in \mathfrak{m}/\mathfrak{m}^2 \end{aligned}$$

then  $\eta$  is onto, hence  $E_0(A)$  is Noetherian. If we write  $M/\mathfrak{m}M = k\{\bar{\alpha}_1, \dots, \bar{\alpha}_r\}$ , then one can check that  $E_0(M)$  is generated by  $\bar{\alpha}_1, \dots, \bar{\alpha}_r$  for  $\bar{\alpha}_i \in M/\mathfrak{m}M$  over  $E_0(A)$ . This implies  $E_0(M)$  is Noetherian and thus  $M$  is finitely-generated over  $A$  by [Corollary 2.46](#).  $\square$

**Corollary 2.49.** Let  $A$  be a commutative ring and  $I$  be a finitely-generated ideal over  $A$  such that  $A/I$  is Noetherian. Suppose  $A$  is  $I$ -adically complete, i.e.,  $A$  is complete with respect to the filtration  $\{I^n\}$ , then  $A$  is Noetherian.

*Proof.* We write down

$$E_0(A) = A/I \oplus I/I^2 \oplus \cdots \oplus I^n/I^{n+1} \oplus \cdots$$

for  $I = (x_1, \dots, x_n)$ , then using the same argument we have a ring homomorphism

$$\begin{aligned} \eta : A/I[x_1, \dots, x_n] &\rightarrow E_0(A) \\ x_i &\mapsto \bar{x}_i \in I/I^2 \end{aligned}$$

which is also surjective. Since  $A/I$  is Noetherian, then  $A/I[x_1, \dots, x_n]$  is also Noetherian, thus  $E_0(A)$  is Noetherian, and by [Corollary 2.46](#), we conclude that  $A$  is Noetherian.  $\square$

**Remark 2.50.** Suppose  $A$  is Noetherian, and consider the completion  $B = A[[x_1, \dots, x_n]]$  of  $A[x_1, \dots, x_n]$  with respect to the  $I$ -adic filtration where  $I = (x_1, \dots, x_n)$ . Therefore,  $A[[x_1, \dots, x_n]] = \varprojlim A[x_1, \dots, x_n]/I^n$ . Now  $B/IB$  is  $A$ -Noetherian, so by [Corollary 2.49](#) we conclude that  $A[[x_1, \dots, x_n]]$  is also Noetherian.

**Exercise 2.51.** Let  $A$  be a commutative ring, and we assume it is Noetherian. Let  $I \subsetneq J$  be ideals of  $A$ , and that  $\bigcap J^n = (0)$ . Suppose  $A$  is complete with respect to the  $J$ -adic topology. Prove that  $A$  is complete with respect to the  $I$ -adic topology as well.

**Remark 2.52.** We saw in [Remark 2.50](#) that  $A[[x_1, \dots, x_n]]$  is complete with respect to  $(x_1, \dots, x_n)$ , then the completeness holds for any  $I \subseteq (x_1, \dots, x_n)$ .

**Proposition 2.53.** Let  $A$  be commutative ring and  $M$  be a finitely-generated  $A$ -module, and suppose  $I$  is an ideal of  $A$  such that  $M = IM$ , then there exists  $a \in I$  such that  $(1 - a)M = 0$ .

**Remark 2.54.** Proposition 2.53 itself is a direct application of Cayley-Hamilton Theorem, and the proof below follows the same approach. This is also sometimes referred to as Nakayama Lemma (c.f., Corollary 2.55).

*Proof.* We write  $M = \langle \alpha_1, \dots, \alpha_n \rangle$  and let  $I$  be such that  $IM = M$ , then

$$\alpha_1 = a_{11}\alpha_1 + \dots + a_{1n}\alpha_n$$

where  $a_{1i} \in I$ . In general, we have

$$\alpha_j = a_{j1}\alpha_1 + \dots + a_{jn}\alpha_n$$

for  $a_{ji} \in I$ . Therefore,

$$\begin{cases} (1 - a_{11})\alpha_1 - a_{12}\alpha_2 - \dots - a_{1n}\alpha_n &= 0 \\ -a_{21}\alpha_1 + (1 - a_{22})\alpha_2 - \dots - a_{2n}\alpha_n &= 0 \\ &\vdots \\ -a_{n1}\alpha_1 - a_{n2}\alpha_2 - \dots + (1 - a_{nn})\alpha_n &= 0 \end{cases}$$

and this gives a matrix

$$C = \begin{pmatrix} 1 - a_{11} & -a_{12} & \dots & -a_{1n} \\ -a_{21} & 1 - a_{22} & \dots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \dots & 1 - a_{nn} \end{pmatrix}$$

such that

$$CX := C \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = 0.$$

If we do the cofactor decomposition with respect to the first column, we have  $\det(C) \cdot \alpha_1 + 0 \cdot \alpha_2 + \dots + 0 \cdot \alpha_n = 0$ , hence  $\det(C) \cdot \alpha_1 = 0$ . If we do this for each column, we have  $\det(C) \cdot \alpha_i = 0$  for all  $i$ , hence  $\det(C) \cdot M = 0$ . But note that  $\det(C) = 1 - a$  for some  $a \in I$ , therefore  $(1 - a)M = 0$ .<sup>3</sup>  $\square$

**Corollary 2.55** (Nakayama Lemma). Suppose  $I$  is an ideal of  $A$  contained in the Jacobson radical of  $A$ , and  $M$  is a finitely-generated  $A$ -module such that  $M = IM$ , then  $M = 0$ .

*Proof.* By Proposition 2.53, there exists  $a \in I$  such that  $(1 - a)M = 0$ . Note that the Jacobson radical is the intersection of all maximal ideals of  $A$ , so  $I$  is contained in all maximal ideals of  $A$ . Since  $a \in I$ , then  $1 - a$  is a unit in  $A$ , so  $M = 0$ .  $\square$

**Exercise 2.56.** Let  $A$  be a commutative ring and  $M$  be a finitely-generated  $A$ -module. Suppose  $f : M \rightarrow M$  is a surjective  $A$ -linear map, then  $f$  is an isomorphism. *Hint:* use Proposition 2.53.

From now on, we assume  $A$  is Noetherian,  $M$  is a finitely-generated  $A$ -module. Usually, we assume  $A$  and  $M$  have  $I$ -adic filtrations for some ideal  $I \subseteq A$ .

**Lemma 2.57** (Artin-Rees). Let  $A$  be Noetherian and  $M$  is a finitely-generated  $A$ -module, and  $I \subseteq A$  is an ideal. Given submodule  $N \subseteq M$ , suppose there exists  $k > 0$  such that for every  $n$  we have  $N \cap I^{n+k}M = I^n(N \cap I^kM)$ .

**Remark 2.58.** The proof essentially refers to the blow-up algebra, i.e., Rees algebra.

<sup>3</sup>The cleanest way to finish the proof would be to observe that  $I \cdot \det(C) = (\text{adj}(C))C$  and so  $I \cdot \det(C)X = (\text{adj}(C))CX = 0$ . In particular,  $\det(C) \cdot X = 0$  and since  $X$  generates  $M$ , then  $\det(C) \cdot M = 0$ . Note that this is equivalent to the given approach since the cofactor matrix induces  $\text{adj}(C)$ .

*Proof.* Note that the  $(\supseteq)$  direction is true by definition, so we only need to show the  $(\subseteq)$  direction. Let us write  $\tilde{A} = A \oplus I \oplus I^2 \oplus \cdots$ , more formally this is  $A \oplus It \oplus I^2 t^2 \oplus \cdots \oplus I^n t^n \oplus \cdots \subseteq A[t]$ .<sup>4</sup> This is a graded ring. Similarly, we write  $\tilde{M} = M \oplus IM \oplus I^2 M \oplus \cdots \oplus I^n M \oplus \cdots$ .

**Claim 2.59.**  $\tilde{A}$  is a graded Noetherian ring.

*Subproof.* Let  $I = (x_1, \dots, x_n)$ , then the ring homomorphism

$$\eta : A[x_1, \dots, x_n] \rightarrow \tilde{A}$$

$$x_i \mapsto x_i,$$

is onto. Since  $A$  is Noetherian, then  $A[x_1, \dots, x_n]$  is also Noetherian. Therefore,  $\tilde{A}$  is a graded Noetherian ring.  $\blacksquare$

Suppose  $M$  is generated by  $\alpha_1, \dots, \alpha_r$ , then  $\tilde{M}$  is a finitely-generated graded  $\tilde{A}$ -module, generated by  $\alpha_1, \dots, \alpha_r \in M$  by the surjectivity of  $\eta$ . This implies that  $\tilde{M}$  is a graded Noetherian module. Now define

$$\tilde{N} = N \oplus (N \cap IM) \oplus (N \cap I^2 M) \oplus \cdots \oplus (N \cap I^k M) \oplus \cdots \oplus (N \cap I^{n+k} M) \oplus \cdots,$$

then  $\tilde{N} \subseteq \tilde{M}$ , so  $\tilde{N}$  is a finitely-generated graded  $\tilde{A}$ -module. Now each generator is a finite sum given by decomposition above, so each of the generating set must be a graded element. Hence,  $\tilde{N}$  is generated by finitely many elements, which are graded elements, say  $\beta_1, \dots, \beta_t$  where  $\deg(\beta_i) = r_i$ . Let  $k = \max_{1 \leq i \leq t} r_i$ , and we think of ways to obtain elements in  $N \cap I^{n+k} M$ . Considering the multiplicity of the degree, we know  $I^{n+k-r_i} \beta_i \subseteq N \cap I^{n+k} M$  for each  $1 \leq i \leq t$ . Therefore, we have

$$N \cap I^{n+k} M = I^{n+k} N + I^{n+k-1} (N \cap IM) + \cdots + I^n (N \cap I^k M) = \sum_{j=0}^k I^{n+k-j} (N \cap I^j M).$$

Each  $I^{n+k-j} (N \cap I^j M) = I^n \cdot I^{k-j} (N \cap I^j M) \subseteq I^n (N \cap I^k M)$ , so the sum  $N \cap I^{n+k} M \subseteq I^n (N \cap I^k M)$ .  $\square$

**Corollary 2.60.** Using the same assumption as in Lemma 2.57, let  $I$  be an ideal of  $A$  contained in the Jacobson radical of Noetherian ring  $A$ , then  $\bigcap I^n M = (0)$ .

*Proof.* Let  $N = \bigcap I^n M$ , then by Lemma 2.57,  $I^n N = N = N \cap I^{n+k} M = I^n (N \cap I^k M)$ , then by Corollary 2.55,  $N = 0$ .  $\square$

**Remark 2.61.** In particular, Corollary 2.60 implies  $M$  is Hausdorff with respect to the  $I$ -adic topology, so the map  $M \hookrightarrow \hat{M}$  is an injection by the mapping

$$M \rightarrow \varprojlim M/I^n M \subseteq \prod M/M^n M$$

$$x \mapsto (x, x, \dots)$$

**Corollary 2.62.** Using the same assumption as in Lemma 2.57, let  $A$  be a domain with ideal  $I$ , then  $\bigcap I^n = (0)$ .

*Proof.* Let  $J = \bigcap I^n$ , then  $J \cap I^{n+k} A = I^n (J \cap I^k)$ , so  $J = I^n J$ , then by Proposition 2.53 there exists  $a \in I^n$  such that  $(1 - a)J = 0$ , and since  $A$  is a domain, then  $J = 0$ .  $\square$

**Remark 2.63.** Corollary 2.62 implies that under  $I$ -adic topology, the map  $A \rightarrow \hat{A}$  is injective.

**Definition 2.64.** Let  $A \sim \{I^n\}$  and  $M \sim \{M_n\}$ , not necessarily with respect to the  $I$ -adic filtration, then  $\{M_n\}$  is called  $I$ -good if there exists  $h > 0$  such that  $M_{n+h} = I^n M_h$ .

**Remark 2.65.** By Lemma 2.57, induced filtration is  $I$ -good. Topologically, given  $A \sim \{I^n\}$  and  $M \sim \{M_n\}$  such that  $\{M_n\}$  is  $I$ -good, then  $I^n M \subseteq M_h$  for some  $h > 0$ , so  $M_{n+h} = I^n M_h \subseteq I^n M$ . In this case,  $\{I^n M\}$  and  $\{M_n\}$  are cofinal with respect to each other and hence give the same topology on  $M$ . Moreover,

$$\varprojlim M/I^n M \cong \varprojlim M/M_n.$$

That is, the  $I$ -adic completion of  $M$  is equivalent to the completion of  $M$  with respect to  $\{M_n\}$ .

<sup>4</sup>For instance, we usually write  $A[t]$  for  $A \oplus At \oplus At^2 \oplus \cdots$ .



**Remark 2.66.** Given an  $I$ -good filtration and a submodule  $N$  of  $M$ ,  $\{I^n N\}$  and  $\{N \cap I^n M\}$  define the same topology on  $N$ , and hence the  $I$ -adic completion of  $N$  is equivalent to the completion of  $M$  with respect to  $\{M_n\}$ .

**Proposition 2.67.** Let  $A$  be Noetherian and a short exact sequence

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} T \longrightarrow 0$$

of finitely-generated  $A$ -modules, and let  $I$  be an ideal of  $A$ , then we have a short exact sequence

$$0 \longrightarrow \hat{N} \xrightarrow{\hat{f}} \hat{M} \xrightarrow{\hat{g}} \hat{T} \longrightarrow 0$$

where all completions are  $I$ -adic completions.

*Proof.* By Lemma 2.57, we know  $\hat{N} = \varprojlim N/I^n N = \varprojlim N/(N \cap I^n M)$ , then we have a short exact sequence

$$0 \longrightarrow N/(N \cap I^n M) \longrightarrow M/I^n M \longrightarrow T/I^n T \longrightarrow 0$$

for every  $n > 0$ . It now suffices to show that

$$0 \longrightarrow \varprojlim N/(N \cap I^n M) \longrightarrow \varprojlim M/I^n M \longrightarrow \varprojlim T/I^n T \longrightarrow 0$$

**Exercise 2.68.**  $\ker(\bar{f}) = 0$  and  $\text{im}(\hat{f}) = \ker(\hat{f})$ .

We now show that  $\hat{g}$  is onto. Taking  $\{z_n\}$  in  $\varprojlim T/I^n T$ , we want to show that there exists  $\{y_n\}$  in  $\varprojlim M/I^n M$  with image  $\{z_n\}$ , and we proceed inductively. Suppose we have constructed  $\{y_i\}_{i \leq n}$  such that  $\text{im}(y_i) = z_i$  with system  $y_n \rightarrow y_{n-1} \rightarrow \cdots \rightarrow y_1$ , then there is a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & N/(N \cap I^{n+1}M) & \xrightarrow{f_{n+1}} & M/I^{n+1}M & \xrightarrow{g_{n+1}} & T/I^{n+1}T \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & N/(N \cap I^n M) & \longrightarrow & M/I^n M & \longrightarrow & T/I^n T \longrightarrow 0 \end{array}$$

where  $y_n \in M/I^n M$  and  $z_n \in T/I^n T$ . Here all rows are exact and the vertical mappings are surjective. We proceed by diagram chasing. To find  $y_{n+1} \in M/I^{n+1}M$  such that  $\text{im}(y_{n+1}) = z_{n+1}$ , since  $g_{n+1} : M/I^{n+1}M \rightarrow T/I^{n+1}T$  is onto, then we lift it back to  $x_{n+1} \in M/I^{n+1}M$  such that  $g_{n+1}(x_{n+1}) = z_{n+1}$ , and now there is  $x_n$  landing in  $M/I^n M$  by the vertical mapping. Note that by definition  $x_n$  now lands in  $z_n$  by the vertical mapping, so we have both  $y_n \rightarrow z_n$  and  $x_n \rightarrow z_n$ , therefore  $y_n - x_n \rightarrow 0$ , now we lift it back to  $w_n$  in  $N/(N \cap I^n M)$ , which lifts to  $w_{n+1} \in N/(N \cap I^{n+1}M)$ , and let the image of  $w_{n+1}$  with respect to  $f_{n+1}$  be  $x'_{n+1}$ , then the element  $x'_{n+1} + x_{n+1}$  in  $M/I^{n+1}M$  is now such that we have

$$\begin{array}{ccc} x'_{n+1} + x_{n+1} & \longrightarrow & z_{n+1} \\ \downarrow & & \downarrow \\ y_n & \longrightarrow & z_n \end{array}$$

via diagram chasing as desired. This is the element  $y_{n+1}$  we want.  $\square$

**Remark 2.69.** Refer to the Mittag-Leffler condition, as well as the complex analysis analogue, i.e., Mittag-Leffler Theorem.

**Proposition 2.70.** Let  $A$  be Noetherian and  $M$  be a finitely-generated  $A$ -module, and let  $I$  be an ideal of  $A$ . Let  $\hat{A}$  and  $\hat{M}$  be  $I$ -adic completions of  $A$  and  $M$ , respectively, then

$$\begin{aligned} \varphi : \hat{A} \otimes_A M &\xrightarrow{\sim} \hat{M} \\ \{a_n\} \otimes x &\mapsto \{a_n x\} \end{aligned}$$

**Remark 2.71.** If we are working over direct limits, we would note

$$(\varinjlim M_\alpha) \otimes_A N = \varinjlim M_\alpha \otimes_A N.$$

This is not the case here, we do not necessarily have

$$(\varprojlim M_\alpha) \otimes_A N = \varprojlim M_\alpha \otimes_A N.$$

*Proof.* Since  $M$  is finitely-generated over Noetherian ring  $A$ , then we have an exact sequence

$$A^r \xrightarrow{\psi} A^s \xrightarrow[e_i \mapsto m_i]{\eta} M \longrightarrow 0$$

where  $M$  is generated by  $m_1, \dots, m_s$ . Tensoring by  $\hat{A}$ , we have an exact sequence

$$\hat{A} \otimes A^r \longrightarrow \hat{A} \otimes A^s \longrightarrow \hat{A} \otimes M \longrightarrow 0$$

Let  $K = \ker(\eta)$  and take  $L$  to be the kernel of  $A^r \rightarrow K$ , then we have exact sequences

$$0 \longrightarrow L \longrightarrow A^r \longrightarrow K \longrightarrow 0$$

and

$$0 \longrightarrow K \longrightarrow A^s \longrightarrow M \longrightarrow 0$$

By [Proposition 2.67](#), the  $I$ -adic filtration gives exact sequences

$$0 \longrightarrow \hat{L} \longrightarrow \hat{A}^r \longrightarrow \hat{K} \longrightarrow 0$$

and

$$0 \longrightarrow \hat{K} \longrightarrow \hat{A}^s \longrightarrow \hat{M} \longrightarrow 0$$

therefore

$$\hat{A}^r \longrightarrow \hat{A}^s \longrightarrow \hat{M} \longrightarrow 0$$

is exact and we have a diagram

$$\begin{array}{ccccccc} \hat{A} \otimes A^r & \longrightarrow & \hat{A} \otimes A^s & \longrightarrow & \hat{A} \otimes M & \longrightarrow & 0 \\ \varphi_{A^r} \downarrow & & \downarrow \varphi_{A^s} & & \downarrow \varphi_M & & \\ \hat{A}^r & \longrightarrow & \hat{A}^s & \longrightarrow & \hat{M} & \longrightarrow & 0 \end{array}$$

Now

$$\begin{aligned} \hat{A} \otimes A^s &= \hat{A} \otimes (A \oplus \dots \oplus A) \\ &= (\hat{A} \otimes_A A) \oplus \dots \oplus (\hat{A} \otimes_A A) \\ &= (\hat{A})^s \end{aligned}$$

and similarly  $\hat{A} \otimes A^r = (\hat{A})^r$ . One can check that  $\varphi_{A^r}$  and  $\varphi_{A^s}$  are isomorphisms. Now the mapping  $A^s = \bigoplus_s A \rightarrow \bigoplus_s \hat{A}$  has dense image, which implies  $\varphi_M$  is an isomorphism by diagram chasing.  $\square$

**Theorem 2.72.** Let  $A$  be Noetherian and  $I$  be an ideal, then  $A \rightarrow \hat{A}$ , the mapping into the  $I$ -adic completion, is a flat map, that is,  $\hat{A}$  is a flat  $A$ -module.

*Proof.* For flatness, we can assume that

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} T \longrightarrow 0$$

is a short exact sequence of finitely-generated modules (since we are working over Noetherian rings), and we want to show that

$$0 \longrightarrow \hat{A} \otimes_A N \xrightarrow{\hat{f}} \hat{A} \otimes_A M \xrightarrow{\hat{g}} \hat{A} \otimes_A T \longrightarrow 0$$

is a short exact sequence as well. But we know this is just

$$0 \longrightarrow \hat{N} \longrightarrow \hat{M} \longrightarrow \hat{T} \longrightarrow 0$$

by [Proposition 2.70](#), which is exact by [Proposition 2.67](#). □

**Corollary 2.73.** The map

$$A[x_1, \dots, x_n] \rightarrow A[[x_1, \dots, x_n]]$$

is flat.

## 2.4 FAITHFULLY FLAT MODULES

**Proposition 2.74.** Let  $A$  be a commutative ring and  $M$  be an  $A$ -module, then the following are equivalent:

1.

$$N_1 \xrightarrow{f} N_2 \xrightarrow{g} N_3$$

is exact if and only if

$$M \otimes N_1 \xrightarrow{f} M \otimes N_2 \xrightarrow{g} M \otimes N_3$$

is exact;

2.

$$0 \longrightarrow N_1 \xrightarrow{f} N_2 \xrightarrow{g} N_3 \longrightarrow 0$$

is exact if and only if

$$0 \longrightarrow M \otimes N_1 \xrightarrow{f} M \otimes N_2 \xrightarrow{g} M \otimes N_3 \longrightarrow 0$$

is exact;

3.  $M$  is an  $A$ -flat module and for any  $A$ -module  $N$ ,  $M \otimes_A N = 0$  implies  $N = 0$ ;

4.  $M$  is an  $A$ -flat module and for any ideal  $I$  of  $A$ ,  $M \otimes_A A/I = 0$  implies  $A = I$ .

*Proof.* The equivalence of (1) and (2) is obvious.

(1), (2)  $\Rightarrow$  (3): the flatness is obvious. Suppose  $M \otimes_A N = 0$ , then consider

$$0 \longrightarrow N \longrightarrow 0$$

and we tensor it with  $M$ , then we have

$$0 \longrightarrow M \otimes N \longrightarrow 0$$

which is exact, so

$$0 \longrightarrow N \longrightarrow 0$$

is exact and so  $N = 0$ .

(3)  $\Rightarrow$  (4): obvious, take  $N = A/I$ .

(4)  $\Rightarrow$  (3): let  $N = \varinjlim N_\alpha$  where each  $N_\alpha$  is a finitely-generated submodule of  $N$ , then  $N = \bigcup_\alpha N_\alpha$ . We know  $M \otimes_A N = \varinjlim M \otimes_A N_\alpha$ , and by flatness this is just  $\bigcup_\alpha (M \otimes_A N_\alpha)$ . It is now enough to show that if  $N$  is finitely-generated, then  $M \otimes N = 0$  implies  $N = 0$ . We proceed by induction. This is obvious when  $N$  is cyclic; suppose  $N$  is generated by a minimal set of generators  $\{x_1, \dots, x_n\}$ , then let  $N'$  be generated by  $\{x_1, \dots, x_{n-1}\}$ , so  $N' \neq N$ , now we have a short exact sequence

$$0 \longrightarrow N' \longrightarrow N \longrightarrow A/I \cong N/N' \longrightarrow 0$$

for some ideal  $I$  of  $A$ , and since  $M$  is  $A$ -flat, then we have a short exact sequence

$$0 \longrightarrow M \otimes N' \longrightarrow M \otimes N \longrightarrow M \otimes (A/I) \cong 0 \longrightarrow 0$$

but that means  $A = I$ , so  $N' = N$ , which is a contradiction unless  $M \otimes_A N = 0$  implies  $N = 0$ .

**Exercise 2.75.** Show that (3)  $\Rightarrow$  (1), (2). □

**Definition 2.76** (Faithfully Flat). Let  $A$  be a commutative ring, an  $A$ -module  $M$  is called faithfully flat if  $M$  satisfies one of the (equivalent) conditions in [Proposition 2.74](#).

**Definition 2.77** (Faithful). Let  $A$  be a commutative ring, an  $A$ -module  $M$  is called faithful if  $\text{Ann}_A(M) = \{a \in A \mid aM = 0\} = (0)$ .

**Remark 2.78.** Faithfully flat implies faithful. Indeed, let  $M$  be faithfully flat, let  $I = \text{Ann}_A(M)$ , then consider the short exact sequence

$$0 \longrightarrow I \longrightarrow A \longrightarrow A/I \longrightarrow 0$$

and therefore

$$\begin{array}{ccccccc} 0 & \longrightarrow & I \otimes_A M & \longrightarrow & A \otimes_A M & \cong & M \longrightarrow A/I \otimes_A M \longrightarrow 0 \\ & & \searrow x \otimes m \mapsto xm & & \downarrow a \otimes m \mapsto am & & \\ & & & & M & & \end{array}$$

is a short exact sequence. In particular,  $I \otimes_A M = 0$  by definition, therefore  $I = 0$  since  $M$  is flat, hence  $M$  is faithful.

**Example 2.79.** Note that  $M$  being flat and faithful does not imply  $M$  is faithfully flat. Let  $A = \mathbb{Z}$  and  $M = \mathbb{Q}$ , so  $\mathbb{Q}$  is faithful and is  $\mathbb{Z}$ -flat, but  $\mathbb{Q}$  is not faithfully flat over  $\mathbb{Z}$  since  $\mathbb{Q} \otimes \mathbb{Z}/n\mathbb{Z} = 0$  but  $\mathbb{Z}/n\mathbb{Z} \neq 0$  for  $n > 1$ .

**Theorem 2.80.** Let  $f : A \rightarrow B$  be a homomorphism of commutative rings. The following are equivalent:

- (i)  $B$  is a faithfully flat  $A$ -module via  $f$ ;
- (ii)  $B$  is  $A$ -flat, and for every ideal  $I$  of  $A$ ,  $f^{-1}(IB) = I$ ;
- (iii)  $B$  is  $A$ -flat, and for every  $A$ -module  $M$ ,  $M \rightarrow M \otimes_A B$  is injective;
- (iv)  $f$  is injective and  $B/f(A) \cong B/A$  is  $A$ -flat.

*Proof.* (i)  $\Rightarrow$  (ii):  $B$  being  $A$ -flat is obvious; let  $J = f^{-1}(IB)$ , then there is a short exact sequence

$$0 \longrightarrow I \longrightarrow J \longrightarrow J/I \longrightarrow 0$$

and tensoring it with  $B$  gives

$$\begin{array}{ccccccc} 0 & \longrightarrow & I \otimes_A B & \longrightarrow & J \otimes_A B & \longrightarrow & J/I \otimes_A B \longrightarrow 0 \\ & & \searrow & & \downarrow j \otimes b \mapsto jb & & \\ & & & & B & & \end{array}$$

where  $J \otimes_A B \cong B \cong A \otimes_A B$ , and so  $\text{im}(J \otimes_A B) = JB$ , and  $\text{im}(I \otimes_A B) = IB$ , therefore having  $J = f^{-1}(IB)$  implies  $JB = IB$ . We have  $I \otimes_A B = J \otimes_A B$ , so  $J/I \otimes_A B = 0$ . Since  $B$  is faithfully flat, then  $J/I = 0$ , so  $I = J$ .

(ii)  $\Rightarrow$  (iii): we want to show that  $i_M : M \rightarrow M \otimes_A B$  is injective. Suppose, towards contradiction, that there exists some element  $0 \neq x \in M$  such that  $i_M(x) = x \otimes 1 = 0$ , then define  $I = \{a \in A \mid ax = 0\}$ . We have a commutative diagram

$$\begin{array}{ccc} A/I & \xrightarrow{\bar{f}} & A/I \otimes_A B \\ \downarrow & & \downarrow \\ M & \longrightarrow & M \otimes_A B \end{array}$$

Note that  $A/I \otimes_A B \hookrightarrow M \otimes_A B$  is injective since  $B$  is  $A$ -flat. This gives a diagram chasing

$$\begin{array}{ccc} \bar{1} & \xrightarrow{\bar{f}} & \bar{1} \otimes 1 \\ \downarrow & & \downarrow \\ x & \longrightarrow & x \otimes 1 = 0 \end{array}$$

By the commutative diagram,  $\bar{f}(A/I) = 0$ , so  $\bar{f}$  is the zero map, and since  $A/I \otimes_A B = B/IB$ , then  $f^{-1}(IB) = A \supsetneq I$ , contradiction.

(iii)  $\Rightarrow$  (iv): let  $B$  be  $A$ -flat and suppose every  $A$ -module  $M$ , every map  $M \rightarrow M \otimes_A B$  is an injection, then  $A \rightarrow A \otimes_A B = B$  is injective. Consider

$$0 \longrightarrow A \longrightarrow B \longrightarrow B/A \longrightarrow 0$$

to show that  $B/A$  is  $A$ -flat, take the following short exact sequence

$$0 \longrightarrow N \longrightarrow T \longrightarrow M \longrightarrow 0$$

and by tensoring via the first short exact sequence we obtain

$$\begin{array}{ccccccc} & & 0 & & 0 & & 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & N & \longrightarrow & T & \longrightarrow & M \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & N \otimes_A B & \longrightarrow & T \otimes_A B & \longrightarrow & M \otimes_A B \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & N \otimes_A B/A & \longrightarrow & T \otimes_A B/A & \longrightarrow & M \otimes_A B/A \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & 0 & & 0 & & 0 \end{array}$$

and it suffices to show exactness at  $N \otimes_A B/A$ . Let  $x \in N \otimes_A B/A$  map to 0 in  $T \otimes_A B/A$ , then lift it to  $y \in N \otimes_A B$ , send it to  $z$  in  $T \otimes_A B$ , by exactness it sends to 0 in  $M \otimes_A B$ . Now  $z$  has a preimage of  $w$  in  $T$ , sending it to  $m$  in  $M$ , but injectivity of  $M \rightarrow M \otimes_A B$  implies  $m = 0$ , therefore  $w$  lifts to some  $n \in N$ , here  $n \in N$  is mapped to  $y'$  in  $N \otimes_A B$ , but that means  $n$  is mapped to 0 in  $T \otimes_A B$  as well, by injectivity of  $N \otimes_A B \rightarrow T \otimes_A B$ , we have  $y' = y$ . Hence,  $n$  maps to  $y' = y$  maps to  $x$  in the column, and by exactness this forces  $x = 0$ .<sup>5</sup>

(iv)  $\Rightarrow$  (iii): it suffices to show the following lemma.

**Lemma 2.81.** Let

$$0 \longrightarrow N \longrightarrow M \longrightarrow T \longrightarrow 0$$

be a short exact sequence of  $A$ -modules, and suppose  $T$  is  $A$ -flat, then for all  $A$ -module  $L$ , we have the short exact sequence

$$0 \longrightarrow L \otimes_A N \longrightarrow L \otimes_A M \longrightarrow L \otimes_A T \longrightarrow 0$$

to be exact.

<sup>5</sup>Instead of diagram chasing, one can apply the snake lemma instead.

*Subproof.* Suppose we have a short exact sequence

$$0 \longrightarrow V \longrightarrow F \longrightarrow L \longrightarrow 0$$

where  $F$  is free. Then consider

$$\begin{array}{ccccccc} & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & V \otimes N & \longrightarrow & F \otimes N & \longrightarrow & L \otimes N \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & V \otimes M & \longrightarrow & F \otimes M & \longrightarrow & L \otimes M \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & V \otimes T & \longrightarrow & F \otimes T & \longrightarrow & L \otimes T \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & 0 & & 0 & & 0 \end{array}$$

We want to show  $L \otimes N$  is exact in the column, i.e.,  $L \otimes N \rightarrow L \otimes M$  is injective. Note that the last row is exact since  $T$  is  $A$ -flat. We can use a similar argument. Take  $x$  in  $L \otimes N$  mapping to 0 in  $L \otimes M$ , lift it to  $y$  in  $F \otimes N$ , map it to  $z$  in  $F \otimes M$  with image 0 in  $L \otimes M$ , lift it to  $w$  in  $V \otimes M$ , send it to  $t \in V \otimes T$  which maps into 0 in  $F \otimes T$  by exactness of middle row, by injectivity we know  $t = 0$ , then lift it to  $n$  in  $V \otimes N$ , send it to  $y'$  in  $F \otimes N$  which maps to  $z$  in  $F \otimes M$ . The middle row is exact since  $F$  is free, so  $y' = y$  by injectivity, so by exactness of the row we know  $x = 0$ . ■

Therefore, consider

$$0 \longrightarrow A \longrightarrow B \longrightarrow B/A \longrightarrow 0$$

where  $B/A$  is  $A$ -flat.

**Exercise 2.82.** If  $A$  and  $B/A$  are both  $A$ -flat, then  $B$  is also  $A$ -flat.

By [Lemma 2.81](#), we know the exact sequence

$$\begin{array}{ccccccc} 0 & \longrightarrow & M \otimes_A A & \longrightarrow & M \otimes_A B & \longrightarrow & M \otimes_A B/A \longrightarrow 0 \\ & & \parallel & & \nearrow & & \\ & & M & & & & \end{array}$$

is exact, therefore  $M \rightarrow M \otimes_A B$  is injective.

(iii), (iv)  $\Rightarrow$  (i): let  $B$  be  $A$ -flat and  $M \rightarrow M \otimes_A B$  be injective. We want to show that for any  $N$  such that  $N \otimes_A B = 0$ , we have  $N = 0$ . Consider

$$0 \longrightarrow A \longrightarrow B \longrightarrow B/A \longrightarrow 0$$

to be a short exact sequence, and we know  $B/A$  is  $A$ -flat, so we now know that

$$\begin{array}{ccccccc} 0 & \longrightarrow & N \otimes_A A & \longrightarrow & N \otimes_A B & \longrightarrow & N \otimes_A B/A \longrightarrow 0 \\ & & \parallel & & \nearrow & & \\ & & N & & & & \end{array}$$

is exact, therefore  $N \otimes_A B = 0$  implies  $N = 0$  by injectivity. □

**Theorem 2.83.** Let  $A$  be a Noetherian ring and  $I$  be an ideal of  $A$ . Then  $A \rightarrow \hat{A}$  is faithfully flat if and only if  $I$  is contained in the Jacobson radical of  $A$ .

*Proof.* Suppose  $I$  is contained in the Jacobson radical of  $A$ , then  $I$  is contained in the intersection of all maximal ideals of  $A$ . For any finitely-generated  $A$ -module  $M$ , we know  $\bigcap_{n \geq 1} I^n M = (0)$ . Therefore,  $M \hookrightarrow \tilde{M} \cong M \otimes_A \hat{A}$  is an injection by [Theorem 2.80](#). Suppose  $M$  is not necessarily finitely-generated, then  $M$  is the union (hence direct limit) of finitely-generated  $A$ -modules  $M_\alpha$ 's. We want to show that  $M \rightarrow M \otimes_A \hat{A}$  is an injection. Suppose  $x \in M$  is mapped to 0, so let  $N = Ax = A/J$  where  $J = \text{Ann}_A(x)$ , then we have a diagram

$$\begin{array}{ccc} 1 \in N & \hookrightarrow & y \in N \otimes_A \hat{A} \\ \downarrow & & \downarrow \\ x \in M & \longrightarrow & 0 \in M \otimes_A \hat{A} \end{array}$$

Since  $N \hookrightarrow M$  and since  $\hat{A}$  is  $A$ -flat, so  $N \otimes_A \hat{A} \hookrightarrow M \otimes_A \hat{A}$  is injective as well. By chasing the diagram, we know  $y = 0$ , therefore by the injection we know  $N = 0$ , hence  $x = 0$ .

Suppose  $I$  is not contained in the Jacobson radical of  $A$ , then there exists some maximal ideal  $\mathfrak{m}$  of  $A$  such that  $I \not\subseteq \mathfrak{m}$ . Consider  $A/\mathfrak{m}$  with  $I$ -adic topology of filtration, then  $\mathfrak{m} + IA = A$ , therefore  $\mathfrak{m} + I^n A = A$ , hence  $A/(\mathfrak{m} + I^n) = 0$ . Therefore,  $(\widehat{A/\mathfrak{m}}) = \varprojlim (A/(\mathfrak{m} + I^n)) = 0$ . But note that  $(\widehat{A/\mathfrak{m}}) = A/\mathfrak{m} \otimes_A \hat{A} = 0$ , with  $A/\mathfrak{m} \neq 0$ , therefore  $\hat{A}$  is not faithfully flat.  $\square$

**Example 2.84.** The map  $k[x_1, \dots, x_n] \rightarrow k[[x_1, \dots, x_n]]$  is flat but not faithfully flat. Indeed, the ideal  $(x_1, \dots, x_n)$ , the ideal is not contained in  $(x_1 - a_1, \dots, x_n - a_n)$  whenever  $a_i$ 's are non-zero.

However, if we factor it via the localization

$$\begin{array}{ccc} k[x_1, \dots, x_n] & \longrightarrow & k[[x_1, \dots, x_n]] \\ \downarrow & \nearrow & \\ k[x_1, \dots, x_n]_{(x_1, \dots, x_n)} & & \end{array}$$

then  $k[x_1, \dots, x_n]_{(x_1, \dots, x_n)} \rightarrow k[[x_1, \dots, x_n]]$  is faithfully flat.

**Exercise 2.85.** Let  $k$  be a field, fix  $n$ . Define  $R_i = k[[X_1, \dots, X_i]]$  for  $i \leq n$ . We say  $0 \neq f \in R_n$  is *regular* of order  $h$  with respect to  $X_n$  if  $h$  is the smallest integer such that  $a_h$ , the coefficient of  $X_n^h$  in  $f$ , is non-zero in  $k$ . Let  $f \in R_n$  be regular with respect to  $X_n$  of order  $h$ . Prove that  $R_n/(f)$  is a free  $R_{n-1}$ -module with basis  $1, \bar{X}_n, \dots, \bar{X}_n^{h-1}$ , where  $\bar{X}_n = \text{im}(\bar{X}_n)$  in  $R_n/(f)$ . Also prove that  $R_n/(f)$  is complete with respect to  $(X_1, \dots, X_{n-1})$ -adic topology.

**Remark 2.86.** In  $\mathbb{C}[[z]]$ ,  $f$  being regular of degree  $h$  implies  $f(z) = a_h z^h + a_{h+1} z^{h+1} + \dots$ , so  $\mathbb{C}[[z]]/(f(z)) = \mathbb{C}[[z]]/(z^h(a_h + a_{h+1}z + \dots))$ , where  $a_h + a_{h+1}z + \dots$  is a unit, so this is just  $\mathbb{C}[[z]]/(z^h)$ , which is just a pole of order  $h$ .

### 3 DIMENSION THEORY

#### 3.1 GRADED RINGS AND HILBERT-SAMUEL POLYNOMIAL

**Definition 3.1.** Let  $\mathcal{F}$  be the set of functions  $f : \mathbb{Z} \rightarrow \mathbb{Z}$ , let  $\mathcal{P}$  be the set of functions  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  such that there exists a polynomial  $g \in \mathbb{Q}[x]$  such that  $f(n) = g(n)$  for  $n \gg 0$ .

**Remark 3.2.** Obviously such  $g$  is unique, since any such choices would agree for all sufficiently large values.

**Definition 3.3.**  $f \in \mathcal{P}$  is called an essentially polynomial, or an essentially polynomial function.

**Definition 3.4** (Degree). We define the degree of  $f$  to be the degree of function  $g$ .

**Remark 3.5.** If  $f = 0$  for  $n \gg 0$ , then  $\deg(f) = -1$ ; if  $f = a$  is a non-zero constant function, then  $\deg(f) = 0$ .

**Example 3.6.** Say  $f(n) = \binom{n}{i}$  where we fix  $i$ . For  $n \geq i$ ,  $f(n)$  is an integer; for  $n < i$ ,  $f(n) = 0$ . Therefore, the function  $f(x) = \binom{x}{i}$  is a function with rational coefficients.

**Definition 3.7.** For  $f \in \mathcal{F}$ , we define  $\Delta f : \mathbb{Z} \rightarrow \mathbb{Z}$  to be a function such that  $\Delta f(n) = f(n+1) - f(n)$ .

**Remark 3.8.** If  $f \in \mathcal{P}$ , then  $\Delta f \in \mathcal{P}$ . For  $n \gg 0$ ,  $f(n) = a_0 n^r + a_1 n^{r-1} + \cdots + a_r$  for  $a_i \in \mathbb{Q}$ , then  $\Delta f(n) = r a_0 n^{r-1} + \cdots$ . Hence,  $\Delta^r(f) = r! a_0$ . But we know  $\Delta^r : \mathbb{Z} \rightarrow \mathbb{Z}$  if we proceed inductively, so  $r! a_0$  is an integer. Note that  $\Delta^{r+1}(f) = 0$ .

**Definition 3.9** (Multiplicity). We say  $\Delta^r(f) \equiv \mu(f)$  is the multiplicity of  $f$ , that is,  $\mu(f) = r! a_0$ .

**Lemma 3.10.** Let  $f : \mathbb{Z} \rightarrow \mathbb{Z}$ , then the following are equivalent:

- (i)  $f \in \mathcal{P}$ ;
- (ii)  $\Delta(f) \in \mathcal{P}$ ;
- (iii) there exists  $r > 0$  such that either  $\Delta^{r+1}f = 0$  for  $n \gg 0$ , or  $\Delta^r(f)$  is constant.

*Proof.* It is enough to show that  $\Delta f \in \mathcal{P}$  implies  $f \in \mathcal{P}$ , and we will induct on degree of  $\Delta f$ . If the degree of  $\Delta f$  is  $-1$ , then  $\Delta f(n) = 0$  for  $n \gg 0$ , so if  $f(n+1) - f(n) = 0$  for  $n \gg 0$ , then  $f(n+1) = f(n)$  for  $n \gg 0$ , thus  $f$  is constant for  $n \gg 0$ , by definition  $f \in \mathcal{P}$ . Now suppose this holds for polynomial  $f$  with degree of  $\Delta f$  at most  $r-1$ . Suppose  $\Delta f$  is of the form  $a_0 n^r + a_1 n^{r-1} + \cdots + a_r$ , then  $r! a_0 = \Delta^{r+1}f = \Delta^r(\Delta f) = r! a_1$  which are integers. We write  $g(x) = r! a_0 \binom{x}{r+1}$  then  $\Delta g(n)$  is dominated by the term  $r! a_0 \frac{r+1}{(r+1)!} n^r$ , which is just  $a_0 n^r$ . We know  $\Delta(f - g) = \Delta(f) - \Delta(g)$  which is a polynomial of degree at most  $r-1$ , so by induction  $f - g \in \mathcal{P}$ , hence  $f = g + h$  for some  $h \in \mathcal{P}$ , hence  $f \in \mathcal{P}$ .  $\square$

**Exercise 3.11.** Show that  $\mathcal{P}$  is a free abelian group with basis  $\binom{x}{i}$  where  $i \geq 0$ .

Recall that  $A$  is Artinian if and only if  $A$  is Noetherian and  $A$  has finitely many prime ideals such that each of which is maximal. Note that  $(0) = \mathfrak{m}_1^{i_1} \cdots \mathfrak{m}_r^{i_r}$  is a decomposition of maximal ideals, if and only if  $\ell_A(A) < \infty$ . Moreover, if  $M$  is a finitely-generated  $A$ -module, then  $\ell_A(M) < \infty$ .

**Definition 3.12.** Suppose  $A$  has a decomposition  $A = A_0 \oplus A_1 \oplus \cdots \oplus A_n \oplus \cdots$  and  $M$  is a graded module  $M = M_0 \oplus M_1 \oplus \cdots \oplus M_n \oplus \cdots$  where  $A_i M_j \subseteq M_{i+j}$ . Suppose  $N \subseteq M$  is a submodule. Let  $x \in N$  be written as  $x = x_{i_1} + \cdots + x_{i_t}$ , then we say  $N$  is a graded submodule if every  $x_{i_j} \in N$ . In particular, this is equivalent to  $N = \bigoplus_i M \cap N_i$ .

**Remark 3.13.** Under this definition,  $M/N$  is also a graded module over  $A$ . Moreover, let  $B = A[X_1, \dots, X_n]$ , and suppose  $I$  is a graded ideal of  $B$ , then  $B/I$  is graded. Moreover, we view  $B$  as an  $A$ -module generated by the  $x_i$ 's, i.e.,  $B = A[x_1, \dots, x_n]$  where each  $x_i$  has degree 1.

**Theorem 3.14** (Hilbert-Serre). Let  $A_0$  be an Artinian ring and  $A = A_0[x_1, \dots, x_r]$  be a finitely-generated graded ring over  $A_0$  with  $\deg(x_i) = 1$  for all  $i$ .<sup>6</sup> Let  $M$  be a finitely-generated  $A$ -module, and denote  $M = M_0 \oplus M_1 \oplus \cdots$ , then we have the following:

<sup>6</sup>Alternatively, we have  $A = A_0 \oplus (x_1, \dots, x_r) \oplus (x_1, \dots, x_r)^2 \oplus \cdots$



- (i) each  $M_n$  is a module of finite length over  $A_0$ ;
- (ii) let  $\chi(M, n) = \ell_{A_0}(M_n)$  be the Hilbert function, then  $\chi(M, n)$  is essentially polynomial of degree at most  $r - 1$ ;
- (iii) suppose  $M_0$  generates  $M$  over  $A$ , then  $\Delta^{r-1}\chi(M, n) \leq \ell_{A_0}(M_0)$ . Moreover, the equality holds if and only if

$$\begin{aligned} M_0[X_1, \dots, X_r] &\rightarrow M \\ mX_1^{i_1} \cdots X_r^{i_r} &\mapsto mx_1^{i_1} \cdots x_r^{i_r}, \end{aligned}$$

where  $m \in M_0$ , is an isomorphism. It is obvious that  $\varphi$  is an onto graded map.

*Proof.* (i) Let  $m_1, \dots, m_t$  be the graded homogeneous generators of  $M$  over  $A$ . For each  $M_n$ , we can write  $x = \sum_{i,j} c_{i_1, \dots, i_r} x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r} m_j$  where  $c_{i_1, \dots, i_r} \in A_0$ , such that each  $x_i$  has degree 1. Suppose  $\deg(m_j) = h_j$ , then  $n = \sum_{j,k} i_k + h_j$ . The solution of this equation consists of finite number of  $(i_1, \dots, i_r)$  and  $h_j$ 's. Therefore,  $M_n$  is finitely-generated over  $A_0$ , hence  $\ell_{A_0}(M_n) < \infty$ .

- (ii) We proceed by induction on  $r$ . Suppose  $r = 0$ , then  $A = A_0$ , and  $M = M_0 \oplus M_1 \oplus \cdots \oplus M_t \oplus 0 \oplus 0 \oplus \cdots$ . This means  $\chi(M, n) = 0$  for  $n \gg 0$ , so the degree of  $\chi(M, n) = -1$ . Suppose this is true degree at most  $r - 1$ , then let  $N = \ker(x_r)$  and  $\bar{M} = M/x_r M$ , then

$$0 \longrightarrow N \longrightarrow M \xrightarrow{x_r} M \longrightarrow \bar{M} \longrightarrow 0$$

Now  $\bar{M}$  and  $N$  are finitely-generated modules over  $A_0[x_1, \dots, x_r]/x_r A_0[x_1, \dots, x_r] = A_0[\bar{x}_1, \dots, \bar{x}_{r-1}]$ . For any  $n$ , we have

$$0 \longrightarrow N_n \longrightarrow M_n \longrightarrow \bar{M}_n \longrightarrow 0$$

therefore

$$\begin{aligned} \ell(\bar{M}_n) - \ell(N_n) &= \ell_{A_0}(M_{n+r}) - \ell_{A_0}(M_n) \\ &= \Delta\chi(M, n) \\ &= \chi(\bar{M}_n) - \chi(N, n). \end{aligned}$$

By induction,  $\chi(\bar{M}, n)$  and  $\chi(N, n)$  are essentially polynomials of degree at most  $r - 1$ , so  $\Delta\chi(M, n)$  is essentially polynomial of degree at most  $r - 2$ , therefore  $\chi(M, n)$  is essentially polynomial of degree at most  $r - 1$ .

- (iii) Suppose  $M_0$  generates  $M$  over  $A$ , then it is obvious that

$$\begin{aligned} M_0[X_1, \dots, X_r] &\rightarrow M \\ mX_1^{i_1} \cdots X_r^{i_r} &\mapsto mx_1^{i_1} \cdots x_r^{i_r} \end{aligned}$$

is an onto graded map where  $m \in M_0$ . This implies  $\varphi_n : (M_0[X_1, \dots, X_r])_n \twoheadrightarrow M_n$  is onto as well. Hence,  $\ell_{A_0}(M_n) \leq \ell_{A_0}(M_0[X_1, \dots, X_r])_n$ . (Note that  $k[x, y]$  has a basis given by  $x^n, x^{n-1}y, \dots, xy^{n-1}, y^n$ .) We observe that  $(M_0[X_1, \dots, X_r])_n$  is just  $M_0 \otimes_{A_0} [A_0[X_1, \dots, X_r]]_n$  (where  $[-]_n$  is the completion on the  $n$ th grading), so  $\ell_{A_0}(M_0[X_1, \dots, X_r])_n$  is just  $\ell_{A_0}(M_0)$  multiplied by the number of monomials of (total) degree  $n$  in  $X_1, \dots, X_r$ , and by stars-and-bars that is just  $\ell_{A_0}(M_0) \binom{n+r-1}{r-1}$ . By part (ii), we know that the degree of  $\chi(M, n)$  is at most  $r - 1$ . Also, we have  $\chi(M_0[X_1, \dots, X_r], n) = \ell_{A_0}(M_0) \binom{n+r-1}{r-1}$ , which is a polynomial of degree  $r - 1$ . We then conclude that  $\Delta^{r-1}\chi(M_0[X_1, \dots, X_r], n) = \ell_{A_0}(M_0)$ . Hence,  $\Delta^{r-1}\chi(M, n) \leq \ell_{A_0}(M_0)$ .

Now suppose  $\varphi$  is an isomorphism, then  $\chi(M, n) = \chi(M_0[X_1, \dots, X_r], n) = \ell_{A_0}(M_0) \binom{n+r-1}{r-1}$ , therefore  $\Delta^{r-1}\chi(M, n) = \ell_{A_0}(M_0)$ . Conversely, if  $\Delta^{r-1}\chi(M, n) = \ell_{A_0}(M_0)$ , then we want to show  $\varphi$  is an isomorphism. Since  $\varphi$  is onto, the kernel  $L$  gives a short exact sequence

$$0 \longrightarrow L \longrightarrow M_0[X_1, \dots, X_r] \longrightarrow M \longrightarrow 0$$

where all terms are all graded components, so have positive lengths. Now we know  $\chi(M_0[X_1, \dots, X_r], n) = \chi(M, n) + \chi(L, n)$ , so  $\Delta^{r-1}\chi(M_0[X_1, \dots, X_r], n) = \Delta^{r-1}\chi(M, n) + \Delta^{r-1}\chi(L, n)$ , therefore  $\Delta^{r-1}\chi(L, n) =$

0 since  $\Delta^{r-1}\chi(M, n) = \ell_{A_0}(M_0)$ . We claim that this is not true if  $L \neq 0$ . Induct on  $\ell_{A_0}(M_0)$ . If  $\ell_{A_0}(M_0) = 1$ , then  $M_0 = k$  a field, so

$$0 \longrightarrow L \longrightarrow B = k[X_1, \dots, X_n] \longrightarrow M \longrightarrow 0$$

If  $L \neq 0$ , then  $L$  is a graded ideal of  $B$ , then for some  $d > 0$  we have  $L_d \neq 0$ . Let  $0 \neq f \in L_d$  be homogeneous of degree  $d$ , then  $B_{n-d}f \in L_n$ . This implies  $\chi(L_n) = \dim_k(L_n) \geq \dim_k(B_{n-d}) = \binom{n-d+r-1}{r-1}$ . This gives  $\Delta^{r-1}\chi(L, n) \geq 1$ , contradiction. Now suppose  $\ell_{A_0}(M_0) > 1$ , then take a Jordan-Hölder series

$$M_0 \supset M_0^{(1)} \supset M_0^{(2)} \supset \dots \supset M_0^{(n)} = 0,$$

such that  $M_0^{(i)}/M_0^{(i+1)} \cong A/\mathfrak{m}_i \cong k_i$ , where  $\mathfrak{m}_i$  is maximal and  $k_i$  is a field (but is only isomorphic as modules). Therefore,

$$M_0[X_1, \dots, X_r] \supset M_0^{(1)}[X_1, \dots, X_r] \supset M_0^{(2)}[X_1, \dots, X_r] \supset \dots$$

is a series such that  $M_0^{(i)}[X_1, \dots, X_r]/M_0^{(i+1)}[X_1, \dots, X_r] = k_i[X_1, \dots, X_r]$ .<sup>7</sup> If we now denote  $L^{(i)} = L \cap M_0^{(i)}[X_1, \dots, X_r]$ , then there is a filtration  $L \supset L^{(1)} \supset L^{(2)} \supset \dots$ , so

$$L^{(i)}/L^{(i+1)} \hookrightarrow M_0^{(i)}[X_1, \dots, X_r]/M_0^{(i+1)}[X_1, \dots, X_r] \cong k_i[X_1, \dots, X_r].$$

Hence,  $\chi(L, n) = \sum_i \chi(L^{(i)}/L^{(i+1)}, n)$ , therefore  $\Delta^{r-1}\chi(L, n) = \sum_i \Delta^{r-1}\chi(L^{(i)}/L^{(i+1)}, n)$ . But  $L \neq 0$ , so there exists some  $i$  such that  $L^{(i)}/L^{(i+1)} \neq 0$ . By the base case (of the induction on  $\ell_{A_0}(M_0)$ ), we know  $\Delta^{r-1}\chi(L^{(i)}/L^{(i+1)}, n) > 0$ , therefore  $\Delta^{r-1}\chi(L, n) > 0$ , contradiction.  $\square$

**Definition 3.15** (Hilbert Multiplicity). Suppose  $\deg(\chi(M, n)) = d$ , then  $\chi(M, n) = a_0 n^d +$  linear terms with higher degrees, where  $n \gg 0$ . Then  $A^d = \chi(M, n) = d!a_0$ . We say  $e_d(M) = d!a_0$  is the Hilbert multiplicity of  $M$  over  $A$ , i.e.,  $a_0 = \frac{e_d(M)}{d!}$ .

**Remark 3.16.** 1. Let  $A$  be Noetherian and  $M$  and  $N$  be (non-zero) finitely-generated  $A$ -modules, then the support of  $M$  is  $\text{supp}(M) = V(M)$ , the set of prime ideals  $P$  of  $A$  such that  $M_P \neq 0$ , which is equivalent to the set of prime ideals  $P$  of  $A$  where  $P \supseteq \text{Ann}_A(M)$ .

In particular, if  $I = \text{Ann}_A(M)$ , then  $\text{supp}(M) = \text{supp}(A/I) = V(A/I) \approx V(I)$ .

2. Under the above assumption,  $\text{supp}(M \otimes_A N) = \text{supp}(M) \cap \text{supp}(N)$ . Indeed, let  $P$  be in the support of  $M \otimes_A N$ , then  $(M \otimes_A N)_P \neq 0$ , so  $(M \otimes_A N)_P = M_P \otimes_{A_P} N_P \neq 0$ , so  $M_P \neq 0$  and  $N_P \neq 0$ , therefore  $P \in \text{supp}(M) \cap \text{supp}(N)$ . Now suppose  $P \in \text{supp}(M) \cap \text{supp}(N)$ , then  $M_P \neq 0$  and  $N_P \neq 0$ .

**Lemma 3.17.** Let  $A$  be a local ring and  $M, N$  be (non-zero) finitely-generated  $A$ -modules, then  $M \otimes_A N \neq 0$ .

**Remark 3.18.** We know  $\mathbb{Q} \otimes \mathbb{Z}/n\mathbb{Z} = 0$ , but  $\mathbb{Q}$  is not finitely-generated as a  $\mathbb{Z}$ -module.

*Proof.* Let  $\mathfrak{m}$  be the maximal ideal of  $A$ . If  $M \otimes_A N = 0$ , then  $A/\mathfrak{m} \otimes_A (M \otimes_A N) = 0$ , therefore  $M/\mathfrak{m}M \otimes_{A/\mathfrak{m}} M/\mathfrak{m}N = 0$ . We run a dimension argument on the vector space, then either  $M/\mathfrak{m}M = 0$  or  $N/\mathfrak{m}N = 0$ . By [Corollary 2.55](#), either  $M = 0$  or  $N = 0$ .  $\square$

This implies  $\text{supp}(M) \cap \text{supp}(N) = \text{supp}(M \otimes N)$ .

3. (a) Let  $\mathfrak{q}$  be an ideal of  $A$ , and  $M$  be a finitely-generated  $A$ -module. Suppose  $\ell(M/\mathfrak{q}M) < \infty$ , then  $\ell(M/\mathfrak{q}^n M) < \infty$  for all  $n$ .
- (b) Consider the short exact sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow T \longrightarrow 0$$

and  $\mathfrak{q}$  is an ideal of  $A$  such that  $\ell(M/\mathfrak{q}M) < \infty$ , then  $\ell(N/\mathfrak{q}N) < \infty$  and  $\ell(T/\mathfrak{q}T) < \infty$ .

<sup>7</sup>Consider the quotient of modules as a short exact sequence, and then tensor it by the polynomial ring structure, then we retrieve a short exact sequence represented by this quotient.

*Proof.* (a) Note that  $\ell(M/\mathfrak{q}M) < \infty$  if and only if  $\text{supp}(M/\mathfrak{q}M)$  consists of finitely many maximal ideals only, therefore  $\text{supp}(M/\mathfrak{q}M) = \text{supp}(A/\mathfrak{q} \otimes_A M) = \text{supp}(A/\mathfrak{q}) \cap \text{supp}(M)$ . Therefore,

$$\begin{aligned}\text{supp}(M/\mathfrak{q}^n M) &= \text{supp}(A/\mathfrak{q}^n) \cap \text{supp}(M) \\ &= \text{supp}(A/\mathfrak{q}) \cap \text{supp}(M),\end{aligned}$$

so it consists of maximal ideals only as well, therefore  $\ell(M/\mathfrak{q}^n M) < \infty$  for all  $n > 0$ .

(b) Note that  $\text{supp}(N/\mathfrak{q}N) = \text{supp}(A/\mathfrak{q}) \cap \text{supp}(N) \subseteq \text{supp}(A/\mathfrak{q}) \cap \text{supp}(M)$ , which consists of maximal ideals only, therefore  $\text{supp}(N/\mathfrak{q}N)$  consists of maximal ideals only as well. That is,  $\ell(N/\mathfrak{q}N) < \infty$ .  $\square$

**Theorem 3.19.** Let  $A$  be a Noetherian ring,  $\mathfrak{q}$  be an ideal of  $A$ , and let  $M$  be a finitely-generated  $A$ -module. Suppose  $A \sim \{\mathfrak{q}^n\}$  and  $M \sim \{M_n\}$  where the filtration is given by  $\mathfrak{q}^i M_j \subseteq M_{i+j}$ . We further assume that  $\ell(M/\mathfrak{q}M) < \infty$ , and that  $\{M_n\}$  is  $\mathfrak{q}$ -good. Define  $P_{\mathfrak{q}}((M_n), n) := \ell_A(M/M_n)$ , then  $\mathfrak{q}^n M \subseteq M_n$ , therefore there is a surjection  $M/\mathfrak{q}^n M \twoheadrightarrow M/M_n$ . Then

- $P_{\mathfrak{q}}((M_n), n)$  is essentially polynomial that depends on  $E_0(M)$ , and
- if  $\ell_A(M/\mathfrak{q}^n M) < \infty$ , then  $\ell_A(M/M_n)$  is finite.

*Proof.* We have

$$\begin{aligned}\Delta P_n((M_n), n) &= \ell_A(M/M_{n+1}) - \ell_A(M/M_n) \\ &= \ell_A(M_n/M_{n+1}),\end{aligned}$$

and take the decomposition  $E_0(M) = M/M_1 \oplus M_1/M_2 \oplus \cdots$ , and  $E_0(A) = A/\mathfrak{q} \oplus \mathfrak{q}/\mathfrak{q}^2 \oplus \cdots$ , then  $E_0(M)$  is an  $E_0(A)$ -module. Since  $A$  is Noetherian, then  $\mathfrak{q}$  is finitely-generated and so we write  $\mathfrak{q} = (x_1, \dots, x_n)$ , and so

$$\begin{aligned}\varphi : A/\mathfrak{q}[x_1, \dots, x_n] &\rightarrow E_0(A) \\ x_i &\mapsto \bar{x}_i \in \mathfrak{q}/\mathfrak{q}^2\end{aligned}$$

is an onto map. Note that  $A/\mathfrak{q}[x_1, \dots, x_n]$  is Noetherian, so  $E_0(A)$  is Noetherian as well. Since  $\{M_n\}$  is  $\mathfrak{q}$ -good, then there exists some  $h$  such that  $M_{n+h} = \mathfrak{q}^n M_h$  for all  $n > 0$ . Therefore,  $M/M_1 \oplus M_1/M_2 \oplus \cdots \oplus M_h/M_{h+1}$  generates  $E_0(M)$  over  $E_0(A)$ . For  $x \in M_n$ , we have  $0 \neq \bar{x} \in M_n/M_{n+1}$ , and  $M_n = \mathfrak{q}^{n-h} M_h$ , so  $x = \sum y_i w_i$  where  $y_i \in \mathfrak{q}^{n-j}$  and  $w_i \in M_h$ . Therefore,  $\bar{x} = \sum \bar{y}_i \bar{w}_i$  in  $E_0(M)$  for  $\bar{y}_i \in \mathfrak{q}^{n-h}/\mathfrak{q}^{n-h+1}$  and  $\bar{w}_i \in M_h/M_{h+1}$ . This shows that  $E_0(M)$  is a finitely-generated  $E_0(A)$ -module with generators from  $M/M_1, \dots, M_h/M_{h+1}$ , where each of them is a finitely-generated  $A/\mathfrak{q}$ -module.

**Remark 3.20.** Note that  $A/\mathfrak{q}$  is not necessarily Artinian, so we cannot apply [Theorem 3.14](#) right now.

Recall  $\ell(M/\mathfrak{q}M) < \infty$ , if we denote  $I = \text{Ann}_A(M)$ , then

$$\begin{aligned}\text{supp}(M/\mathfrak{q}M) &= \text{supp}(A/\mathfrak{q}) \cap \text{supp}(M) \\ &= \text{supp}(A/\mathfrak{q}) \cap \text{supp}(A/I) \\ &= \text{supp}(A/\mathfrak{q} \otimes_A A/I) \\ &= \text{supp}(A/(\mathfrak{q} + I)).\end{aligned}$$

If we denote  $\bar{A} = A/I$ , then  $\bar{A}/\bar{\mathfrak{q}} = A/(\mathfrak{q} + I)$ , therefore  $\ell_{\bar{A}}(\bar{A}/\bar{\mathfrak{q}}) < \infty$ . We write down  $E_0(\bar{A}) = \bar{A}/\bar{\mathfrak{q}} \oplus \bar{\mathfrak{q}}/\bar{\mathfrak{q}}^2 \oplus \cdots$ .

**Claim 3.21.**  $E_0(M)$  is a finitely-generated  $E_0(\bar{A})$ -module.

*Subproof.* Since  $IM = 0$ , then for any  $i$ ,  $(\mathfrak{q} + I)^n M_i = \mathfrak{q}^n M$ .  $\blacksquare$

Since  $\ell_{\bar{A}}(\bar{A}/\bar{\mathfrak{q}}) < \infty$ , then  $\bar{A}/\bar{\mathfrak{q}}$  is Artinian, and now by [Theorem 3.14](#) we know  $\Delta P_{\mathfrak{q}}((M_n), n)$  is essentially polynomial. Therefore,  $P_{\mathfrak{q}}((M_n), n)$  is essentially polynomial.

Let  $M_n = \{\mathfrak{q}^n M\}$ , then  $E_0(M) = M/\mathfrak{q}M \oplus \mathfrak{q}M/\mathfrak{q}^2 M \oplus \cdots$ , and  $E_0(\bar{A}) = \bar{A}/\bar{\mathfrak{q}} \oplus \bar{\mathfrak{q}}/\bar{\mathfrak{q}}^2 \oplus \cdots$ , then  $E_0(M)$  is generated by  $M/\mathfrak{q}M$  over  $E_0(\bar{A})$ . Write  $P_{\mathfrak{q}}(M, n) = \ell(M/\mathfrak{q}^n M)$ , then  $\Delta P_{\mathfrak{q}}(M, n) = \ell(\mathfrak{q}^n M/\mathfrak{q}^{n+1} M)$ . Suppose

$(\mathfrak{q} + I)/I$ , that is,  $\bar{q}$  in  $\bar{A}$ , is minimally generated by  $r$  elements  $\bar{x}_1, \dots, \bar{x}_r$ , so  $E_0(\bar{A}) = \bar{A}[\bar{x}_1, \dots, \bar{x}_r]$ , then  $\Delta P_{\bar{q}}(M, n)$  is of degree at most  $r - 1$ , and  $\Delta^{r-1}(\Delta P_{\bar{q}}(M, n)) \leq \ell(M/\mathfrak{q}M)$ , and note that the equality holds if and only if

$$\varphi : M/\mathfrak{q}M \otimes_{\bar{A}/\bar{q}} \bar{A}/\bar{q}[x_1, \dots, x_n] \rightarrow E_0(M) = M/\mathfrak{q}M \oplus \mathfrak{q}M/\mathfrak{q}^2M \oplus \dots$$

is an isomorphism. In particular,  $\Delta^r(P_{\bar{q}}(M, n)) \leq \ell(M/\mathfrak{q}M)$  therefore  $\ell_A(M/M_n)$  is finite.  $\square$

**Corollary 3.22.** Under the same assumption,  $\ell(M/\mathfrak{q}^n M) \geq \ell(M/M_n)$ . Moreover, if we write down the polynomials of  $P_{\bar{q}}(M, n)$  and  $P_{\bar{q}}((M_n), n)$ , then

- the degree of  $P_{\bar{q}}(M, n)$  is the degree of  $P_{\bar{q}}((M_n), n)$ , the leading coefficient of  $P_{\bar{q}}(M, n)$  is the leading coefficient of  $P_{\bar{q}}((M_n), n)$ , hence  $\Delta^r(P_{\bar{q}}(M, n)) = \Delta^r(P_{\bar{q}}((M_n), n))$  where  $r$  is the degree of  $P_{\bar{q}}(M, n)$ ;
- $P_{\bar{q}}(M, n) = P_{\bar{q}}((M_n), n) + R(n)$  where  $R(n)$  is essentially polynomial whose degree is less than the degree of  $P_{\bar{q}}(M, n)$ , and the leading coefficient is non-negative.

*Proof.* • Let  $P_{\bar{q}}(M, n)$  has degree  $d$  and leading coefficient  $a_0$ , and let  $P_{\bar{q}}((M_n), n)$  has degree  $d'$  and leading coefficient  $b_0$ . Since  $\ell(M/\mathfrak{q}^n M) \geq \ell(M/M_n)$  for all  $n$ , then  $d \geq d'$ . Now  $M_{n+h} = \mathfrak{q}^n M_h \subseteq \mathfrak{q}^n M$  since this is a good filtration, therefore  $\ell(M/M_{n+h}) \geq \ell(M/\mathfrak{q}^n M)$ , therefore  $d' \geq d$ , hence  $d = d'$ . Similarly, the argument above implies  $a_0 \geq b_0$  and  $b_0 \geq a_0$ , so  $a_0 = b_0$ .

This implies  $\Delta^d(P_{\bar{q}}(M, n)) = \Delta^d(P_{\bar{q}}((M_n), n)) = a_0 \cdot d!$ .

- Consider

$$0 \longrightarrow M_n/\mathfrak{q}^n M \longrightarrow M/\mathfrak{q}^n M \longrightarrow M/M_n \longrightarrow 0$$

therefore  $\ell(M/\mathfrak{q}^n M) = \ell(M/M_n) + \ell(M_n/\mathfrak{q}^n M)$ . Let  $R(n) = \ell(M_n/\mathfrak{q}^n M)$ , then  $P_{\bar{q}}(M, n) = P_{\bar{q}}(M_n, n) + R(n)$ , therefore the degree of  $R(n)$  is less than  $d$ , the degree of  $P_{\bar{q}}(M, n)$ , and by definition of  $R(n)$ , the coefficient of the leading term of  $R(n)$  is non-negative.  $\square$

**Definition 3.23** (Hilbert-Samuel Polynomial). Let  $A$  be a Noetherian ring,  $\mathfrak{q}$  be an ideal of  $A$ ,  $M$  be a finitely-generated  $A$ -module, with  $\ell(M/\mathfrak{q}M) < \infty$ , then  $P_{\bar{q}}(M, n)$  is called the Hilbert-Samuel polynomial of  $M$  with respect to  $\mathfrak{q}$ . We define the degree of  $P_{\bar{q}}(M, n) = a_0 n^d + a_1 n^{d-1} + \dots$  to be  $d$ , then  $\Delta^d(P_{\bar{q}}(M, n)) = d!a_0$  is called the Hilbert-Samuel multiplicity of  $M$  with respect to  $\mathfrak{q}$ .

**Proposition 3.24.** Let  $A$  be a Noetherian ring,  $\mathfrak{q}$  be an ideal of  $A$ ,  $M$  be a finitely-generated  $A$ -module, with  $\ell(M/\mathfrak{q}M) < \infty$ . Let  $\mathfrak{q}'$  be another ideal of  $A$  such that  $\ell(M/\mathfrak{q}'M) < \infty$ . Suppose  $\text{supp}(M/\mathfrak{q}M) = \text{supp}(M/\mathfrak{q}'M)$ , then the degree of  $P_{\bar{q}}(M, n)$  equals to the degree of  $P_{\bar{q}'}(M, n)$ .

*Proof.* Let  $I = \text{Ann}_A(M)$ . Recall that

$$\begin{aligned} \text{supp}(M/\mathfrak{q}M) &= A/\mathfrak{q} \otimes_A M \\ &= \text{supp}(A/\mathfrak{q}) \cap \text{supp}(M) \\ &= \text{supp}(A/\mathfrak{q}) \cap \text{supp}(A/I) \\ &= \text{supp}(A/\mathfrak{q} \otimes A/I) \\ &= \text{supp}(A/\mathfrak{q} + I), \end{aligned}$$

then similarly  $\text{supp}(M/\mathfrak{q}'M) = \text{supp}(A/(\mathfrak{q}' + I))$ . Since  $I = \text{Ann}_A(M)$ , then  $IM = 0$ , so we can assume  $M$  to be an  $A/I$ -module, that is,  $M$  is an  $A$ -module such that  $\text{Ann}_A(M) = 0$ . In that case, then  $\text{supp}(M/\mathfrak{q}M) = \text{supp}(A/\mathfrak{q})$  and  $\text{supp}(M/\mathfrak{q}'M) = \text{supp}(A/\mathfrak{q}')$ . Recall that  $\ell(M/\mathfrak{q}M) < \infty$ , so  $\text{supp}(A/\mathfrak{q})$  consists of maximal ideals only. (Since it is Artinian, there are finitely many of them.) Similarly,  $\ell(M/\mathfrak{q}'M) < \infty$ , so  $\text{supp}(A/\mathfrak{q}')$  consists of maximal ideals only as well. In particular,  $\text{supp}(A/\mathfrak{q})$  is the set of prime ideals containing  $\mathfrak{q}$ , and  $\text{supp}(A/\mathfrak{q}')$  is the set of prime ideals containing  $\mathfrak{q}'$ , but they are the same, so the radicals agree, i.e.,  $\sqrt{\mathfrak{q}} = \sqrt{\mathfrak{q}'}$ . Since  $A$  is Noetherian, then  $\mathfrak{q}^r \subseteq \mathfrak{q}'$  for some  $r > 0$  and  $\mathfrak{q}'^{r'} \subseteq \mathfrak{q}$  for some  $r' > 0$  as well.

**Claim 3.25.** The degree of  $P_{\bar{q}}(M, n)$  equals to the degree of  $P_{\bar{q}^r}(M, n)$ .

*Subproof.* If we write  $P_q(M, n) = a_0 n^d + \dots$ , with lower degree terms, and  $P_{q^r}(M, n) = \ell(M/q^{rn}M) = P_q(M, rn) = a_0(rn)^d + \dots = a_0 r^d \cdot n^d + \dots$ , with lower degree terms. Therefore, the degree of  $P_q(M, n)$  is the degree of  $P_{q^r}(M, n)$ , and the degree of  $P_{q^r}(M, n)$  is the degree of  $P_{q^{r'}}(M, n)$ . ■

Recall that  $q^r \subseteq q'$  for some  $r > 0$  and  $q^{r'} \subseteq q$  for some  $r' > 0$ , therefore the degree of  $P_q(M, n)$  is at least the degree of  $P_{q'}(M, n)$ , and the degree of  $P_{q'}(M, n)$  is at least the degree of  $P_q(M, n)$ , therefore the degree of  $P_q(M, n)$  is the degree of  $P_{q'}(M, n)$ . □

**Remark 3.26.** If  $\ell(M/qM) < \infty$ , then we can assume that  $\text{Ann}_A(M) = q$ . Therefore,  $\text{supp}(M/qM) = \text{supp}(A/q)$ , consists of maximal ideals only.

If we write  $q = I_1 \cap I_2 \cap \dots \cap I_r$  where each  $I_i$  is  $\mathfrak{m}_i$ -primary for maximal ideal  $\mathfrak{m}_i$ . By the Chinese Remainder Theorem, we have  $q = I_1 I_2 \dots I_r$ . Thus,  $q^n M = I_1^n I_2^n \dots I_r^n M$ , and  $A/q \cong A/I_1 \oplus \dots \oplus A/I_r$ , and so  $A/q^n = A/I_1^n \oplus \dots \oplus A/I_r^n$ . Therefore,  $I_i = q A_{\mathfrak{m}_i}$ , and  $M/q^n M \cong \bigoplus_i M/I_i^n M$  by tensoring  $M$ . Therefore,  $P_q(M, n) = \sum_i P_{q A_{\mathfrak{m}_i}}(M_{\mathfrak{m}_i}, n)$ . Therefore, it suffices to understand the Hilbert-Samuel polynomials in the local case (assuming  $M/qM$  has finite length).

**Proposition 3.27.** Let  $A$  be Noetherian,  $q$  be an ideal. Consider the short exact sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow T \longrightarrow 0$$

of finitely-generated  $A$ -modules. Suppose  $\ell(M/qM) < \infty$ , (so  $\ell(T/qT)$  and  $\ell(N/qN)$  are also finite,) then  $P_q(M, n) = P_q(T, n) + P_q(N, n) - R(n)$ , where  $R(n)$  is an essentially polynomial of degree less than degree of  $P_q(N, n)$ , and the leading term of  $R(n)$  has non-negative coefficient.

*Proof.* Consider

$$0 \longrightarrow N/(N \cap q^n M) \longrightarrow M/q^n M \longrightarrow T/q^n T \longrightarrow 0$$

The corresponding filtrations  $\{N_n = N \cap q^n M\}$  and  $\{q^n N\}$  are  $q$ -good. By Corollary 3.22,  $P_q(N, n) = P_q(N_n, n) + R(n)$ . From the short exact sequence above,  $P_q(M, n) = P_q(T, n) + P_q(N_n, n)$ , thus  $\ell(M/q^n M) = \ell(T/q^n T) + \ell(N/N_n)$ , so one can write  $P_q(M, n) = P_q(T, n) + P_q(N, n) - R(n)$  with  $R(n)$  as specified above. □

### 3.2 DIMENSION OVER ZARISKI TOPOLOGY

**Definition 3.28** (Zariski Topology). Let  $A$  be a commutative ring, then the Zariski spectrum is the set  $\text{Spec}(A) = \{P \mid P \text{ is a prime ideal in } A\}$ . This becomes a topological space  $X = \text{Spec}(A)$  with the following (Zariski) topology: we declare the closed sets of  $X$  to be  $V(I) = \{P \in \text{Spec}(A) \mid P \supseteq I\}$ , i.e., the vanishing set of an ideal  $I$ .

**Exercise 3.29.** •  $\bigcap_{i \in I} V(I_i) = V(\sum_{i \in I} I_i)$ ,

•  $V(I) \cup V(J) = V(I \cap J) = V(IJ)$ .

If  $I = (f_i)_{i \in I}$ , then  $V(I) = V(\sum_{i \in I} A f_i) = \bigcap_{i \in I} V(f_i)$ , so  $X \setminus V(I) = X \setminus \bigcap_{i \in I} V(f_i) = \bigcup_{i \in I} (X \setminus V(f_i)) = \bigcup_{i \in I} D(f_i)$ , where we define  $D(f_i) = X \setminus V(f_i) = \{p \in \text{Spec}(A) \mid f_i \notin p\}$ . Therefore,  $\{D(f_i)\}$  forms a family of basic open subsets of  $X$ . Therefore,  $D(f_i)$  corresponds to  $\text{Spec}(A_{f_i})$ .

**Exercise 3.30.** Let  $Y \subseteq X$  be a subset, then  $\bar{Y} = V(I)$  where  $I = \bigcap_{p \in Y} p$ . Therefore,  $V(I) = V(\sqrt{I})$ . In particular,

$V(I) \subsetneq V(J)$  if and only if  $\sqrt{J} \subsetneq \sqrt{I}$ . One can check that there exists a one-to-one inclusion-reversing correspondence between closed subsets of  $X$  and radical ideals of  $A$ .

**Exercise 3.31.**  $[p] \in X$  is a closed point if and only if  $p$  is a maximal ideal of  $A$ . In particular, the spectrum as a topological space is non-Hausdorff.

**Definition 3.32** (Irreducible Subset). Let  $X$  be a topological space and  $Y \subseteq X$  be a subset. Then  $Y$  is called irreducible if  $Y$  cannot be expressed as a union of two proper closed subsets of  $Y$ .

**Exercise 3.33.** •  $Y$  is irreducible if and only if any two non-empty open subsets of  $Y$  has a non-empty intersection.

•  $Y$  being irreducible implies  $\bar{Y}$  irreducible.

**Example 3.34.** Let  $X = \text{Spec}(A)$  be a topological space and  $Y$  be a closed subset of  $X$ , with  $Y = V(I)$ . Then  $Y$  is irreducible if and only if  $\sqrt{I}$  is a prime ideal of  $A$ .

Therefore, we have an increasing sequence of closed subsets  $Y_0 \subsetneq Y_1 \subsetneq Y_2 \subsetneq \cdots \subseteq Y_r$  in  $X = \text{Spec}(A)$  if and only if  $P_r \subsetneq P_{r-1} \subsetneq \cdots \subsetneq P_0$  for  $V(P_i) = Y_i$  for all  $0 \leq i \leq r$ .

**Remark 3.35.** • Let  $X$  be a topological space and let  $\mathcal{F}$  be the family of irreducible closed subsets  $Y$  of  $X$ , then  $\mathcal{F}$  has a maximal element. Let  $Y_0 \subseteq Y_1 \subseteq Y_2 \subseteq \cdots$  be an increasing chain of irreducible closed subsets, then one can check that  $Y = \bigcup_{i \geq 0} Y_i$  is irreducible and closed. By Zorn's lemma, there exists a maximal element of  $\mathcal{F}$ .

- For any  $x \in X$ ,  $\{x\}$  irreducible does not imply  $\overline{\{x\}}$  irreducible. (In contrast, in Hausdorff spaces, every singleton set is closed.)

**Definition 3.36** (Component). A maximal irreducible closed subset of a space  $X$  is called a component of  $X$ . Therefore, a space  $X$  is the union of its components.

**Definition 3.37** (Noetherian). Let  $X$  be a topological space, then  $X$  is Noetherian if

- (i) every non-empty of open subsets of  $X$  has a maximal element, or equivalently,
- (ii) every non-empty of closed subsets of  $X$  has a minimal element.

**Remark 3.38.** (i) If  $X$  is Noetherian, then any subset  $Y$  of  $X$  is Noetherian as well.

- (ii) Conversely, if  $X = \bigcup_{i=1}^n X_i$  where each  $X_i$  is Noetherian, then  $X$  is Noetherian.

- (iii) If  $X$  is Noetherian, then every subset of  $X$  is quasi-compact.

**Example 3.39.** If  $A$  be a Noetherian ring, then  $\text{Spec}(A)$  is Noetherian. The converse is not necessarily true.

**Remark 3.40.** Suppose  $A$  is Noetherian, then  $(0) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$  where  $\mathfrak{q}_i$  is  $P_i$ -primary. Let  $\{P_1, \dots, P_t\} = \min\{P_1, \dots, P_r\}$  be the minimal primes, then  $\text{Spec}(A) = V(0) = V(\mathfrak{q}_1) \cup \cdots \cup V(\mathfrak{q}_r)$ , but since  $\mathfrak{q}_i$  is  $P_i$ -primary for all  $i$ , then  $V(\mathfrak{q}_i) = V(P_i)$ , so  $P_i = \text{Ass}(A/\mathfrak{q}_i) = V(P_1) \cup \cdots \cup V(P_r)$ . But if  $P_i \subsetneq P_j$ , then  $V(P_j) \subsetneq V(P_i)$ , so the union is just  $V(P_1) \cup \cdots \cup V(P_t)$ , where each  $V(P_i)$  is a component of  $\text{Spec}(A)$  for  $1 \leq i \leq t$ .

**Proposition 3.41.** A Noetherian space  $X$  has finite components, i.e.,  $X = X_1 \cup \cdots \cup X_n$  is a finite union.

*Proof.* Let  $\mathcal{F}$  be the collection of closed subsets  $Z$  of  $X$  for which the proposition is not true, that is, each  $Z$  is a finite union of its components. Suppose, towards contradiction, that  $\mathcal{F}$  is non-empty. Since  $X$  is Noetherian, then there exists a minimal element  $Z_0$  of  $\mathcal{F}$ , therefore  $Z_0$  is not irreducible, otherwise  $Z_0 \notin \mathcal{F}$ , so  $Z_0 = W_0 \cup V_0$  is the union of two proper closed subsets. By minimality  $W_0, V_0 \notin \mathcal{F}$ , therefore  $W_0$  and  $V_0$  should be the finite union of their (finitely many) irreducible components, but that means  $\mathcal{F}$  is also a finite union of irreducible components, contradiction.  $\square$

**Definition 3.42** (Dimension). Let  $X$  be a topological space, then the dimension of  $X$ , denoted  $\dim(X)$ , is defined as

$$\dim(X) = \sup\{r \mid \text{there exists a decreasing chain of irreducible closed subsets } X_r \supsetneq X_{r-1} \supsetneq \cdots \supsetneq X_1 \supsetneq X_0\}.$$

**Exercise 3.43.** Let  $A$  be a commutative ring,  $X = \text{Spec}(A)$ . Show that  $X$  is quasi-compact, i.e., every open cover has a finite subcover.

**Definition 3.44** (Dimension). Let  $A$  be a commutative ring and  $X = \text{Spec}(A)$ , then

$$\dim(X) = \sup\{r \mid \text{there exists an increasing chain of prime ideals } P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_r\}.$$

This follows from the definition above.

**Definition 3.45** (Krull Dimension). The Krull dimension of a commutative ring  $A$ , denoted  $\dim(A)$ , is  $\dim(\text{Spec}(A))$ .

**Remark 3.46.** For any space  $X$ ,  $\dim(X) = \sup_i \dim(X_i)$  where each  $X_i$  is a component of  $X$ .

**Remark 3.47.** Let  $A$  be a commutative ring,  $X = \text{Spec}(A)$ , then

$$\dim(X) = \sup\{\dim(A/P_i) \mid P_1, \dots, P_t \text{ are minimal prime ideals of } A\}.$$

**Remark 3.48** (Nagata). There exists Noetherian rings  $A$  such that  $\dim(A) = \infty$ .

**Definition 3.49** (Krull Dimension). Let  $A$  be a Noetherian ring (this would probably be the implicit assumption from now on) and let  $M$  be an  $A$ -module, then the Krull dimension of  $M$  is  $\dim(M) = \dim(A/I)$  where  $I = \text{Ann}_A(M)$ .

**Exercise 3.50.**  $\dim(M) = \sup_{\mathfrak{m}}(\dim(M_{\mathfrak{m}}))$  where  $\mathfrak{m}$  is a maximal ideal. Note that now the dimension of  $M$  can be studied locally. This is similar to the case of studying the degree of  $P_{\mathfrak{q}}(M, n)$ , where  $\text{supp}(\mathfrak{q} + I) = \{\mathfrak{m}_1, \dots, \mathfrak{m}_n\}$  we just need to study  $P_{\mathfrak{q}A_{\mathfrak{m}}}(M_{\mathfrak{m}}, n)$  for maximal ideals  $\mathfrak{m}$  in the support.

**Definition 3.51** (Length). Let  $(A, \mathfrak{m})$  be a local ring, i.e.,  $A$  is Noetherian with a unique maximal ideal  $\mathfrak{m}$ , and let  $M$  be a finitely-generated  $A$ -module. We denote the length  $s(M) = \inf\{n \mid \exists x_1, \dots, x_n \in \mathfrak{m} \text{ such that } \ell(M/(x_1, \dots, x_n)M) < \infty\}$ . Note that since  $M$  is finitely-generated, then  $\dim_{A/\mathfrak{m}}(M/\mathfrak{m}M) < \infty$ , so  $s(M)$  is always finite.

**Definition 3.52** (System of Parameters). We say  $x_1, \dots, x_r \in \mathfrak{m}$  is a system of parameters of  $M$  if  $r = s(M)$  and  $\ell(M/(x_1, \dots, x_r)M) < \infty$ .

Let  $(A, \mathfrak{m})$  be a local ring,  $M$  be a finitely-generated  $A$ -module, then we denote  $d(M) = \deg(P_{\mathfrak{m}}(M, n))$

**Remark 3.53.** For Noetherian ring  $A$  (but not necessarily quasi-local), we have  $\dim(A) = \sup(\dim(A_{\mathfrak{m}}))$  and  $d(M) = \sup(d(M_{\mathfrak{m}}))$ .

**Theorem 3.54** (Dimension Theorem). Let  $(A, \mathfrak{m})$  be a local ring,  $M$  be a finitely-generated  $A$ -module, then  $\dim(M) = d(M) = s(M)$ .

*Proof.* We will show that  $\dim(M) \leq d(M) \leq s(M) \leq \dim(M)$ .

- To show  $\dim(M) \leq d(M)$ , we will induct on  $d(M)$ . If  $d(M) = 0$ , then  $P_{\mathfrak{m}}(M, n) = \ell(M/\mathfrak{m}^n M)$ , and since  $d(M) = 0$  is the degree of  $P_{\mathfrak{m}}(M, n)$ , then  $\ell(M/\mathfrak{m}^n M) = \ell(M/\mathfrak{m}^{n+1} M) = \dots$ , therefore  $\ell(\mathfrak{m}^n M/\mathfrak{m}^{n+1} M) = 0$ , hence we have a short exact sequence

$$0 \longrightarrow \mathfrak{m}^n M/\mathfrak{m}^{n+1} M \longrightarrow M/\mathfrak{m}^{n+1} M \longrightarrow M/\mathfrak{m}^n M \longrightarrow 0$$

therefore  $\mathfrak{m}^n M/\mathfrak{m}^{n+1} M = 0$ , so  $\mathfrak{m}^n M = \mathfrak{m}^{n+1} M = \mathfrak{m}(\mathfrak{m}^n M)$ , then by Nakayama Lemma ([Corollary 2.55](#)), we have  $\mathfrak{m}^n M = 0$ , so  $\text{supp}(M) = \{\mathfrak{m}\}$ . Therefore,  $\dim(M) = 0$ .

Now suppose  $d(M) > 0$ , and we have shown the case for dimension  $0, \dots, d(M) - 1$ . Since  $(A, \mathfrak{m})$  is local, then it has finitely many components. Let  $P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_n$  be a chain of prime ideals in  $\text{supp}(M)$  such that  $P_0$  is a minimal prime ideal in  $\text{supp}(M)$ . We need to show that  $n \leq d(M)$ . Denote  $N = A/P_0$  and take  $x \in P_1 \setminus P_0$ , then  $x$  is a non-zero-divisor of  $N$ , therefore

$$0 \longrightarrow N \xrightarrow{x} N \longrightarrow N/xN \longrightarrow 0$$

is a short exact sequence. By [Proposition 3.27](#),  $d(N/xN) \leq d(N) - 1$ . By the inductive hypothesis,  $\dim(N/xN) \leq d(N/xN) \leq d(N) - 1$ , then note that  $N/xN = A/(P_0 + x_1 A)$ , so  $P_0 + x_1 A \subseteq P_1 \subseteq P_2 \subseteq \dots \subseteq P_n$ , therefore  $n - 1 \leq \dim(N/xN) \leq d(N/xN) \leq d(N) - 1$ , therefore  $n \leq d(N) \leq d(M)$ .

- To show  $d(M) \leq s(M)$ , let  $x_1, \dots, x_n$  be a system of parameters of  $M$ , i.e.,  $n = s(M)$  and  $\ell(M/(x_1, \dots, x_n)M) < \infty$ . This implies  $\deg(P_{(x_1, \dots, x_n)}(M, n)) \leq n$ , but  $V(M/(x_1, \dots, x_n)M) = V(M/\mathfrak{m}M)$ , therefore we have  $\text{supp}(M/(x_1, \dots, x_n)M) = \{\mathfrak{m}\} = \text{supp}(M/\mathfrak{m}M)$ , thus by [Proposition 3.24](#) we conclude  $\deg(P_{\mathfrak{m}}(M, n)) = \deg(P_{(x_1, \dots, x_n)}(M, n))$ , so  $d(M) \leq s(M) = n$ .
- To show  $s(M) \leq \dim(M)$ , we proceed by induction on  $\dim(M)$ . If  $\dim(M) = 0$ , then  $\text{supp}(M) = \{\mathfrak{m}\}$ , so  $\ell_A(M) < \infty$ , therefore  $s(M) = 0$ . Let  $\{P_1, \dots, P_r\}$  be the minimal primes of  $\text{supp}(M)$ . Take  $x \in \mathfrak{m} \setminus \bigcup_{i=1}^r P_i$ , then  $s(M) - 1 \leq s(M/xM) \leq \dim(M/xM) \leq \dim(M - 1)^8$ , hence  $s(M) \leq \dim(M)$ .

<sup>8</sup>The first inequality follows from definition, and the second inclusion follows from the inductive hypothesis.

□

**Remark 3.55.** If  $A$  is a PID, then every prime has height 1, therefore  $\dim(A) = 1$ . For instance,  $\dim(\mathbb{Z}) = \dim(k[x]) = 1$ . For  $A = k[x_1, \dots, x_n]$ , we have  $(x_1, \dots, x_n) \supseteq (x_1, \dots, x_{n-1}) \supseteq \dots \supseteq (x_1) \supseteq (0)$ , so  $\dim(A) \geq n$ .

**Corollary 3.56.** Let  $(A, \mathfrak{m})$  be a local ring with  $M$  a finitely-generated  $A$ -module, then  $\dim_A(M) = \dim_{\hat{A}}(\hat{M})$ .

*Proof.* Note  $\dim_A(M) = d(M) = \deg(P_{\mathfrak{m}}(M, n))$ ,  $P_{\mathfrak{m}}(M, n) = \ell(M/\mathfrak{m}^n M)$ ; similarly  $\dim_{\hat{A}}(\hat{M}) = d(\hat{M}) = \deg(P_{\hat{\mathfrak{m}}}(\hat{M}, n)) = \ell(\hat{M}/\hat{\mathfrak{m}}^n \hat{M})$ , therefore  $M/\mathfrak{m}^n M \cong \hat{M}/\hat{\mathfrak{m}}^n \hat{M}$ . □

**Corollary 3.57.** Let  $(A, \mathfrak{m})$  be a local ring, then  $\dim(A)$  is the minimal number of elements required to generate an  $\mathfrak{m}$ -primary ideal.

*Proof.* Note  $\dim(A) = s(A)$  is the minimal number  $n$  such that  $x_1, \dots, x_n \in \mathfrak{m}$  gives  $\ell(A/(x_1, \dots, x_n)) < \infty$ . Since  $s(A) = d$ , then there exists  $x_1, \dots, x_d$  such that  $\ell(A/(x_1, \dots, x_d)) < \infty$ , so  $\{\mathfrak{m}\} = \text{Ass}_A(A/(x_1, \dots, x_d))$ , i.e.,  $(x_1, \dots, x_d)$  is  $\mathfrak{m}$ -primary. □

**Corollary 3.58.** Let  $A$  be Noetherian, any descending chain of prime ideals must stop after a finite number of steps.

*Proof.* Take a descending chain  $P = P_0 \supseteq P_1 \supseteq P_2 \supseteq \dots$ , then taking the localization at  $P$ , we have  $PA_P \supseteq P_1 A_P \supseteq P_2 A_P \supseteq \dots$  in  $A_P$ . But  $A_P$  is a local ring with maximal ideal  $PA_P$ , therefore  $\dim(A_P) < \infty$ , so there exists some  $r > 0$  such that  $P_r A_P = P_{r+1} A_P = \dots$ . This implies  $P_r = P_{r+1} = \dots$ , by pulling back via  $i_P : A \rightarrow A_P$ . (One needs to check that  $i_P^{-1}(P_r A_P) = P_r$ .) □

**Definition 3.59** (Height). Let  $A$  be Noetherian,  $P \subseteq A$  be a prime ideal. The height of  $P$ , denoted  $\text{ht}(P)$ , is  $\dim(A_P)$ . Alternatively, it is  $\sup\{r \mid \exists \text{ a chain of prime ideals } P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_r \subsetneq P_r = P\}$ .

Let  $I$  be an ideal of  $A$ , then  $\text{ht}(I) = \inf_{P \supseteq I} \text{ht}(P) = \inf_{\text{minimal } P \supseteq I} \text{ht}(P)$ . By the primary decomposition, if we write down  $I = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_r$  with minimal primes  $P_1, \dots, P_r$ , then this is just  $\inf_{\text{minimal primes } P_i} \text{ht}(P_i)$  in a primary decomposition of  $I$ .

**Corollary 3.60** (Generalized Krull's Principal Ideal Theorem). Let  $A$  be a Noetherian ring and  $P$  be a prime ideal, then  $\text{ht}(P) \leq n$  if and only if there exists  $a_1, \dots, a_n \in P$  such that  $P$  contains  $(a_1, \dots, a_n)$  minimally.

*Proof.* ( $\Rightarrow$ ): note that  $\text{ht}(P) \leq n$  if and only if  $\dim(A_P) \leq n$ , which implies  $s(A_P) \leq n$ . Let  $\frac{a_1}{1}, \dots, \frac{a_d}{1}$  be a system of parameters for  $A_P$  where  $d \leq n$ . Therefore,  $\text{Ass}_{A_P}(A_P/(a_1, \dots, a_d)A_P) = PA_P$ , that is,  $PA_P$  contains  $(a_1, \dots, a_d)_{A_P}$  minimally. This implies  $P \supseteq (a_1, \dots, a_d)$  minimally.

( $\Leftarrow$ ): suppose  $P \supseteq (a_1, \dots, a_n)$  minimally, then  $PA_P \supseteq (a_1, \dots, a_n)A_P$  minimally, therefore we have  $PA_P = \text{Ass}_{A_P}(A_P/(a_1, \dots, a_n)A_P)$ , therefore  $\ell(A_P/(a_1, \dots, a_n)A_P) < \infty$ , thus  $\dim(A_P) \leq n$ . □

**Exercise 3.61.** Let  $(A, \mathfrak{m})$  be a local ring. Suppose there exists a principal prime ideal  $P$ , then  $A$  is a domain.

**Exercise 3.62.** Let  $A$  be a Noetherian ring with  $\dim(A) \geq 2$ . Show that  $A$  has infinitely many prime ideals of height 1.

**Exercise 3.63.** Let  $(A, \mathfrak{m})$  be a local ring and  $M$  be a finitely-generated  $A$ -module. Let  $x_1, \dots, x_i \in \mathfrak{m}$ , then show that  $\dim(M/(x_1, \dots, x_i)) \geq \dim(M) - i$ . The equality holds if and only if  $x_1, \dots, x_i$  form a part of a system of parameters of  $M$ .

**Theorem 3.64.** Let  $A$  be a Noetherian ring, then  $\dim(A[x]) = \dim(A) + 1$ .

*Proof.* First, we need two lemmas.

**Lemma 3.65.** Let  $\mathfrak{p} \supsetneq \mathfrak{q}$  be two prime ideals in  $A[x]$  such that  $\mathfrak{q}_0 = \mathfrak{q} \cap A = P \cap A$ , then  $\mathfrak{q} = \mathfrak{q}_0[x]$ .

**Remark 3.66.** In particular, this implies there is no prime ideal between  $\mathfrak{p}$  and  $\mathfrak{q}$ . Otherwise, say  $\mathfrak{p} \supsetneq \mathfrak{q}' \supsetneq \mathfrak{q}$ , then  $\mathfrak{q}' = \mathfrak{q}_0[x]$ , so  $\mathfrak{q} = \mathfrak{q}'$ .



*Subproof.* Suppose, towards contradiction, that  $\mathfrak{q}_0[x] \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$ , then  $\bar{A} := A/\mathfrak{q}_0 \rightarrow A/\mathfrak{q}_0[x] = A[x]/\mathfrak{q}_0[x] = \bar{A}[x]$ . Now  $\bar{A}[x]$  has a strict chain:

$$\bar{0} \subseteq \bar{\mathfrak{q}} \subseteq \bar{\mathfrak{p}}$$

where  $\bar{\mathfrak{q}}$  is the image of  $\mathfrak{q}$  in  $\bar{A}[x]$  and  $\bar{\mathfrak{p}}$  is the image of  $\mathfrak{p}$  in  $\bar{A}[x]$ . Also note that  $(\bar{0}) = (\bar{0}) \cap \bar{A} = \bar{\mathfrak{q}} \cap \bar{A} = \bar{\mathfrak{p}} \cap \bar{A}$ . Let  $k = S^{-1}\bar{A}$  for  $S = \bar{A} \setminus \{0\}$ , then by tensoring with  $\bar{A}$  on  $k \rightarrow k[x]$  (as  $\bar{A} \hookrightarrow \bar{A}[x]$  where  $S^{-1}\bar{A}$  is  $\bar{A}$ -flat), we have a strict chain

$$\bar{0} \subsetneq S^{-1}\bar{\mathfrak{q}} \subsetneq S^{-1}\bar{\mathfrak{p}}$$

of length 2. Therefore  $\dim(k[x]) \geq 2$ , but  $\dim(k[x]) = 1$ , contradiction. Therefore  $\mathfrak{q} = \mathfrak{q}_0[x]$ . ■

**Lemma 3.67.** Let  $A$  be a Noetherian ring and  $I$  be an ideal, then  $\text{ht}(I) = \text{ht}(I[x])$ .

*Subproof.* We have  $I = \inf_{P \supseteq I} \text{ht}(P) = \inf_{\text{minimal } P \supseteq I} \text{ht}(P)$  and  $I[x] = \inf_{A[x] \supseteq \mathfrak{q} \supseteq I[x]} \text{ht}(\mathfrak{q}) = \inf_{\text{minimal } P[x] \supseteq I[x]} \text{ht}(P)$ , therefore it is enough to show that  $\text{ht}(P) = \text{ht}(P[x])$ .

Given any chain  $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_r = P$ , then  $P_0[x] \subsetneq P_1[x] \subsetneq \cdots \subsetneq P_r[x] = P[x]$ . This says  $\text{ht}(P[x]) \geq \text{ht}(P)$ . Also, suppose  $\text{ht}(P) = t$ , then there exists  $a_1, \dots, a_t \in P$  such that  $P \supseteq (a_1, \dots, a_t)$  minimally. By the primary decomposition, we know  $P[x] \supseteq (a_1, \dots, a_t)[x]$  minimally, then  $\text{ht}(P[x]) \leq t = \text{ht}(P)$ , thus  $\text{ht}(P) = \text{ht}(P[x])$ . ■

Suppose  $\dim(A) = \infty$ , then take a strict chain of prime ideals in  $A$ , i.e.,  $P_0 \subsetneq \cdots \subsetneq P_r$ , so  $P_0[x] \subsetneq \cdots \subsetneq P_r[x]$  is also a strict chain in  $A[x]$ , so  $\dim(A[x]) = \infty$ .

Now suppose  $\dim(A) < \infty$ . Take any chain  $P_0 \subsetneq \cdots \subsetneq P_r$ , then we have another chain  $P_0[x] \subsetneq P_1[x] \subsetneq \cdots \subsetneq P_r[x] \subsetneq (P_r[x], x)$ , so  $\dim(A[x]) \geq \dim(A) + 1$ . We now proceed by induction on  $\dim(A)$ . Suppose  $\dim(A) = 0$ , then it is equivalent to  $\ell_A(A) < \infty$ , i.e., all the associated primes of  $A$  are maximal. By Lemma 3.65,  $\dim(A) = 1$ .<sup>9</sup>

We now want to show that  $\dim(A[x]) \leq \dim(A) + 1$ . Take a strict chain of ideals in  $A[x]$  of any length (say  $r$ ), that is  $P_r \supsetneq \cdots \supsetneq P_1 \supsetneq P_0$ , then by intersecting with  $A$  we have another chain  $\mathfrak{p}_r \supsetneq \cdots \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_0$ , where  $\mathfrak{p}_i = P_i \cap A$ . We now want to show that  $r \leq \dim(A) + 1$ . We have two cases:

- suppose  $\mathfrak{p}_r \neq \mathfrak{p}_{r-1}$ , so  $\text{ht}(P_{r-1}) < \dim(A)$ . By induction,  $\dim(A_{\mathfrak{p}_{r-1}}[x]) = \dim(A_{\mathfrak{p}_{r-1}}) + 1$ , so  $\dim(A_{\mathfrak{p}_{r-1}}[x]) \leq \dim(A)$ , and by localization we have a chain  $A_{\mathfrak{p}_{r-1}}[x] \supsetneq P_{r-1}A_{\mathfrak{p}_{r-1}}[x] \supsetneq \cdots \supsetneq P_0A_{\mathfrak{p}_{r-1}}[x]$ , therefore  $r - 1 \leq \dim(A_{\mathfrak{p}_{r-1}}[x]) \leq \dim(A)$ , so  $r \leq \dim(A) + 1$ .
- suppose  $\mathfrak{p}_r = \mathfrak{p}_{r-1}$ , so  $P_{r-1} = \mathfrak{p}_{r-1}[x]$  by Lemma 3.65, with  $\text{ht}(P_{r-1}) = \text{ht}(\mathfrak{p}_{r-1})$ . Therefore,  $r - 1 \leq \text{ht}(P_{r-1}) = \text{ht}(P_{r-1}) \leq \dim(A)$ , so  $r \leq \dim(A) + 1$ .

□

**Corollary 3.68.** • Let  $A$  be a Noetherian ring, then  $\dim(A[x_1, \dots, x_n]) = \dim(A) + n$ .

- Let  $k$  be a field, then  $\dim(k[x_1, \dots, x_n]) = n$ .
- $\dim(\mathbb{Z}[x_1, \dots, x_n]) = n + 1$ .

**Exercise 3.69.** Let  $A$  be a Noetherian ring, then  $\dim(A[[x]]) = \dim(A) + 1$ .

*Hint:* is  $X$  contained in the Jacobson radical of  $A[[x]]$ ?

**Corollary 3.70.** • For a Noetherian ring  $A$ ,  $\dim(A[[x]]) = \dim(A) + n$ .

- For a field  $k$ ,  $\dim(k[[x]]) = n$ .
- $\dim(\mathbb{Z}[[x_1, \dots, x_n]]) = n + 1$ .

**Remark 3.71.** For rings like  $k[x_1, \dots, x_n]$ , the dimension and the transcendental degree are both  $n$ . For rings like  $k[[x]]$ , the degree is still  $n$ , but the transcendental degree is  $\infty$ .

<sup>9</sup>Indeed, take the primary decomposition  $0 = I_1 \cap \cdots \cap I_r$  where  $I_i$  is  $\mathfrak{m}_i$ -primary, then pushing it out to the polynomial ring, we have  $0 = I_1[x] \cap \cdots \cap I_r[x]$ , where  $I_r[x]$  is  $\mathfrak{m}_i[x]$ -primary. Take the chain given by  $P = (\mathfrak{m}_1[x], x) \supsetneq \mathfrak{m}_1[x]$ , but they both collapse onto  $\mathfrak{m}_1$ , so by Lemma 3.65 this is the maximal chain, thus has length 1.

**Remark 3.72.** If  $f : A \rightarrow B$  is a ring homomorphism, then

$$\begin{aligned}\mathrm{Spec}(f) : \mathrm{Spec}(B) &\rightarrow \mathrm{Spec}(A) \\ [p] &\mapsto [f^{-1}(p)]\end{aligned}$$

is a continuous map with respect to the Zariski topology.

**Exercise 3.73.**  $\mathrm{im}(\mathrm{Spec}(f)(\mathrm{Spec}(B)))$  is dense in  $\mathrm{Spec}(A)$  if and only if  $f^{-1}(0)$  consists of nilpotent elements in  $A$ .

## 4 INTEGRAL EXTENSIONS

## 4.1 GOING-UP AND GOING-DOWN

**Definition 4.1** (Integral). Let  $A \hookrightarrow B$  be an inclusion of commutative rings, sending multiplicative identity to multiplicative identity. An element  $0 \neq x \in B$  is called integral over  $A$  if  $x$  satisfies a monic equation  $x^n + a_1x^{n-1} + \cdots + a_n = 0$  for  $a_i \in A$ . If every element of  $B$  is integral over  $A$ , we say  $B$  is integral over  $A$ .

**Proposition 4.2.** Suppose  $A \hookrightarrow B$ , and let  $x \in B$ , then the following are equivalent:

- (i)  $x$  is integral over  $A$ ;
- (ii)  $A[x]$  is a finitely-generated  $A$ -module;
- (iii)  $A[x] \subseteq C$ , a subring of  $B$ , such that  $C$  is a finitely-generated  $A$ -module.
- (iv) There exists an  $A[x]$ -submodule  $M$  of  $B$  such that  $M$  is a finitely-generated  $A$ -module and  $M$  is faithful as an  $A[x]$ -module.

*Proof.* (i)  $\Rightarrow$  (ii): since  $x$  is integral over  $A$ , then we have  $x^n + a_1x^{n-1} + \cdots + a_n = 0$ , so  $x^n = -a_1x^{n-1} - \cdots - a_n$ , therefore  $x^{n+1} = -a_1x^n - \cdots - a_nx = -a_1(x^{n-1} + \cdots + a_n) - a_2x^{n-1} - \cdots$ , but this is a linear combination of the set  $\{1, x, \dots, x^{n-1}\}$  over  $A$ , hence  $A[x]$  is a finitely-generated  $A$ -module with generators  $1, x, \dots, x^{n-1}$ .

(ii)  $\Rightarrow$  (iii): take  $C = A[x]$ .

(iii)  $\Rightarrow$  (iv): take  $M = C$ .

(iv)  $\Rightarrow$  (i): let  $M$  be the said finitely-generated  $A$ -module, so we write  $m_1, \dots, m_n$  to be the generator of  $M$ . Since  $M$  is an  $A[x]$ -module, then we write

$$\begin{aligned} xm_1 &= a_{11}m_1 + \cdots + a_{1n}m_n \\ xm_2 &= a_{21}m_1 + \cdots + a_{2n}m_n \\ &\vdots \\ xm_n &= a_{n1}m_1 + \cdots + a_{nn}m_n \end{aligned}$$

and we write

$$\begin{aligned} (x - a_{11})m_1 - a_{12}m_2 - \cdots - a_{1n}m_n &= 0 \\ -a_{21}m_1 + (x - a_{22})m_2 - \cdots - a_{2n}m_n &= 0 \\ &\vdots \\ -a_{n1}m_1 - a_{n2}m_2 - \cdots + (x - a_{nn})m_n &= 0 \end{aligned}$$

then we can write it down as a matrix

$$M = \begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{pmatrix}$$

The following the same procedure as in [Proposition 2.53](#). We do cofactorization of  $x - a_{11}$  on the first row, cofactorization of  $-a_{21}$  on the second row, and so on, until we do cofactorization of  $-a_{n1}$  on the last row. By adding them together, we get  $\det(N) \cdot m_1 = 0$ , and similarly  $\det(N) \cdot m_n = 0$ , therefore  $\det(N) \cdot M = 0$ , but  $\det(N) \in A[x]$ , but  $M$  is faithful as an  $A[x]$ -module, so  $\det(N) = 0$  gives us a monic equation of degree  $n$  with respect to  $x$ , therefore  $x$  is integral over  $A$ .  $\square$

**Corollary 4.3.** Suppose  $A \hookrightarrow B$ . Suppose  $B = A[x_1, \dots, x_n]$ , we view this as an algebra generated by  $n$  elements, i.e., as  $A[X_1, \dots, X_n]/I$  for some ideal  $I$ . Suppose each  $x_i$  is integral over  $A$ , then  $B$  is integral over  $A$ .

*Proof.* We have

$$A \hookrightarrow A[x_1] \subseteq A[x_1, x_2] \subseteq \cdots \subseteq A[x_1, \dots, x_n] \hookrightarrow A[x_1, \dots, x_n]$$

where each extension is a finitely-generated module, then  $A[x_1, \dots, x_n]$  is a finitely-generated  $A$ -module. We can then apply [Proposition 4.2](#).  $\square$

**Corollary 4.4.** Suppose  $A \hookrightarrow B$ , and suppose  $b_1, b_2$  are integral elements over  $A$ , then  $b_1 \pm b_2$  and  $b_1 b_2$  are integral over  $A$ . If we write  $B'$  as the set of all elements in  $B$  that are integral over  $A$ , then  $B'$  is a subring of  $B$  that contains  $A$ , therefore  $B'$  is an  $A$ -subalgebra of  $B$ . Therefore,  $A[b_1, b_2]$  is a finitely-generated  $A$ -algebra.

**Definition 4.5** (Integral Closure, Integrally Closed).  $B'$  is called the integral closure of  $A$  in  $B$ . We say  $A$  is integrally closed in  $B$  if  $B' = B$ .

**Definition 4.6** (Integrally Closed). Let  $A$  be an integral domain. We say  $A$  is integrally closed if the integral closure of  $A$  in  $\text{Frac}(A)$  is  $A$  itself, i.e.,  $A$  is integrally closed in  $\text{Frac}(A)$ .

**Example 4.7.** Let  $A = k[x, y]/(y^2 = x^3)$  be a domain<sup>10</sup>, then we know  $\text{Frac}(A) \ni \left(\frac{y}{x}\right)^2 = x \in A$ , so  $\frac{y}{x} \in \text{Frac}(A)$ . Since  $\frac{y}{x}$  is integral over  $A$ , then  $A$  is not integrally closed.

**Exercise 4.8.** Let  $A$  be a UFD, then  $A$  is integrally closed.

**Exercise 4.9.** Suppose  $A \hookrightarrow B$  is an integral extension, let  $S$  be a multiplicatively closed subset of  $A$ , then  $S^{-1}A \hookrightarrow S^{-1}B$  is also an integral extension.

**Exercise 4.10.** Let  $A$  be an integral domain,  $A$  is integrally closed if and only if  $A_{\mathfrak{m}}$  is integrally closed for every maximal ideal  $\mathfrak{m}$  in  $A$ .

*Hint:* since  $A$  is an integral domain, then  $A$  is exactly the intersection of all  $A_{\mathfrak{m}}$ 's where  $\mathfrak{m}$  is a maximal ideal of  $A$ .

**Corollary 4.11.** Let  $A \hookrightarrow B \hookrightarrow C$  be a composition of integral extensions, then  $A \hookrightarrow C$  is also an integral extension.

*Proof.* For  $c \in C$ , we have  $c^n + b_1 c^{n-1} + \cdots + b_n = 0$  for  $b_i \in B$  to be integral over  $A$ . Looking at the extension  $A \hookrightarrow A[b_1, \dots, b_n] \hookrightarrow A[b_1, \dots, b_n, c]$ , we know the first extension is a finitely-generated  $A$ -module, and since  $c$  is integral in  $B$ , then the second extension is a finitely-generated  $A[b_1, \dots, b_n]$ -module, so  $A[b_1, \dots, b_n, c]$  is a finitely-generated  $A$ -module as well.  $\square$

**Remark 4.12** (Facts about integral extensions). Let  $A \hookrightarrow B$  be an integral extension.

1. Suppose  $B$  is a (integral) domain, then  $B$  is a field if and only if  $A$  is a field.

*Proof.* Suppose  $B$  is a field, then  $A$  is a domain as well, therefore for  $a \neq 0$ , we want to show that  $\frac{1}{a} \in A$ . Since  $B$  is a field, then  $\frac{1}{a} \in B$ , but that means it satisfies an equation

$$\left(\frac{1}{a}\right)^n + \lambda_1 \left(\frac{1}{a}\right)^{n-1} + \cdots + \lambda_n = 0.$$

Multiply it by  $a^{n-1}$ , we get

$$\left(\frac{1}{a}\right) + \lambda_1 + \lambda_2 a + \cdots + \lambda_n a^{n-1} = 0,$$

therefore  $\frac{1}{a} = -(\lambda_1 + \lambda_2 a + \cdots + \lambda_n a^{n-1})$ , therefore  $\frac{1}{a} \in A$ .

Suppose  $A$  is a field, let  $0 \neq b \in B$ , so we want to show  $\frac{1}{b} \in B$ . Since  $B$  is integral, then we can choose the smallest  $n$  such that  $b^n + a_1 b^{n-1} + \cdots + a_n = 0$ , then  $b(b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1}) + a_n = 0$ , so  $b(b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1}) = -a_n$ , but  $A$  is a field, then  $a_n$  is invertible by minimality, then  $b$  has to be a unit.  $\square$

**Definition 4.13** (Lying Over). Let  $A \hookrightarrow B$  be a ring extension, let  $\mathfrak{p}$  be a prime ideal in  $B$ , and let  $\mathfrak{q}$  is a prime ideal in  $A$ . We say  $\mathfrak{p}$  lies over  $\mathfrak{q}$  if  $\mathfrak{q} = \mathfrak{p} \cap A$ .

<sup>10</sup>To see this, use the fact that  $x^m - y^n$  is irreducible in  $A[x, y]$  if and only if  $\gcd(x, y) = 1$ .

2. Let  $A \hookrightarrow B$  be an integral extension, and suppose  $\mathfrak{p} \in \text{Spec}(B)$  lies over  $\mathfrak{q} \in \text{Spec}(A)$ , then  $\mathfrak{p}$  is a maximal ideal if and only if  $\mathfrak{q}$  is a maximal ideal.

*Proof.* Since  $A \hookrightarrow B$  is integral, then  $A/\mathfrak{q} \hookrightarrow B/\mathfrak{p}$  is also integral, but  $B/\mathfrak{p}$  is a domain, so we are done after applying the previous fact.  $\square$

3. Let  $A \hookrightarrow B$  be an integral extension, suppose  $0 \neq x \in B$  is a non-zero-divisor in  $B$ , then  $Bx \cap A \neq (0)$ .

*Proof.* Since  $x$  is a non-zero-divisor, we can choose the smallest  $n$  such that  $x^n + a_1x^{n-1} + \cdots + a_n = 0$ .

**Claim 4.14.**  $a_n \neq 0$ .

*Subproof.* Suppose not, then  $a_n = 0$ , then  $x(x^{n-1} + \cdots + a_{n-1}) = 0$ , but  $x$  is a non-zero-divisor, which forces  $x^{n-1} + \cdots + a_{n-1} = 0$ , a contradiction to the minimality of  $n$ .  $\blacksquare$

Therefore  $x(x^{n-1} + \cdots + a_{n-1}) = -a_n \neq 0$  in  $A$ , so  $-a_n \in xB \cap A$ .  $\square$

4. Suppose  $P \subseteq \mathcal{L}$  are ideals of  $B$ , where  $P$  is a prime ideal. Suppose  $P \cap A = \mathcal{L} \cap A$ , then  $P = \mathcal{L}$ .

*Proof.* Let  $\mathfrak{q} = P \cap A = \mathcal{L} \cap A$ , then  $A/\mathfrak{q} \hookrightarrow B/\mathfrak{p}$  is an integral extension, and  $B/\mathfrak{p}$  is a domain. If  $P \subsetneq \mathcal{L}$ , then  $\tilde{\mathcal{L}} := \mathcal{L}/\mathfrak{p} \neq 0$ , therefore by the second fact we know  $A/\mathfrak{q} \cap \tilde{\mathcal{L}} \neq (0)$ , contradiction to the fact that  $P \cap A = \mathcal{L} \cap A$ .  $\square$

5. Suppose  $P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_n$  is a strict chain of prime ideals in  $B$ . Let  $p_i = P_i \cap A$ , then  $p_1 \subsetneq p_2 \subsetneq \cdots \subsetneq p_n$  is a strict chain of prime ideals in  $A$ .
6. Using the notation above,  $\dim(B) \leq \dim(A)$ ,  $\text{ht}(P_n) \leq \text{ht}(p_n)$ .

**Theorem 4.15** (Going-up). Let  $A \hookrightarrow B$  be an integral extension. Given a prime  $\mathfrak{q}$  in  $A$ , there exists a prime  $\mathfrak{p}$  in  $B$  such that  $\mathfrak{p}$  lies over  $\mathfrak{q}$ .

*Proof.* Let  $S = A \setminus \mathfrak{q}$ , then we have

$$\begin{array}{ccc} B & \xrightarrow{i_S} & S^{-1}B \\ \uparrow & & \uparrow \\ A & \longrightarrow & S^{-1}A = A_{\mathfrak{q}} \end{array}$$

Since  $A \hookrightarrow B$  is integral, then  $S^{-1}A \hookrightarrow S^{-1}B$  is also integral, so  $S^{-1}B \neq 0$ , with  $1 \in S^{-1}B$ , so it is a commutative ring with multiplicative identity, then  $S^{-1}B$  has a maximal ideal  $\mathfrak{m}$ . Since  $S^{-1}B$  is integral over  $S^{-1}A$ , then  $\mathfrak{m}$  must lie over  $\mathfrak{q}A_{\mathfrak{q}}$ , so we pick  $\mathfrak{p} = i_S^{-1}(\mathfrak{m})$ , such that  $\mathfrak{p} \cap A = \mathfrak{q}$ .

$$\begin{array}{ccc} \mathfrak{q} & \xleftarrow{i_S^{-1}} & \mathfrak{m} \\ \uparrow & & \uparrow \\ \mathfrak{q} & \longrightarrow & \mathfrak{q}A_{\mathfrak{q}} \end{array}$$

$\square$

**Corollary 4.16.** Suppose  $A \hookrightarrow B$  is an integral extension, then  $\dim(B) = \dim(A)$ .

*Proof.* Consider the strict chain of prime ideals  $\mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_r$  in  $A$ . We proceed by induction on  $r$ . If  $r = 1$ , this is just [Theorem 4.15](#). Suppose  $r > 1$ . Let  $\mathfrak{p}_1$  in  $\text{Spec}(B)$  lie over  $\mathfrak{q}_1$  by [Theorem 4.15](#), then  $A/\mathfrak{q}_1 \hookrightarrow B/\mathfrak{p}_1$  is an integral extension, therefore we have a strict chain  $\bar{\mathfrak{q}}_2 \subsetneq \bar{\mathfrak{q}}_3 \subsetneq \cdots \subsetneq \bar{\mathfrak{q}}_r$ , then by induction we know there exists a chain  $\bar{\mathfrak{p}}_2 \subsetneq \cdots \subsetneq \bar{\mathfrak{p}}_r$  in  $B/\mathfrak{p}_1$  such that  $\bar{\mathfrak{p}}_i$  lies over  $\bar{\mathfrak{q}}_i$ . Consider the mapping  $\eta : B \rightarrow B/P_1$ , then let  $\mathfrak{p}_i = \eta^{-1}(\bar{\mathfrak{p}}_i)$ , so we have a strict chain  $\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$  such that  $\mathfrak{p}_i \cap A = \mathfrak{q}_i$  for all  $i$ . In particular,  $\dim(B) = \dim(A)$ .  $\square$

**Example 4.17.** Suppose  $A \hookrightarrow B$  is an integral extension, suppose  $J$  is an ideal in  $B$ , let  $I = J \cap A$ , then  $\text{ht}(J) \subseteq \text{ht}(I)$ .

**Remark 4.18.** 1. Consider the usual AKLB setup, that is, let  $A$  be an integral domain, let  $K = \text{Frac}(A)$  be the field of fractions of  $A$ , let  $L/K$  be an algebraic extension, and let  $B$  be the integral closure of  $A$  in  $L$ , so we have the diagram

$$\begin{array}{ccc} B & \hookrightarrow & L \\ \uparrow & & \uparrow \\ A & \hookrightarrow & K \end{array}$$

Then every element of  $L$  is of the form  $\frac{b}{a}$  for  $b \in B$  and  $0 \neq a \in A$ . To see this, for any element  $x \in L$ , we have  $x^n + \lambda_1 x^{n-1} + \dots + \lambda_n = 0$  for  $\lambda_i \in K$ , so  $\lambda_i = \frac{a_i}{s}$  for  $0 \neq s \in A$  and  $a_i \in A$ , so  $sx^n + a_1 x^{n-1} + \dots + a_n = 0$ , by multiplication of  $s^{n-1}$ , we know  $sx$  is integral over  $A$ , so  $sx \in B$ , thus  $x = \frac{b}{s}$ .

Implicitly, this means for  $S = A \setminus \{0\}$ , we have  $L = S^{-1}B$ .

2. Let  $\sigma \in \text{Aut}(L/K)$ , then  $\sigma(B) \subseteq B$ . If  $x$  is integral over  $A$ , then  $\sigma(x)$  is integral over  $A$ .

**Claim 4.19.**  $\sigma(B) = B$ .

*Proof.* Note  $\sigma^{-1}(B) \subseteq B$ , then  $B \subseteq \sigma(B)$ , so  $B = \sigma(B)$ . □

Let  $P$  be a prime ideal in  $B$  lying over  $\mathfrak{p}$  in  $A$ , then  $\sigma(P) \cap A = \mathfrak{p}$ . This implies  $\sigma(B)$  lies over  $\mathfrak{p}$  as well.

**Theorem 4.20.** Let  $A$  be an integrally closed domain, let  $K$  be the field of fractions of  $A$ , let  $L/K$  be a normal extension. Let  $B$  be the integral closure of  $A$  in  $L$ . Let  $G = \text{Aut}(L/K)$  and let  $\mathfrak{p}$  be a prime ideal in  $A$ , then  $G$  acts transitively on the primes in  $B$  lying over  $\mathfrak{p}$ . That is, if  $P$  and  $Q$  both lie over  $\mathfrak{p}$ , then there exists  $\sigma \in G$  such that  $\sigma(P) = Q$ .

*Proof.* To show there exists such  $\sigma$ , it suffices to show that there exists  $\sigma$  such that  $\sigma(P) \subseteq Q$ , then since both  $\sigma(P)$  and  $Q$  lie over  $\mathfrak{p}$ , we have equality.

We have two cases:

- suppose  $[L : K] < \infty$ , let  $G = \{\sigma_1, \dots, \sigma_n\}$  where  $\sigma_1 = \text{id}$ , and suppose for no  $\sigma_i$  we have  $P \subseteq \sigma_i^{-1}(Q)$ , then  $P \not\subseteq \bigcup_{i=1}^n \sigma_i^{-1}(Q)$ .

**Exercise 4.21.** If  $I \subseteq \bigcup_{i=1}^n P_i$ , then  $I \subseteq P_i$  for some  $i$ .

Let  $z \in P \setminus \bigcup_{i=1}^n \sigma_i^{-1}(Q)$ , so let  $w = z\sigma_2(z) \cdots \sigma_n(z)$ , then by choice of  $z$  we know  $w \in P \setminus Q$ , therefore  $\sigma_i(w) = w$  for  $1 \leq i \leq n$ , therefore  $w$  is fixed under the action of  $G$ .

- If  $\text{char}(K) = 0$ , then  $L/K$  is a Galois extension since  $L/K$  is separable and normal. Therefore, the fixed field of  $L$  under the action of  $G$  is  $K$ , so  $w \in K$ , but  $w$  is integral over  $A$ , and since  $A$  is integrally closed, then  $w \in A$ , therefore  $w \in P \cap A = \mathfrak{p}$ , so  $w \in Q$ , contradiction.
- If  $\text{char}(K) = p > 0$ , recall that we know there exists intermediate extension  $L/F/K$  such that  $L/F$  is purely separable and  $F/K$  is separable. In fact, when  $L/K$  is a normal extension, then we can find intermediate extension  $L/F/K$  such that  $L/F$  is separable and  $F/K$  is purely inseparable. Therefore,  $L/F$  is both separable and normal, hence  $L/F$  is Galois, and so  $w \in F$  by construction. Since  $F/K$  is purely inseparable, then  $w^l \in K$  for some  $l = p^t > 0$ . Since  $w^l$  is integral over  $A$ , then  $w^l \in A$ , thus  $w^l \in P \cap A = \mathfrak{p}$ , thus  $w^l \in Q$ , so  $w \in Q$ , contradiction.

Therefore, we must be able to find some  $\sigma$  such that  $\sigma(P) \subseteq Q$ .

**Remark 4.22.** The fact that  $F$  being bijective to  $G(L/F)$  only holds for finite extension  $L/F$ . In general, if we have an infinite extension, then  $F \rightarrow G(L/F)$  is only an injection.

- suppose  $[L : K] = \infty$ , let  $\mathcal{F}$  be the family of pairs  $(L_i, \varphi_i)$  where  $L_i/K$  is a normal extension where  $L_i \subseteq L$ , and for  $B_i = B \cap L_i$ ,  $P_i = P \cap B_i$ ,  $Q_i = Q \cap B_i$ ,  $\sigma_i \in G$  is such that  $\sigma_i(P_i) = Q_i$ . In this family, there is a poset relation given by  $(L_i, \sigma_i) \leq (L_j, \sigma_j)$  defined by  $L_i \subseteq L_j$  and  $\sigma_j|_{L_i} = \sigma_i$ . By Zorn's lemma,  $\mathcal{F}$  has a maximal element, which we call  $(L_0, \sigma_0)$ .

**Claim 4.23.**  $L_0 = L$ .

*Subproof.* Consider

$$\begin{array}{ccc} B & \text{---} & L \\ | & & | \\ B_0 & \text{---} & L_0 \\ | & & | \\ A & \text{---} & K \end{array}$$

where  $B_0 = B \cap L_0$ ,  $\sigma(P_0) = Q_0$ , and  $P_0 = P \cap B_0$ ,  $Q_0 = Q \cap B_0$ . That is,  $P, Q$  in  $B$  lie over  $P_0, Q_0 \in B_0$ . Suppose  $L_0 \neq L$ , then we can get a finite maximal extension  $L/L'/L_0$  given by  $L'$  over  $L_0$ , where  $P' = P \cap B'$ ,  $Q' = Q \cap B'$ , where  $B' = B \cap L'$ .

$$\begin{array}{ccc} P, Q & & B \text{ --- } L \\ & & | \quad \quad | \\ P', Q' & & B' \text{ --- } L' \\ & & | \quad \quad | \\ P_0, Q_0 & & B_0 \text{ --- } L_0 \\ & & | \quad \quad | \\ P, Q & & A \text{ --- } K \end{array}$$

This extends to an automorphism  $\sigma'$  of  $L'/K$  where  $\sigma'(P')$  and  $Q'$  both lie over  $Q_0$ . Since  $[L' : L_0]$  is finite, then by the previous case, we know there exists  $\sigma'' \in \text{Aut}(L'/L_0)$ , so  $\sigma''(\sigma'(P')) = Q'$ , therefore we have an automorphism  $\varphi = \sigma''\sigma'$  such that  $\varphi(P') = Q'$ , but that means  $(L'/\varphi) \in \mathcal{F}$ , a contradiction to the maximality of  $(L_0, \sigma_0)$ . ■

□

**Remark 4.24.** Suppose  $L/K$  is Galois with

$$\begin{array}{ccc} B & \text{---} & L \\ | & & | \\ A & \text{---} & K \end{array}$$

Let  $X$  be the set of all primes in  $\text{Spec}(B)$  lying over  $p \in A$ . We have a group action

$$\begin{aligned} G \times X &\rightarrow X \\ (\sigma, P) &\mapsto \sigma(P) \end{aligned}$$

and by fixing  $P \in X$ , we have a map

$$\begin{aligned} \varphi : G &\rightarrow X \\ \sigma &\mapsto \sigma(P) \end{aligned}$$

The stabilizer, also known as the isotropy subgroup of  $P$  under the action of  $G$ , is  $G_P = \{\sigma \in G \mid \sigma(P) = P\}$ . This is usually known as the decomposition subgroup of  $G$  with respect to  $P$  in algebraic number theory.

Let  $F$  be the fixed field of  $G_P$  over  $L/K$ , and let  $C = B \cap F$ , then there is  $\tilde{P} = P \cap C$ , with diagram

$$\begin{array}{ccccc} P & & B & \text{---} & L \\ & & \downarrow & & \downarrow \\ \tilde{P} & & C & \text{---} & F \\ & & \downarrow & & \downarrow \\ p & & A & \text{---} & K \end{array}$$

In fact,  $P$  is the unique prime lying over  $\tilde{P}$ .

**Theorem 4.25** (Going-down). Let  $A$  be an integrally closed domain,  $B$  be integral over  $A$  and is torsion-free as an  $A$ -module. Let  $\mathfrak{q} \subseteq \mathfrak{p}$  be two prime ideals in  $A$ , and let  $P$  be a prime ideal in  $B$  lying over  $\mathfrak{p}$ , then there exists a prime ideal  $Q$  in  $B$  such that  $Q \subseteq P$  and  $Q$  lies over  $\mathfrak{q}$ .

**Remark 4.26.** Let  $\mathfrak{p}$  be a prime in  $\text{Spec}(A)$  with Zariski topology, then  $\mathfrak{p} \in U$  for some open subset  $U$ , therefore  $\mathfrak{p} \in \text{Spec}(A_f)$ , therefore looking at the mapping  $A \rightarrow A_f$ , it sends  $\mathfrak{p}$  to some prime ideal in  $A_f$ , which means  $\mathfrak{p}$  does not vanish in  $A_f$ , thus  $\mathfrak{p}$  does not contain  $f$ , and that means any prime  $\mathfrak{q} \subseteq \mathfrak{p}$  does not contain  $f$  as well.

*Proof.* First suppose  $B$  is an integral domain, then let  $K = \text{Frac}(A)$ ,  $L = \text{Frac}(B)$ . Let  $\bar{L}$  be the normal closure of  $L$  and let  $\bar{B}$  be the integral closure of  $B$  in  $\bar{L}$ , then by [Theorem 4.15](#), there is  $\bar{P}$  in  $\bar{B}$ . In particular,  $\bar{P}$  lies over  $\mathfrak{p}$ . It suffices to show that there exists  $\bar{Q} \subseteq \bar{P}$  over  $\bar{B}$ , with  $\bar{Q} \cap A = \mathfrak{q}$ .

$$\begin{array}{ccccc} \bar{P} & & \bar{B} & \text{---} & \bar{L} \\ & & \downarrow & & \downarrow \\ P & & B & \text{---} & L \\ & & \downarrow & & \downarrow \\ \mathfrak{q} \subseteq \mathfrak{p} & & A & \text{---} & K \end{array}$$

Since  $\mathfrak{q} \subseteq \mathfrak{p}$ , then there exists  $\mathfrak{q}' \subseteq \mathfrak{p}'$  in  $\bar{B}$  such that  $\mathfrak{q}'$  lies over  $\mathfrak{q}$ ,  $\mathfrak{p}'$  lies over  $\mathfrak{p}$ . but since  $P$  also lies over  $\mathfrak{p}$ , then by [Theorem 4.20](#), there exists  $\sigma \in \text{Aut}(\bar{L}/K)$  such that  $\sigma(\mathfrak{p}') = \bar{P}$ . Therefore,  $\sigma(\mathfrak{q}') \subseteq \sigma(\mathfrak{p}')$ , and  $\sigma(\mathfrak{q}') =: \bar{Q}$  lies over  $\bar{Q}$ , as desired.

Now suppose  $B$  is not necessarily an integral domain, so we want to find a prime ideal  $\mathfrak{q}_0$  in  $B$  such that  $\mathfrak{q}_0 \cap A = (0)$  and  $\mathfrak{q}_0 \subseteq P$ , then  $A \rightarrow B/\mathfrak{q}_0$  allows us to reduce it to the previous case. Let  $S_1 = A \setminus \{0\}$  and  $S_2 = B \setminus P$ , take  $S = S_1 S_2$ , which is multiplicatively closed since  $B$  is torsion-free over  $A$ , then we have

$$\begin{array}{ccc} B & \xrightarrow{i_S} & S^{-1}B \\ \uparrow & & \uparrow \\ A & \xrightarrow{i} & K \end{array}$$

In particular,  $S^{-1}B \neq 0$ , with  $1 \in S^{-1}B$ , so there exists a prime ideal  $\mathfrak{m}$  in  $S^{-1}B$ , then  $i_S^{-1}(\mathfrak{m}) =: \mathfrak{q}_0$  is such that  $\mathfrak{q}_0 \cap A = (0)$  and  $\mathfrak{q}_0 \subseteq P$ .  $\square$

**Definition 4.27.** Let  $f : A \rightarrow B$  be a ring homomorphism as an extension.

- We say such an extension has a going-up property if given any prime  $\mathfrak{p}$  in  $A$ , there exists prime  $P$  in  $B$  such that  $f^{-1}(P) = \mathfrak{p}$ .
- We say such an extension has a going-down property if given any primes  $\mathfrak{q} \subseteq \mathfrak{p}$  in  $A$  and prime ideal  $P$  in  $B$  such that  $f^{-1}(P) = \mathfrak{p}$ , then there exists a prime ideal  $Q \subseteq P$  in  $B$  such that  $f^{-1}(Q) = \mathfrak{q}$ .

**Exercise 4.28.** (i) Let  $f : A \rightarrow B$  be faithfully flat, then  $f$  has the going-up property.

(ii) Let  $f : A \rightarrow B$  be flat, then  $f$  has the going-down property.



**Theorem 4.29** (Serre). Let  $A$  be Noetherian and let  $f : A \rightarrow B$  be a ring homomorphism where  $B$  is a finitely-generated  $A$ -algebra such that going-down property holds, then  $\tilde{f} : \text{Spec}(B) \rightarrow \text{Spec}(A)$  is an open map.

*Proof.* Omitted. □

**Corollary 4.30.** Let  $f : A \rightarrow B$  be a flat map between rings  $A, B$  as in [Theorem 4.29](#), then  $\tilde{f}$  is an open map.

#### 4.2 DISCRETE VALUATION RING (DVR) AND DEDEKIND DOMAIN

**Definition 4.31** (Normal, DVR). We say a domain is normal if it is Noetherian and integrally closed. We say a local PID is called a discrete valuation ring (DVR).<sup>11</sup>

**Proposition 4.32.** Let  $(A, \mathfrak{m})$  be a local domain, the following are equivalent:

- (i)  $A$  is a DVR;
- (ii)  $A$  is normal with  $\dim(A) = 1$ ;
- (iii)  $A$  is normal and there exists  $x \in \mathfrak{m}$  such that  $x \in \text{Ass}(A/Ax)$ ;
- (iv)  $\mathfrak{m} \neq 0$  is principal.

*Proof.* (i)  $\Rightarrow$  (ii): Since  $A$  is a local PID, then  $A$  is integrally closed, with  $\text{ht}(\mathfrak{m}) = 1$  since  $\mathfrak{m} = (x)$ , so  $\dim(A) = 1$ .

(ii)  $\Rightarrow$  (iii): let  $x \neq 0$ , the prime ideals are  $(0)$  and  $\mathfrak{m}$ , so  $\mathfrak{m} \in \text{Ass}(A/Ax)$  where  $Ax$  is  $\mathfrak{m}$ -primary.

(iii)  $\Rightarrow$  (iv): let  $\mathfrak{m} \in \text{Ass}(A/Ax)$ , then there exists an injection

$$\begin{aligned} A/\mathfrak{m} &\hookrightarrow A/Ax \\ \bar{1} &\mapsto \bar{y} \end{aligned}$$

and so there exists  $y \notin Ax$  such that  $\mathfrak{m}y \in Ax$ , thus  $\mathfrak{m}yx^{-1} \subseteq A$ , which is an ideal in  $A$ . There are two possibilities:

- if  $\mathfrak{m}yx^{-1} = A$ , then  $\mathfrak{m} = Ax y^{-1}$ , i.e.,  $\mathfrak{m}$  is principal generated by  $xy^{-1}$ ;
- if  $\mathfrak{m}yx^{-1} \subseteq \mathfrak{m}$ , then say  $\mathfrak{m}$  is generated by  $y_1, \dots, y_n$ , then write  $z = yx^{-1}$ , so we have

$$\begin{cases} zy_1 &= a_{11}y_1 + \dots + a_{1n}y_n \\ \vdots &= \vdots \\ zy_n &= a_{n1}y_1 + \dots + a_{nn}y_n \end{cases}$$

where  $a_{ij} \in A$ . Using the same trick as in [Proposition 2.53](#) and in [Proposition 4.2](#), we have  $\det(C) \cdot y_i = 0$  for all  $i$ , thus  $\det(C) \cdot \mathfrak{m} = 0$ , thus  $\det(C) = 0$  since  $\mathfrak{m} \subseteq A$  is in a domain, thus  $z$  satisfies an integral equation over  $A$ . Since  $A$  is integrally closed, then  $z \in A$ , so  $yx^{-1} \in A$ , thus  $y \in xA$ , which is a contradiction to the fact that  $y \notin Ax$ . Therefore, we must have  $\mathfrak{m}yx^{-1} = A$  instead, so  $\mathfrak{m}$  is principal.

(iv)  $\Rightarrow$  (i): suppose  $I = (a_1, \dots, a_m)$  for  $a_i \in \mathfrak{m}$ , then since  $\mathfrak{m} = (x)$ , we have  $0 = \bigcap_n \mathfrak{m}^n = \bigcap_n (x^n)$ , so for  $a_i \in (x^{t_i}) \setminus (x^{t_i+1})$ , we have  $a_i = \lambda_i x^{t_i}$  where  $\lambda_i$  is a unit. Let  $t$  be the smallest  $t_i$  among them, then  $I = (x^t)$ . □

**Theorem 4.33** (Serre). Let  $A$  be a Noetherian domain, then  $A$  is normal if and only if

- (i) for any prime ideal  $\mathfrak{p}$  with  $\text{ht}(\mathfrak{p}) = 1$ ,  $A_{\mathfrak{p}}$  is a DVR, and
- (ii) for any  $0 \neq x \in A$ ,  $xA = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$  where  $\mathfrak{q}_i$  is  $\mathfrak{p}_i$ -primary, where each prime  $\mathfrak{p}_i$  has  $\text{ht}(\mathfrak{p}_i) = 1$ , i.e., there is no embedded prime.

<sup>11</sup>In our case, we take the canonical discrete valuation, so we do not specify it.

*Proof.* Suppose  $A$  is normal, then  $\text{ht}(\mathfrak{p}) = 1$ , then  $A_{\mathfrak{p}}$  is normal of dimension 1. By Proposition 4.32,  $A_{\mathfrak{p}}$  is a DVR. This proves (i). Now suppose  $xA = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$  where  $\mathfrak{q}_i$  is  $\mathfrak{p}_i$ -primary. If possible, let one of  $\mathfrak{p}_i$ 's be of height at least 2, say  $\mathfrak{p}_1$ . Since  $\mathfrak{q}_1$  is  $\mathfrak{p}_1$ -primary with height at least 2, localizing at  $\mathfrak{p}_1$ , we have  $A_{\mathfrak{p}_1}$  with  $\mathfrak{p}_1 A_{\mathfrak{p}_1}$  is associated to  $xA_{\mathfrak{p}_1}$ . Since  $A_{\mathfrak{p}_1}$  is normal, then it has unique maximal ideal  $\mathfrak{p}_1 A_{\mathfrak{p}_1}$ . Therefore,  $\mathfrak{p}_1 A_{\mathfrak{p}_1}$  is the associated prime of  $A_{\mathfrak{p}_1}/xA_{\mathfrak{p}_1}$ . By Proposition 4.32, we know  $A_{\mathfrak{p}_1}$  is a DVR, since  $\text{ht}(\mathfrak{p}_1) > 1$ , then  $\dim(A_{\mathfrak{p}_1}) > 1$ , contradiction. Therefore, every associated prime of  $xA$  has height 1.

Now suppose both (i) and (ii) holds, it suffices to show that  $A = \bigcap_{\text{ht}(\mathfrak{p})=1} A_{\mathfrak{p}} \hookrightarrow \text{Frac}(A)$ . Suppose  $z \in \bigcap_{\text{ht}(\mathfrak{p})=1} A_{\mathfrak{p}}$ , then by the embedding we have  $z = \frac{x}{y}$  for  $x, y \in A$ . We want to show that  $x \in yA$ . We can write  $yA = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$  where  $\mathfrak{q}_i$  is  $\mathfrak{p}_i$ -primary for  $\text{ht}(\mathfrak{p}_i) = 1$ . Therefore, we have  $yA_{\mathfrak{p}_1} = \mathfrak{q}_1 A_{\mathfrak{p}_1}$ , so  $x \in yA_{\mathfrak{p}_1}$  for all height-1 prime  $\mathfrak{p}$ . This means  $x \in yA_{\mathfrak{p}_i} = \mathfrak{q}_i A_{\mathfrak{p}_i}$ , so  $x \in \mathfrak{q}_i^{12}$ , then  $x \in yA$ .  $\square$

**Example 4.34.** •  $k[x, y]/(y^2 - x^3)$  and  $k[x, y]/(y^2 - x^2(1 + x))$  are not normal.

•  $k[x, y, u, v]/(xy - uv)$  is the coordinate ring of  $\mathbb{P}^1 \times \mathbb{P}^1$ , then  $A$  is normal.

**Definition 4.35** (Dedekind). A normal domain of dimension 1 is called a Dedekind domain.

**Exercise 4.36.** Let  $A$  be a Dedekind domain with  $I \neq 0$  an ideal of  $A$ . Show that  $I$  is a product of prime ideals. This follows from primary decomposition. The converse is also true: suppose  $A$  is a domain such that every ideal  $I \neq 0$  is a product of prime ideals, then  $A$  is a Dedekind domain.

**Remark 4.37.** Consider the AKLB setup where  $A$  is normal,  $K = \text{Frac}(A)$ ,  $[L : K] < \infty$ , and  $B$  is the integral closure of  $A$  in  $L$ . Is  $B$  a finitely-generated  $A$ -module? Not necessarily.

1. In the case of  $\dim(A) = 1$ , we have

**Theorem 4.38** (Krull-Akizuki). Let  $A$  be a Noetherian domain with  $\dim(A) \leq 1$ ,  $K = \text{Frac}(A)$ ,  $[L : K] < \infty$ , and  $A \subseteq B \subseteq L$  where  $B$  is a subring of  $L$ , then  $B$  is Noetherian with dimension at most 1.

By Nagata, even if  $A$  is normal in this case, and if  $B$  is the integral closure of  $A$  in  $L$ ,  $B$  may not be a finitely-generated  $A$ -module.

2. In the case of  $\dim(A) = 2$ , by a very hard proof, one can show that  $B$  is Noetherian, but Nagata also showed that  $B$  may not be a finitely-generated  $A$ -module.

3. In the case of  $\dim(A) \geq 3$ , Nagata showed that  $B$  may not be Noetherian.

**Remark 4.39** (Hilbert's 14th Problem). Let  $K \subseteq k(x_1, \dots, x_n)$  be a subfield, is  $K \cap k[x_1, \dots, x_n]$  Noetherian? By Zariski, this is true for  $n = 1$  and 2; by Nagata, this is false in general.

**Theorem 4.40.** Consider the AKLB setup, where  $A$  is normal,  $K = \text{Frac}(A)$ ,  $[L : K] < \infty$ ,  $B$  is the integral closure of  $A$  in  $L$ . Moreover, suppose  $L$  is separably algebraic over  $K$ , then  $B$  is a finitely-generated  $A$ -module.

**Remark 4.41** (Prerequisites). 1. Suppose  $L/K$  is an algebraic finite extension, take  $x \in L$ . We know  $L = K \langle e_1, \dots, e_n \rangle$  where  $e_1, \dots, e_n$  gives a basis. Now  $x : L \rightarrow L$  is a  $K$ -linear map, so  $xe_i = \sum a_{ij}e_j$ , where we write  $A = (a_{ij})$ . Then  $\text{Tr}_{L/K}(x) = \text{Tr}(A) = \sum a_{ii}$ .

2. Suppose  $L/K$  is an extension such that  $L = K(x)$  where  $x$  is algebraic over  $K$ . Let  $f$  be the minimal polynomial of  $x$ , i.e., with  $f(x) = 0$ , then we can write  $f(X) = X^n + a_1X^{n-1} + \cdots + a_n$  for  $a_i \in K$ . Therefore,  $K(x)$  is a  $k$ -vector space with basis  $1, x, \dots, x^{n-1}$ . One can show that  $\text{Tr}_{K(x)/K}(x) = -a_1$ , which is the sum of all the roots. Moreover, one can show that if  $x$  is not separable over  $K$  (so  $\text{char}(K) = p > 0$ ), then  $\text{Tr}_{K(x)/K}(x) = 0$ .

3. Suppose  $L/F/K$  is a field extension with  $[L : K] < \infty$ . Suppose  $[L : F] = m$ , and let  $x \in F$ , then  $\text{Tr}_{L/K}(x) = m \cdot \text{Tr}_{F/K}(x)$ .

4. Suppose  $[L : K] < \infty$ , then  $L/K$  is separable if and only if there exists  $0 \neq x \in L$  such that  $\text{Tr}_{L/K}(x) \neq 0$ .

<sup>12</sup>We can pullback  $i_{\mathfrak{p}_i} : A \rightarrow A_{\mathfrak{p}_i}$  sending  $\mathfrak{q}_i$  to  $\mathfrak{q}_i A_{\mathfrak{p}_i}$ , i.e.,  $i_{\mathfrak{p}_i}^{-1}(\mathfrak{q}_i A_{\mathfrak{p}_i}) = \mathfrak{q}_i$ .

*Proof.* Consider the AKLB setup. Say  $[L : K] = n$ , we can choose  $e_1, \dots, e_n \in B$  such that  $e_1, \dots, e_n$  form a basis of  $L$  over  $K$ . (Recall that  $L = S^{-1}B$  for  $S = A \setminus \{0\}$ .) Note that this does not mean  $B$  is a free module. Consider

$$\begin{aligned} \text{Tr} : L \times L &\rightarrow K \\ (x, y) &\mapsto \text{Tr}_{L/K}(xy). \end{aligned}$$

as a non-degenerate bilinear form.

**Claim 4.42.** Given any  $x \in L$ , there exists  $y \in L$  such that  $\text{Tr}(x, y) \neq 0$ .

*Subproof.* Since  $L/K$  is separable, then there exists  $0 \neq \xi \in L$  such that  $\text{Tr}(\xi) \neq 0$  (by the fourth fact). Let  $y = \frac{\xi}{x}$ , then  $\text{Tr}(x, \frac{\xi}{x}) = \text{Tr}(\xi) \neq 0$ . ■

Consider

$$\begin{aligned} \tilde{\text{Tr}} : L &\rightarrow L^* = \text{Hom}_K(L, K) \\ x &\mapsto (y \mapsto \text{Tr}(x, y) = \text{Tr}(xy) := \text{Tr}_{L/K}(xy)) \end{aligned}$$

Thus, one can also write this as  $\tilde{\text{Tr}}(x)(y) = \text{Tr}(x, y) = \text{Tr}(xy)$ . Now the assignment  $x \mapsto \tilde{\text{Tr}}(x)$  is a  $K$ -linear map which is injective, and since  $[L : K] < \infty$ , then  $\tilde{\text{Tr}} : L \rightarrow L^*$  is an  $K$ -isomorphism.

Let  $e_1, \dots, e_n \in B$  be a basis of  $L/K$ , with dual basis  $e_1^*, \dots, e_n^* \in L^*$ , so

$$e_i^*(e_j) = \begin{cases} 0, & i \neq j \\ 1, & i = j. \end{cases}$$

Let  $\tilde{e}_i = \tilde{\text{Tr}}^{-1}(e_i^*)$  be the pullback on  $L$ . One can show that

$$\text{Tr}(\tilde{e}_i e_j) = \begin{cases} 0, & i \neq j \\ 1, & i = j. \end{cases}$$

Therefore,  $\{\tilde{e}_1, \dots, \tilde{e}_n\}$  forms a basis of  $L$  over  $K$ . Let  $\tilde{B} = \{\lambda \in L \mid \text{Tr}(\lambda B) \subseteq A\}$ .

**Claim 4.43.**  $B \subseteq \tilde{B} \subseteq A\{\tilde{e}_1, \dots, \tilde{e}_n\}$ , the free  $A$ -module generated by  $\tilde{e}_1, \dots, \tilde{e}_n$ .

**Remark 4.44.** Claim 4.43 implies  $B$  is a finitely-generated  $A$ -module.

*Subproof of Claim 4.43.* For any  $b \in B$ ,  $b$  is integral over  $A$ , so let  $f(x) = x^n + \lambda_1 x^{n-1} + \dots + \lambda_n$  be the minimal polynomial of  $b \in K[x]$ , i.e.,  $\lambda_i \in K$  for  $1 \leq i \leq n$ .

**Claim 4.45.**  $\lambda_i \in A$  for all  $i$ .

*Subproof of Claim 4.45.* Note  $b^n + \lambda_1 b^{n-1} + \dots + \lambda_n = 0$ , then let  $b = c_1, \dots, c_n$  be the roots of  $f(x)$ , then  $\lambda_1 = \sum e_i$ , and each  $\lambda_i$  is a symmetric polynomial in  $c_1, \dots, c_n$  of degree  $i$ . But any  $c_i = \sigma_i(b)$  for  $\sigma_i : L \rightarrow \bar{K}$  embedding, and the coefficients are now fixed by  $\sigma_i$ 's, so whatever integral equation  $b$  satisfies,  $c_i$ 's also satisfy. Therefore, since  $b$  is integral over  $A$ , then every  $c_i$  has to be integral over  $A$ , therefore  $\lambda_i$ 's are integral over  $A$ . Since  $A$  is normal, then  $\lambda_i \in K$ , therefore  $\lambda_i$ 's are all in  $A$ . ■

Therefore,  $\text{Tr}(b) = -\lambda_1 \in A$ , so  $B \subseteq \tilde{B}$  by definition.

We will now show that  $\tilde{B} \subseteq A\{\tilde{e}_1, \dots, \tilde{e}_n\}$ . Let  $\tilde{b} \in \tilde{B}$ , then  $\tilde{b} = \mu_1 \tilde{e}_1 + \dots + \mu_n \tilde{e}_n$  for  $\mu_i$ 's in  $K$ . Therefore,  $\tilde{b} e_i = \sum_j \mu_j \tilde{e}_j e_i$  for  $e_i \in B$ , therefore

$$\begin{aligned} \text{Tr}(\tilde{b} e_i) &= \sum_j \mu_j \text{Tr}(\tilde{e}_j e_i) \\ &= \mu_i. \end{aligned}$$

Since  $\text{Tr}(\tilde{b} e_i) \in A$ , then  $\mu_i \in A$  for all  $1 \leq i \leq n$ , therefore  $\tilde{B} \subseteq A\{\tilde{e}_1, \dots, \tilde{e}_n\}$ . ■

□

## 5 NOETHER'S NORMALIZATION LEMMA

**Definition 5.1** (Affine Algebra). Let  $k$  be a field,  $A$  be a finitely-generated  $k$ -algebra. We say  $A$  is an affine  $k$ -algebra. That is,  $A$  is of the form  $k[X_1, \dots, X_n]/I$  for some ideal  $I$  of  $k$ .

**Theorem 5.2** (Noether's Normalization Lemma). Let  $A$  be an affine  $k$ -algebra, and let  $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \dots \subsetneq \mathfrak{a}_r$  be a finite increasing chain of ideals in  $A$ .

- (i) There exists  $x_1, \dots, x_n \in A$  such that  $x_1, \dots, x_n$  are algebraically independent over  $k$ .
- (ii)  $A$  is integral over  $k[x_1, \dots, x_n]$ .
- (iii) There exists a function  $h : \{1, \dots, r\} \rightarrow \{0, 1, \dots, n\}$  such that
  - $h(i) \geq 0$  for all  $i \in \{1, \dots, r\}$ ;
  - $h(i) \leq h(j)$  whenever  $i < j$  in  $\{1, \dots, r\}$ , satisfying

$\mathfrak{a}_i \cap k[x_1, \dots, x_n] = (x_1, \dots, x_{h(i)})$ . In particular, if  $h(i) = 0$ , then the ideal is zero.

**Exercise 5.3.** Given the setup in the Going-down Theorem (Theorem 4.25), if  $\mathfrak{b}$  is an ideal in  $B$  and  $\mathfrak{b} \cap A = \mathfrak{a}$ , then  $\text{ht}(\mathfrak{b}) = \text{ht}(\mathfrak{a})$ .

*Proof.* Step 1: Reduction to the case where  $A$  is a polynomial ring. Consider

$$\begin{aligned} \varphi : B = k[Y_1, \dots, Y_d] &\rightarrow A = k[y_1, \dots, y_d] \\ Y_i &\mapsto y_i \end{aligned}$$

to be the surjection. Note that here  $y_1, \dots, y_d \in A$  are elements that may not be algebraically independent of each other. Consider  $\varphi^{-1}(0) \subsetneq \varphi^{-1}(\mathfrak{a}_1) \subsetneq \dots \subsetneq \varphi^{-1}(\mathfrak{a}_r)$  as a strict chain in  $B$  because  $\varphi$  is surjective. Suppose we prove the theorem in  $B$ , then there exists  $z_1, \dots, z_d$  algebraically independent over  $k$  such that  $B$  is integral over  $C = k[Z_1, \dots, Z_d]$ ,  $\varphi^{-1}(0) \cap C = (Z_1, \dots, Z_{h(0)})$ , and  $\varphi^{-1}(\mathfrak{a}_i) \cap C = (Z_1, \dots, Z_{h(0)}, \dots, Z_{h(i)})$  for all  $i$ . We now mod out  $\varphi^{-1}(0)$ , then let  $x_1 = \bar{Z}_{h(0)+1}, \dots, x_n = \bar{Z}_d$  in  $A \cong B/\varphi^{-1}(0)$ , and one can check that  $A$  is integral over  $k[x_1, \dots, x_n]$  and  $\mathfrak{a}_i \cap k[x_1, \dots, x_n] = (x_1, \dots, x_{h(i)})$ .<sup>13</sup>

Step 2: We can write  $A = k[Y_1, \dots, Y_n]$ , then let  $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \dots \subsetneq \mathfrak{a}_r$  be a chain of ideals in  $A$ . For  $r = 1$ , we have  $\mathfrak{a} = \mathfrak{a}_1$  as a principal ideal  $\mathfrak{a} = (x_1)$ , then  $x_1$  is algebraically independent over  $k$ . Let  $x_2 = Y_2 - Y_1^{\alpha_2}, \dots, x_n = Y_n - Y_1^{\alpha_n}$ , and we will postpone the choice of  $\alpha_2, \dots, \alpha_n$ . We can write

$$\begin{aligned} x_1 &= f(Y_1, \dots, Y_n) \\ &= \sum a_{i_1 \dots i_n} Y_1^{i_1} \dots Y_n^{i_n} \\ &= \sum a_{i_1 \dots i_n} Y_1^{i_1} (x_2 + Y_1^{\alpha_2})^{i_2} \dots (x_n + Y_1^{\alpha_n})^{i_n} \end{aligned}$$

where  $a_{i_1 \dots i_n} \in k$ . This represents a polynomial equation in  $Y_1$  and  $k[x_1, \dots, x_n]$ . For each term  $a_{i_1 \dots i_n} Y_1^{i_1} (x_2 + Y_1^{\alpha_2})^{i_2} \dots (x_n + Y_1^{\alpha_n})^{i_n}$ , the highest power of  $Y_1$  is  $i_1 + i_2\alpha_2 + \dots + i_n\alpha_n$ , given by the term  $a_{i_1 \dots i_n} Y_1^{i_1 + i_2\alpha_2 + \dots + i_n\alpha_n}$ . We need to show that if  $(i_1, \dots, i_n)$  and  $(j_1, \dots, j_n)$  appearing as powers in the exponent of  $f$ , then  $i_1 + i_2\alpha_2 + \dots + i_n\alpha_n \neq j_1 + j_2\alpha_2 + \dots + j_n\alpha_n$  for our choice of  $\alpha_i$ 's, otherwise they cancel each other (e.g., by characteristic argument, etc.).<sup>14</sup> Now  $f$  has in its expression finitely many  $(i_1, \dots, i_k)$  appearing as powers. Let  $s$  be larger than the maximal of  $i_j$  for any  $(i_1, \dots, i_n)$  appearing as powers in the expression of  $f$ . Take  $\alpha_2 = s, \alpha_3 = s^2$ , and so on, until  $\alpha_n = s^{n-1}$ .

**Claim 5.4.** With this choice of  $\alpha_i$ 's,  $i_1 + i_2\alpha_2 + \dots + i_n\alpha_n \neq j_1 + j_2\alpha_2 + \dots + j_n\alpha_n$  whenever  $(i_1, \dots, i_n) \neq (j_1, \dots, j_n)$ .

*Subproof.* Otherwise, we have  $(i_1 - j_1) = -\alpha_2(i_2 - j_2) - \dots - \alpha_n(i_n - j_n)$ , but  $i_1, j_1 < s$  and  $\alpha_i > s^{i-1}$ , so such an equation cannot hold.<sup>15</sup> ■

<sup>13</sup>Basically, because we have an extension  $k[Z_1, \dots, Z_d] \hookrightarrow B$ , then by modding out  $\varphi^{-1}(0)$  we have  $k[x_1, \dots, x_n] = k[Z_1, \dots, Z_d]/(\varphi^{-1}(0) \cap k[Z_1, \dots, Z_d])$  which has an integral extension into  $A = B/\varphi^{-1}(0)$ .

<sup>14</sup>Even if the powers have the same sum, they may not cancel each other because the coefficient  $a$ 's, but we want to guarantee that would not happen. We want the coefficient to be with respect to  $k$  only, that way we can divide the coefficient from the field  $k$  and get an integral equation; if the highest degree terms cancel, then the new highest degree term of the expression of  $x_1$  may involve  $x_2, \dots, x_n$ 's, making it not an integral equation of  $x_1$ .

<sup>15</sup>Basically, this is saying an integer has a unique  $s$ -adic expansion.

Therefore,  $Y_1$  is integral in  $k[x_1, \dots, x_n]$ , so by construction  $Y_2, \dots, Y_n$  are all integral over  $k[x_1, \dots, x_n]$ . Hence,  $A = k[Y_1, \dots, Y_n]$  is integral over  $k[x_1, \dots, x_n]$ . We know  $A = k[Y_1, \dots, Y_n]$  has dimension  $n$ , and that means  $\dim(k[x_1, \dots, x_n]) \geq n$  by the property of lying over, but having only  $n$  variables it has dimension at most  $n$ , so it has dimension exactly  $n$ , hence  $k[x_1, \dots, x_n]$  is a polynomial ring, i.e.,  $x_1, \dots, x_n$  are algebraically independent over  $k$ .

**Claim 5.5.**  $\mathfrak{a} \cap C = x_1 C$  for  $C = k[x_1, \dots, x_n]$ .

*Subproof.* Obviously  $\mathfrak{a} \cap C \supseteq x_1 C$ . If  $\mathfrak{a} \cap C \neq x_1 C$ , then  $\mathfrak{a} \cap C \supsetneq x_1 C$  which is a prime ideal of height 1 in  $C$ . Therefore,  $\text{ht}(\mathfrak{a} \cap C) \geq 2$ , but  $\text{ht}(\mathfrak{a}) = 1$ , contradiction. ■

□

## 6 HOMOLOGICAL ALGEBRA

## REFERENCES

- [Ati18] Michael Atiyah. *Introduction to commutative algebra*. CRC Press, 2018.
- [Bou98] Nicolas Bourbaki. *Commutative algebra: chapters 1-7*, volume 1. Springer Science & Business Media, 1998.
- [Mat70] Hideyuki Matsumura. *Commutative algebra*, volume 120. WA Benjamin New York, 1970.
- [Ser12] Jean-Pierre Serre. *Local algebra*. Springer Science & Business Media, 2012.
- [ZS13] Oscar Zariski and Pierre Samuel. *Commutative algebra: Volume II*, volume 29. Springer Science & Business Media, 2013.
- [ZSC59] Oscar Zariski, Pierre Samuel, and Irvin Sol Cohen. *Commutative algebra*, volume 1. Springer, 1959.