Commutative Algebra II

Marco Schlichting
Notes by Florian Bouyer

23rd April 2013

Contents

1 Introduction and Review **2**
1.1 Introduction . . . 2
1.2 Outline . . . 2
1.3 Review of Commutative Algebra I . . . 2
1.3.1 Basic Definitions . . . 2
1.3.2 Localization, Exact Sequences and Tensor Products . . . 3
1.3.3 Noetherian and Artinian Modules . . . 5
1.3.4 Special Rings . . . 5
1.3.5 Krull Dimension . . . 5

2 Completion **6**
2.1 Inverse limits . . . 7
2.2 Cauchy sequences and completions . . . 8
2.3 Filtrations . . . 10
2.4 Graded rings and the Artin-Rees Lemma . . . 10
2.5 Flat modules and Krull's Intersection Theorem . . . 12
2.6 Hensel's Lemma . . . 14
2.7 Cohen's Structure Theorem . . . 16

3 Dimension Theory **19**
3.1 Length . . . 19
3.2 Hilbert Polynomial . . . 19
3.3 Characteristic Polynomial . . . 21
3.4 Dimension Theorem . . . 22
3.5 Faithfully Flat and Going Down. . . . 25
3.6 Dimension and Integral Extensions . . . 27
3.7 Groebner basis and an algorithmic computation of the Hilbert Polynomial . . . 30
3.7.1 Algorithm for computing $H(S/I)$ where $I \subset S$ is a monomial ideal. . . . 31
3.7.2 Division Algorithm . . . 33
3.7.3 Buchberger's Algorithm for finding a Groebner basis . . . 34

4 Smooth and Etale Extensions **37**
4.1 Derivations and the Module of Kähler Differentials . . . 37
4.2 Formally smooth and êtale Extensions . . . 40
4.3 Smoothness and Regularity . . . 44

<u>*All rings are commutative with* 1</u>

1 Introduction and Review

1.1 Introduction

These are the lecture notes for MA4J8 "Commutative Algebra II" taught at the University of Warwick in Spring 2013. I based the lectures for Section 1 on the lecture notes of MA3G6. Sections 2.1 - 2.5 are based on Atiyah-Macdonald "Commutative Algebra". Sections 2.6, 2.7 are based on Eisenbud "Commutative Algebra with a view toward Algebraic Geometry". Sections 3.1 - 3.4 are based on Atiyah-Macdonald's book. Sections 3.5, 3.6 are based on Matsumura "Commutative ring theory". Section 3.7 is based on Hasset "Introduction to Algebraic Geometry" except for the last theorem of that section which is based on the corresponding theorem in Eisenbud's book. Section 4 is based on my recollection of Grothendieck's EGA IV part of which you may also find in Eisenbud's or Matsumura's book. Please send comments, corrections etc to m.schlichting at warwick.ac.uk.

Marco Schlichting

1.2 Outline

1. Review of Commutative Algebra I
2. Completions
3. Dimension Theory
4. Smooth and Etale Extension

1.3 Review of Commutative Algebra I

1.3.1 Basic Definitions

Definition 1.1. A *ring* is a tuple $(R, \cdot, +, 0, 1)$ where R is a set, $0, 1 \in R$ and $\cdot, + : R \times R \to R$ such that:

- $(R, +, 0)$ is an abelian group
- $(R, \cdot, 1)$ is a unital monoid
- $(\cdot, +)$ are distributive

Remark. In this module, all rings will be commutative containing 1, i.e., $ab = ba\, \forall a, b \in R$.

Example. $\mathbb{Z}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}/n\mathbb{Z}, k[T_1, \dots, T_n]$ where k is a field, $R/I, S^{-1}R$

Definition 1.2. An *ideal* in a ring R is a subset $I \subset R$ such that $a - b \in I\, \forall a, b \in I$ and $ax \in I\, \forall a \in I, x \in R$.

If $f : R \to S$ is a ring map then $\ker(f) \subset R$ is an ideal, and every ideal $I \subset R$ is $\ker(f)$ where $f : R \to R/I$ defined by $r \mapsto r + I$. (Recall $R/I = \{R/\sim : a \sim b \iff a - b \in I\}$)

Isomorphism Theorem. *If $f : R \to S$ is a <u>surjective</u> ring map then $R/\ker(f) \to S$ defined by $x + \ker(f) \mapsto f(x)$ is a ring isomorphism*

Definition 1.3. An ideal $I \subset R$ is called

- *proper* if $I \neq R$
- *principal* if $I = (f) = fR$ for some $f \in R$
- *prime* if it is proper and $\forall a, b \in R$ with $ab \in I \Rightarrow a \in I$ or $b \in I$
- *maximal* if I is maximal among proper ideal

Fact. *Every proper ideal is contained in a maximal ideal. (Proved using Zorn's lemma)*
Maximal ideals are prime ideals
$I \subset R$ is prime if and only if R/I is a domain (see definition 1.9).
$I \subset R$ is maximal if and only if R/I is a field

Definition 1.4. An *R-module* is an abelian group $(M, +, 0)$ together with a map $\cdot : R \times M \to M$, called scalar product, such that:

- $1 \cdot x = x \, \forall x \in M$
- $(a+b) \cdot x = a \cdot x + b \cdot x \, \forall a, b \in R, x \in M$
- $a \cdot (x+y) = a \cdot x + a \cdot y \, \forall a \in R, x, y \in M$

Example.
- R is an R-module via $R \times R \to R$
- An ideal in R is the same as a submodule of R

1.3.2 Localization, Exact Sequences and Tensor Products

Definition 1.5. Let $S \subset R$ be a multiplicative subset (i.e., $1 \in S, a, b \in S \Rightarrow ab \in S \, \forall a, b \in R$), let M be an R-module. Then $S^{-1}M$ is an R-module together with a module map $L : M \to S^{-1}M$ such that:

- $\forall a \in S : S^{-1}M \xrightarrow{\cdot a} S^{-1}M$ (defined by $x \mapsto ax$) is an isomorphism
- For all maps $f : M \to N$ of R-modules such that $\forall a \in S$ the map $N \xrightarrow{\cdot a} N$ is an isomorphism, $\exists! \, \overline{f} : S^{-1}M \to N$ such that

$$\begin{tikzcd} & S^{-1}M \arrow[d, "\overline{f}"] \\ M \arrow[ur, "L"] \arrow[r, "f"'] & N \end{tikzcd}$$

commutes

$S^{-1}M$ is called the *localization* of M with respect to S.

The construction of this is: $S^{-1}M = \left\{ \frac{x}{b} | x \in M, a \in S \right\} / \sim$ where $\frac{x}{a} \sim \frac{y}{b} \iff \exists c \in S$ such that $cbx = cay$. $S^{-1}M$ is an R-module via:

- $\frac{x}{a} + \frac{y}{b} = \frac{bc+ay}{ab} \, \forall a, b \in S, x, y \in M$
- $r\frac{x}{a} = \frac{rx}{a} \, \forall a \in S, r \in R, x \in M$

Remark. $S^{-1}R$ is a ring via $\frac{x}{a} \cdot \frac{y}{b} = \frac{xy}{ab}$. $R \to S^{-1}R$ defined by $x \mapsto \frac{x}{1}$ is a ring map.

Example. $\mathbb{Q} = S^{-1}\mathbb{Z}$ where $S = \mathbb{Z} \setminus \{0\}$.

Notation. If $f \in R$, $R_f = S^{-1}R$ where $S = \{1, f, f^2, \dots\}$ (similarly for M_f)
If $P \subset R$ is a prime ideal, $R_P = S^{-1}R$ where $S = R \setminus P$ (similarly for M_P)

Definition 1.6. A sequence $M \xrightarrow{f} N \xrightarrow{g} P$ of R-module maps is called *exact* if $\operatorname{im} f = \ker g$. (Equivalently: $gf = 0$ and $\forall y \in N, g(y) = 0$ there exists $x \in M : f(x) = y$)

Fact. *The functor: R-modules $\to$ $S^{-1}R$-module, $M \mapsto S^{-1}M$ is exact, i.e., if $M \to N \to P$ is exact then $S^{-1}M \to S^{-1}N \to S^{-1}P$ is also exact.*

Definition 1.7. Let M, N be R-modules. The *tensor product* $M \otimes_R N$ is an R-module together with a bilinear map $b : M \times N \to M \otimes_R N$ such that for all R-bilinear maps $f : M \times N \to P$ (where P is a R-module) $\exists!$ R-linear map $\overline{f} : M \otimes_R N \to P$ such that

$$\begin{tikzcd} & M \otimes_R N \arrow[d, "\overline{f}"] \\ M \times N \arrow[ur, "b"] \arrow[r, "f"'] & P \end{tikzcd}$$

commutes

The construction of this is: $M \otimes_R N = \{x_1 \otimes y_1 + \cdots + x_n \otimes y_n |\ n \in \mathbb{N}, x_i \in M, y_i \in N\} / \sim$ where $\sim$ is generated by:

- $(x_1 + x_2) \otimes y \sim x_1 \otimes y + x_2 \otimes y$
- $x \otimes (y_1 + y_2) \sim x \otimes y_1 + x \otimes y_2$
- $a(x \otimes y) \sim (ax) \otimes y \sim x \otimes (ay)\, \forall a \in R, x_1, x_2 \in M, y_1, y_2 \in N$

The map $b : M \times N \to M \otimes_R N$ is defined by $(x, y) \mapsto x \otimes y$

Fact. *Tensor product is right exact, i.e., if $M_1 \to M_2 \to M_3 \to 0$ is exact then $M_1 \otimes_R N \to M_2 \otimes_R N \to M_3 \otimes_R N \to 0$ is also exact.*
$R \otimes_R M \cong M$ where the isomorphism is defined by $a \otimes m \mapsto am$
$S^{-1}M \cong S^{-1}R \otimes_R M$, where the isomorphism is defined by $\frac{x}{a} \mapsto \frac{1}{a} \otimes x$
$M \otimes N \cong N \otimes M$ where the isomorphism is defined by $x \otimes y \mapsto y \otimes x$
$(M_1 \oplus M_2) \otimes N \cong M_1 \otimes N \oplus M_2 \otimes N$
If $R \to A$ and $R \to B$ are ring maps then $A \otimes_R B$ is a ring via $(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1 a_2 \otimes b_1 b_2$ and

$$A \longrightarrow A \otimes_R B \longleftarrow B$$

$$a \longmapsto a \otimes 1; 1 \otimes b \longleftarrow\!\shortmid\, b$$

are ring maps

Example. • How to compute $M \otimes_R N$?
$\mathbb{Z}/12\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/9\mathbb{Z} =?$. We have $\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ so

$$\begin{aligned} \mathbb{Z}/12\mathbb{Z} \otimes \mathbb{Z}/9\mathbb{Z} &\cong (\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}) \otimes \mathbb{Z}/9\mathbb{Z} \\ &\cong \mathbb{Z}/4\mathbb{Z} \otimes \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \otimes \mathbb{Z}/9\mathbb{Z} \end{aligned}$$

Now $\mathbb{Z} \xrightarrow{4} \mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to 0$ is exact $\Rightarrow \underbrace{\mathbb{Z} \otimes \mathbb{Z}/9\mathbb{Z}}_{\mathbb{Z}/9\mathbb{Z}} \underset{\cong}{\xrightarrow{4}} \underbrace{\mathbb{Z} \otimes \mathbb{Z}/9\mathbb{Z}}_{\mathbb{Z}/9\mathbb{Z}} \to \mathbb{Z}/4\mathbb{Z} \otimes \mathbb{Z}/9\mathbb{Z} \to 0$ is exact $\Rightarrow \mathbb{Z}/4\mathbb{Z} \otimes \mathbb{Z}/9\mathbb{Z} = 0$
Also $\mathbb{Z} \xrightarrow{9} \mathbb{Z} \to \mathbb{Z}/9\mathbb{Z} \to 0$ is exact $\Rightarrow \underbrace{\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z}}_{\mathbb{Z}/3\mathbb{Z}} \underset{=0}{\xrightarrow{4}} \underbrace{\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z}}_{\mathbb{Z}/3\mathbb{Z}} \to \mathbb{Z}/9\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z} \to 0$ is exact $\Rightarrow \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \otimes \mathbb{Z}/9\mathbb{Z}$.
Alternatively, one can show (exercise) that $R/I \otimes_R R/J = R/(I + J)$ and apply this to see that $\mathbb{Z}/n \otimes_{\mathbb{Z}} \mathbb{Z}/m \cong \mathbb{Z}/\gcd(m, n)$.

- How to compute $A \otimes_R B$?
  use:
  - $A \otimes_R R[T] \cong A[T]$, where the isomorphism is defined by $a \otimes \sum_{i=1}^n x_i T^i \mapsto \sum_{i=1}^n a x_i T^i$
  - $A/f \otimes_R B \cong (A \otimes_R B)/(f \otimes 1)$, because of the exact sequence $A \xrightarrow{f} A \to A/f \to 0$ and tensor product is right exact, i.e., $A \otimes_R B \xrightarrow{f \otimes 1} A \otimes_R B \to A/f \otimes_R B \to 0$ is exact.

  Example.

$$\begin{aligned} \mathbb{C} \otimes_R \mathbb{C} &= \mathbb{C} \otimes_{\mathbb{R}} \frac{\mathbb{R}[T]}{T^2 + 1} \\ &= \frac{\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[T]}{1 \otimes (T^2 + 1)} \\ &= \mathbb{C}[T]/(T^2 + 1) \\ &= \mathbb{C}[T]/(T + i)(T - i) \\ &\cong \mathbb{C} \times \mathbb{C} \text{ By the Chineses Remainder Theorem} : f \mapsto (f(i), f(-i)) \end{aligned}$$

1.3.3 Noetherian and Artinian Modules

Definition 1.8. An R-module M is called *Noetherian* (respectively *Artinian*) if the submodules satisfies the ACC (respectively DCC), i.e., every ascending (respectively descending) chain of submodules eventually stops.

A ring R is *Noetherian* (respectively *Artinian*) if the R-module R is Noetherian (respectively Artinian)

Fact.
- *If R is Noetherian then an R-module M is Noetherian if and only if M is finitely generated*
- *If R is Artinian then an R-module M is Artinian if and only if M is finitely generated.*
- *If R is Noetherian then $R[T]$ is Noetherian (Hilbert's basis Theorem)*
- *If R is Noetherian (respectively Artinian) then R/I and $S^{-1}R$ are Noetherian (respectively Artinian)*

1.3.4 Special Rings

Definition 1.9. A ring R is a *domain* if $R \neq 0$ and $\forall a, b \in R$ such that $ab = 0$, then either $a = 0$ or $b = 0$

A PID (*principal ideal domain*) is a ring R which is domain in which every ideal is principal.

A ring R is a UFD (*unique factorization domain*) if R is a domain and every $x \in R$ is a product of prime elements. ($p \in R$ is *prime* if $(p) = pR$ is a prime ideal)

Fact.
- *PID are UFD*
- *If R is a UFD then $R[T]$ is a UFD*

Example. $\mathbb{Z}$, $k[T]$ where k is a field are PID

$\mathbb{Z}, k[T], \mathbb{Z}[T_1, \ldots, T_n], k[T_1, \ldots, T_n]$ are UFD

Definition 1.10. R is called *local* if R has a unique maximal ideal m. In this case, $k = R/m$ is a field called the residue field (at m). When R is a local ring we will often write (R, m, k) to mean that $m \subset R$ is the unique maximal ideal and $k = R/m$ its residue field.

Example. R any ring and $P \subset R$ a prime ideal. Then R_P is a local ring with maximal ideal PR_P

Fact.
- *Let (R, m, k) be a local ring then $x \in R$ is a unit if and only if $x \notin m$*
- *Let (R, m, k) be a local ring, M a finitely generated R-module such that $M/mM = 0$, then $M = 0$ (Nakayama's lemma)*

Definition 1.11. R is a DVR (*discrete valuation ring*) if R is a local PID which is not a field.

Example. $\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} | a, b \in \mathbb{Z}, p \nmid b \right\}$ is local with maximal ideal $(p) = p\mathbb{Z}_{(p)}$

Definition 1.12. R is a *Dedekind domain* if R is a Noetherian domain which is not a field and $\forall P \neq 0 \subset R$ prime ideal, R_P is a DVR

Example. Any PID, DVR and ring of integers in a number field is a Dedekind domain.

1.3.5 Krull Dimension

Definition 1.13. Let R be a ring. The *Krull dimension* of R is $\dim R = \max\{n \in \mathbb{Z} | \exists P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n \subset R, P_i \text{ prime ideals}\}$

Example. In this module we set $\dim 0 = -1$, though some authors may set $\dim 0 = -\infty$

Fact.
- $\dim 0$*:*
  - *Let $R \neq 0$ be a Noetherian ring then $\dim R = 0$ if and only if R is Artinian*
  - *If $R \neq 0$ is Artinian then $R = A_1 \times \cdots \times A_n$ where A_i are local Artinian rings*
  - *(R, m, k) is a local Artinian ring then m is nilpotent (i.e., $m^n = 0$ for some n)*

  Example. k a field, $\mathbb{Z}/n\mathbb{Z}$ have dimension 0.
- $\dim 1$*:*
  - *If R a PID which is not a field, then $\dim R = 1$ (e.g., $\mathbb{Z}, K[T]$)*
  - *Any DVR or Dedekind domain has dimension* 1.

2 Completion

First a few examples before the definition.

Example. Let R be a ring. The (T)-adic completion of $R[T]$ is the formal power series ring

$$R\left[[T]\right] = \left\{ a_0 + a_1 T + a_2 T^2 + \cdots = \sum_{i=0}^{\infty} a_i T^i \right\}$$

Formally, elements of $R[[T]]$ are sequences $(a_i)_{i\in\mathbb{N}} = (a_0, a_1, a_2, \dots)$ $a_i \in R$, with addition:

$$\left(\sum_{i\geq 0} a_i T^i\right) + \left(\sum_{i\geq 0} b_i T^i\right) = \sum_{i\geq 0}(a_i + b_i)T^i$$

and multiplication:

$$\left(\sum_{i\geq 0} a_i T^i\right) \cdot \left(\sum_{i\geq 0} b_i T^i\right) = \sum_{i\geq 0} c_i T^i \text{ where } c_k = \sum_{i+j=k} a_i b_j$$

The element 0 is $(0,0,0,\dots)$ and the element 1 is $(1,0,0,0,\dots)$. This is a ring and $R[T] \subset R[[T]]$ is a ring map.

It is easier to solve equations in $R[[T]]$ than in $R[T]$. For example:

Lemma 2.1. *1. The element $x = \sum_{i=0}^{\infty} a_i T^i$ is a unit in $R[[T]]$ (i.e., $xy = 1$ has a solution y) if and only if a_0 is a unit in R*

2. The element $x = \sum_{i=0}^{n} a_i T^i$ is a unit in $R[T]$ if and only if $a_0 \in R$ is a unit and $a_1, a_2, \dots, a_n$ are nilpotent.

Proof. 1. "$\Rightarrow$": $f : R[[T]] \to R$ defined by $x = \sum a_i T^i \mapsto a_0$ is a ring map. Hence x is a unit $\Rightarrow f(x) = a_0$ is a unit.
"$\Leftarrow$": $1 - fT$ is a unit for all $f \in R[[T]]$ with inverse $\sum_{i=0}^{\infty} f^i T^i$ (Exercise!). For $x = \sum_{i=0}^{\infty} a_i T^i, a_0$ a unit, the element $x = a_0(1 - T\sum -\frac{a_i}{a_0} T^{i-1})$ is the product of two units, hence a unit.
2. is left as an exercise. □

Remark 2.2. $R[T] \to R[[T]]$ induces an isomorphism $R[T]/T^n \cong R[[T]]/T^n$ (Exercise!)

Example. Let $p \in \mathbb{Z}$ be a prime. The p-adic completion of $\mathbb{Z}$ (or of $\mathbb{Z}_{(p)}$) is $\widehat{\mathbb{Z}}_p = \mathbb{Z}_p = \mathbb{Z}[[T]]/(p - T)$. This is the ring of *$p$-adic integers*. An element $x = \sum_{i\geq 0} a_i T^i \in \mathbb{Z}_p$ is in *canonical* form if $0 \leq a_i < p \,\forall i \in \mathbb{N}$. We have a natural map $\mathbb{Z} \to \mathbb{Z}_p$ defined by $n \mapsto n$. This is called the *completion map*.

Lemma 2.3. *1. Every $x \in \mathbb{Z}_p$ has a unique representative in canonical form.*

2. The map $\mathbb{Z} \to \mathbb{Z}_p$ induces an isomorphism $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p \,\forall n \geq 1$

3. The map $\mathbb{Z}_p \to \{(x_1, x_2, \dots) | x_n \in \mathbb{Z}/p^n, x_{n+1} \equiv x_n \mod p^n\}$ defined by $x \mapsto (x \mod p, x \mod p^2, \dots)$ is an isomorphism of rings.

Proof. 1. Given any element $x = \sum a_i T^i \in \mathbb{Z}[[T]]$, we need to solve $\sum_{i\geq 0} a_i T^i = \sum_{i\geq 0} b_i T^i + (p - T)\sum_{i\geq 0} c_i T^i$ where $0 \leq b_i < p \,\forall i$ as the canonical representatives of x is the solutions $\sum_{i\geq 0} b_i T^i$ of this equation. The equation has a unique solution (hence a unique representative in canonical form) defined recursively by $c_i + a_{i+1} = b_{i+1} + pc_{i+1}$ for $i \geq -1$ where $0 \leq b_{i+1} < p$, $a_i, b_i, c_i \in \mathbb{Z}$, and $c_{-1} = 0$.

2.

$$
\begin{aligned}
\mathbb{Z}_p/p^n\mathbb{Z}_p &= \frac{\mathbb{Z}[[T]]}{(p^n, p-T)} \\
&= \frac{\mathbb{Z}[[T]]}{(T^n, p-T)} \qquad \text{(as } T = p\text{)} \\
&= \left(\frac{\mathbb{Z}[[T]]}{T^n}\right)/p-T \\
&= \left(\frac{\mathbb{Z}[T]}{T^n}\right)/p-T \quad \text{(Remark 2.2)} \\
&= \frac{\mathbb{Z}[T]}{(T^n, p-T)} \\
&= \frac{\mathbb{Z}[T]}{(p^n, p-T)} \qquad (T = p) \\
&= \left(\frac{\mathbb{Z}[T]}{p^n}\right)/p-T \\
&= (\mathbb{Z}/p^n\mathbb{Z})\,[T]/(p-T) \\
&\cong \mathbb{Z}/p^n\mathbb{Z}
\end{aligned}
$$

where the last isomorphism is defined by the map $T \mapsto p$

3. The map is well defined by 2. It is bijective by 1.

□

Remark. 1. It is easier to solve equations in $\mathbb{Z}_p$ than in $\mathbb{Z}$.

2. Sometimes knowing solutions in $\mathbb{Z}_p$ ($\mathbb{Q}_p = \mathrm{Frac}\mathbb{Z}_p$), tells us something about solutions in $\mathbb{Z}$ (or $\mathbb{Q}$) (The Hasse principle)

3. Lemma 2.3 part 3 says $\mathbb{Z}_p \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ (inverse limit to be defined below).

2.1 Inverse limits

Definition 2.4. An *inverse system* of sets (groups, modules, rings) is a sequence $\{A_\bullet \theta\} : \cdots \to A_3 \xrightarrow{\theta_3} A_2 \xrightarrow{\theta_2} A_1$ of sets (groups, modules, rings) where the *transition* (or *structure*) maps θ_i are homomorphisms of sets (groups, modules, rings).

Example. $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z} \to \cdots \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ where all the maps are defined by $1 \mapsto 1$. This is an inverse systems of rings.

Definition 2.5. Let $\to A_n \xrightarrow{\theta_n} A_{n-1} \xrightarrow{\theta_{n-1}} \dots \xrightarrow{\theta_2} A_1$ be an inverse system of sets (groups, modules, rings). Its *inverse* (or *projective*) *limit* is the subset of $\prod_{i\geq 1} A_i$

$$\varprojlim_{n\in\mathbb{N}}\{A_n\} = \{(a_1, a_2, a_3, \dots)|\theta_{n+1}a_{n+1} = a_n \,\forall n \geq 1\} \subset \prod_{i\geq 1} A_i$$

If $\{A_n\}$ is an inverse system of groups (modules, rings), then $\lim_{\leftarrow}\{A_n\}$ is a group (module,ring). In fact a subgroup (submodule, subring) of $\prod_{i\geq a} A_i$ because θ_n is a homomorphism for all n.

Example. From Lemma 2.3 we have $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ for the inverse system $\cdots \to \mathbb{Z}/p^n\mathbb{Z} \to \cdots \to \mathbb{Z}/p\mathbb{Z}$

Definition 2.6. A *map of inverse systems* $f : \{A_\bullet, \theta^A\} \to \{B_\bullet, \theta^B\}$ of groups (rings, modules) is a sequence of homomorphism $f_i : A_i \to B_i$ of groups (rings, modules) commuting with the transition maps: $\theta_i^B \circ f_i = f_{i-1} \circ \theta_i^A \,\forall i$

Remark. A map $f : \{A_\bullet\} \to \{B_\bullet\}$ of inverse systems induces a map of inverse limits

$$f = \varprojlim f : \varprojlim\{A_\bullet\} \to \varprojlim\{B_\bullet\}$$

$$(a_1, a_2, a_3, \dots) \mapsto (f(a_1), f(a_2), f(a_3), \dots)$$

Lemma 2.7. *Let $\{A_\bullet, \theta^A\} \to \{B_\bullet, \theta^B\} \to \{C_\bullet, \theta^C\}$ be a sequence of inverse systems of abelian groups.*

1. *If $\forall n\ 0 \to A_n \to B_n \to C_n$ is exact then $0 \to \varprojlim\{A_\bullet\} \to \varprojlim\{B_\bullet\} \to \varprojlim\{C_\bullet\}$ is exact.*
2. *If $\forall n\ 0 \to A_n \to B_n \to C_n \to 0$ exact and $\{A_\bullet\}$ is a surjective system, i.e., $\theta_n : A_n \to A_{n-1}$ is surjective for all n, then $0 \to \varprojlim\{A_\bullet\} \to \varprojlim\{B_\bullet\} \to \varprojlim\{C_\bullet\} \to 0$ is exact.*

Proof. If $\{A_\bullet, \theta_\bullet\}$ is an inverse system of abelian groups, then

$$\varprojlim A_\bullet = \ker\left\{\prod_{i\geq 1} A_i \overset{1-\theta}{\to} \prod_{i\geq 1} A_i \text{ defined by } (a_1, a_2, \dots) \mapsto (a_1 - \theta a_2, a_2 - \theta a_3, \dots)\right\} \quad (*)$$

1. $\prod_{i\geq 1}$ preserves exact sequence, so we get maps of exact sequence:

$$\begin{tikzcd} 0 \arrow[r] & \prod A_i \arrow[r] \arrow[d, "1-\theta^A"'] & \prod B_i \arrow[r] \arrow[d, "1-\theta^B"'] & \prod C_i \arrow[d, "1-\theta^C"'] \\ 0 \arrow[r] & \prod A_i \arrow[r] & \prod B_i \arrow[r] & \prod C_i \end{tikzcd}$$

   Taking the kernels of vertical maps we get $0 \to \ker(1-\theta^A) \to \ker(1-\theta^B) \to \ker(1-\theta^C)$ is exact. So then $(*)$ implies the result.

2. By assumption we get a map of exact sequence:

$$\begin{tikzcd} 0 \arrow[r] & \prod A_i \arrow[r] \arrow[d, "1-\theta^A"'] & \prod B_i \arrow[r] \arrow[d, "1-\theta^B"'] & \prod C_i \arrow[r] \arrow[d, "1-\theta^C"'] & 0 \\ 0 \arrow[r] & \prod A_i \arrow[r] & \prod B_i \arrow[r] & \prod C_i \arrow[r] & 0 \end{tikzcd}$$

   By the Snake Lemma we have

$$0 \to \ker(1-\theta^A) \to \ker(1-\theta^B) \to \ker(1-\theta^C) \to \operatorname{coker}(1-\theta^A) \to \operatorname{coker}(1-\theta^B) \to \operatorname{coker}(1-\theta^C) \to 0 \quad (**)$$

   is exact. Since $\{A_\bullet\}$ is a surjective inverse system we have $1-\theta : \prod A_i \to \prod A_i$ defined by $(a_1, a_2, \dots) \mapsto (a_1 - \theta a_2, a_2 - \theta a_3, \dots)$ is surjective. This is because one can solve the equation $a - \theta(a) = b$ for any $b = (b_1, b_2, b_3, \dots)$ recursively by solving $\theta a_{n+1} = a_n - b_n, a_1 = 0$ (which has a solution because θ is surjective). Since $1-\theta^A$ is surjective we have $\operatorname{coker}(1-\theta^A) = 0$. Together with $(*)$ and $(**)$ we have the result.

□

2.2 Cauchy sequences and completions

Definition 2.8. Let $M \supset M_1 \supset M_2 \supset \dots$ be a descending chain of submodules. A sequence $\{x_i\} = (x_1, x_2, x_3, \dots)$ of elements $x_i \in M$ is said to *converge* to $x \in M$ (in the $\{M_\bullet\}$ topology) if $\forall n\, \exists N$ such that $\forall i \geq N, x_i - x \in M_n$. In this case we write $\{x_i\} \to x$.

A sequence $\{x_i\}$ is called a *Cauchy sequence* (for the $\{M_\bullet\}$ topology) if $\forall n\, \exists N$ such that $\forall i, j \geq N, x_i - x_j \in M_n$

Example. Not every Cauchy sequence needs to converge: $\{x_n\}$ defined by $x_n = 1 + T + T^2 + \dots + T^n \in k[T]$ does not converge in the $\{(T^n)\}$ topology on $k[T]$, (i.e., the descending chain is $k[T] \supset (T) \supset (T^2) \supset (T^3) \supset \dots$). For if $x_n \to f \in k[T]$ then $\forall m\ \exists N$, $x_n - f \in (T^m)\, \forall n \geq N$. This means $f = 1 + T + \dots + T^{m-1}$+higher order terms $\forall m$. But no such polynomial exists in $k[T]$. However the sequence is Cauchy (exercise).

Definition 2.9. A module M is *complete* (in the $M_\bullet$ topology) if every Cauchy sequence in M converges (in the $M_\bullet$ topology).

Definition 2.10. Let M be a module with a filtration $M_\bullet$: $M \supset M_1 \supset M_2 \supset \dots$. Let $\{x_i\}, \{y_i\}$ be two Cauchy sequence (for $M_\bullet$ topology). We say $\{x_i\} \sim \{y_i\}$ is $\{x_i - y_i\} \to 0$.

(Exercise: check that this is indeed an equivalence relation on the set of Cauchy sequences (with respect to $M_\bullet$))

We define the *completion* on M (with respect to $M_\bullet$) to be $\widehat{M} = \{$equivalence classes of Cauchy Sequence$\}$. This comes equipped with the map $M \to \widehat{M}$ defined by $x \mapsto x =$ constant sequence $\{x_i = x\}$

Remark. M is complete if and only if $M \to \widehat{M} : x \mapsto x$ is bijective.

Exercise. Check that $\{x_i\} \sim \{\overline{x}_i\}, \{y_i\} \sim \{\overline{y}_i\}$ implies $\{x_i + y_i\} \sim \{\overline{x_i} + \overline{y_i}\}$ and $\{rx_i\} \sim \{r\overline{x_i}\}$. Hence $\widehat{M}$ is an R-module and $M \to \widehat{M}$ is R-linear.

Given a filtration $M \supset M_1 \supset M_2 \supset \dots$ we get an inverse system: $\dots \twoheadrightarrow M/M_3 \twoheadrightarrow M/M_2 \twoheadrightarrow M/M_1$. We want to construct a map $\widehat{M} \to \varprojlim M/M_n$ as follows: Let $\{x_i\}$ be a Cauchy sequence, fix $n \in \mathbb{N}$. Look at the sequence $\{x_i + M_n\}$ in M/M_n. This sequence is eventually constant because there $\exists N \, \forall i, j \geq N$ we have $x_i - x_j \in M_n$ (i.e., $x_i = x_j \in M/M_n$). So let $\xi_n := \varinjlim \{x_i + M_n\}$ be the common eventually constant value. If $\{x_i\} \sim \{y_i\}$ then $\exists N \, \forall i \geq N, x_i = y_i \in M/M_n \Rightarrow \lim\{x_i + M_n\} = \lim\{y_i + M_n\} \in M/M_n$. So this defines a map $\widehat{M} \to M/M_n$ by $\{x_i\} \mapsto \xi_n = \lim\{x_i + M_n\}$, which is R-linear. Note that $\xi_{n+1} = \xi_n \in M/M_n$. So we obtain a module map $\widehat{M} \to \varprojlim M/M_n$

Lemma 2.11. *Let M be an R-module with filtration $M_\bullet : M \supset M_1 \supset M_2 \supset \dots$ by submodules then:*

1. *The map $\widehat{M} \to \varprojlim M/M_n$ defined by $\{x_i\} \mapsto (\lim\{x_i + M_1\}, \lim(x_i + M_2), \dots)$ is an isomorphism.*
2. *The map $M \to \widehat{M}$ induces isomorphism $M/M_n \to \widehat{M}/\widehat{M_n}$ where $\widehat{M_n}$ is the completion of M_n with respect to the filtration $M_n \supset M_{n+1} \supset M_{n+2} \supset \dots$.*
3. *$\widehat{M}$ is complete with respect to the filtration $\{\widehat{M_n}\}$.*

Proof. 1. Let $f : \widehat{M} \to \varprojlim M/M_n \subset \prod_{n \geq 1} M/M_n$.

We show that this is injective. Let $\{x_i\}$ be a Cauchy sequence. Fix $n \in \mathbb{N}$, if $\lim(x_i + M_n) = 0 \in M/M_n$. Then $\exists N \, \forall i \geq N$, $x_i \in M_n$. So if $f(\{x_i\}) = 0$ then $\forall n \, \exists N \, \forall i \geq N$ such that $x_i \in M_n \Rightarrow \{x_i\} \sim 0$, hence $0 = \{x_i\} \in \widehat{M}$. So f is injective.

Next we show that f is surjective. Let $(\xi_1, \xi_2, \xi_3, \dots) \in \varprojlim M/M_n$. Choose $x_n \in M$ such that $x_n + M_n = \xi_n \in M/M_n$, then $\{x_i\}$ is a Cauchy sequence because $\forall n \, \exists N = n$ such that $\forall i, j \geq N = n$: $x_i - x_j = \xi_i - \xi_j \in M/M_n$, i.e., $x_i - x_j \in M_n$. This defines $\{x_i\} \in \widehat{M}$ and by definition $f(\{x_i\}) = (\xi_1, \xi_2, \dots) \in \varprojlim M/M_n$

2. For all $k \geq n$ we have an exact sequence

$$0 \longrightarrow M_n/M_k \longrightarrow M/M_k \longrightarrow M/M_n \longrightarrow 0$$

and $\dots \twoheadrightarrow M_n/M_{k+1} \twoheadrightarrow M_n/M_k$ is a surjective system. Hence

$$0 \longrightarrow \underbrace{\varprojlim_k M_n/M_k}_{=\widehat{M_n}} \longrightarrow \underbrace{\varprojlim_k M/M_k}_{=\widehat{M}} \longrightarrow \underbrace{\varprojlim_k M/M_n}_{=M/M_n} \longrightarrow 0$$

where the equality follows from 1. So we get the exact sequence

$$0 \longrightarrow \widehat{M_n} \longrightarrow \widehat{M} \longrightarrow M/M_n \longrightarrow 0$$

hence $\widehat{M}/\widehat{M_n} \cong M/M_n$

3. $\widehat{M} \to \widehat{\widehat{M}}$ is an isomorphism because

$$\begin{aligned} \widehat{\widehat{M}} &\cong \varprojlim \widehat{M}/\widehat{M_n} && \text{by 1} \\ &\cong \varprojlim M/M_n && \text{by 2} \\ &\cong \widehat{M} && \text{by 1} \end{aligned}$$

□

Remark. If R is a ring and $R \supset I_1 \supset I_2 \supset I_3 \supset \dots$ is a filtration by ideals, then $\widehat{R}$ is a ring with multiplication $\{x_i\} \cdot \{y_i\} := \{x_i y_i\}$. (Check that this is independent of choice of representative). The map $R \to \widehat{R}$ defined by $x \mapsto x$ =constant sequence, is a ring homomorphism.

Definition 2.12. Let $I \subset R$ be an ideal. Then the completion of R with respect to the I-adic filtration $R \supset I \supset I^2 \supset I^3 \supset \ldots$ is called the *I-adic completion of* R. It is denoted by $\widehat{R} = \widehat{R}_I$.

Example. $\mathbb{Z}_p$ is the p-adic completion of $\mathbb{Z}$.

Remark. $\widehat{R}_I \cong \varprojlim_n R/I^n$

2.3 Filtrations

Definition 2.13. Let $I \subset R$ be an ideal, M an R-module with filtration $M_\bullet : M = M_0 \supset M_1 \supset M_2 \supset \ldots$. The filtration is called *I-filtration* if $IM_n \subset M_{n+1}\ \forall n$.

Remark. (Exercise) If $M_\bullet$ is an I-filtration then $\widehat{M}$ is an $\widehat{R}_I$-module via the multiplication map $\widehat{R}_I \times \widehat{M} \to \widehat{M}$defined by $(\{a_i\}, \{x_i\}) \mapsto \{a_i x_i\}$.

Example. If M is any R-module, then $\{I^n M\}_{n\geq 0}$ is an I-filtration. The completion of M with respect to $\{I^n M\}_{n\geq 0}$ is called the *I-adic completion* of M. This is denoted $\widehat{M_I}$.

Definition 2.14. An I-filtration $M_\bullet$ on an R-module M is called *stable* if $\exists N$ such that $\forall n \geq N$, $IM_n = M_{n+1}$

Example. $\{I^n M\}$ is a stable I-filtration.

Lemma 2.15. *Let M be an R-module, and $M_\bullet, M'_\bullet$ be two stable I-filtration of M. Then*

1. *A sequence $\{x_i\}$ in M is Cauchy with respect to $M_\bullet$ if and only if $\{x_i\}$ is Cauchy with respect to $M'_\bullet$*
2. *A sequence $\{x_i\}$ in M converges to 0 with respect to $M_\bullet$ if and only if $\{x_i\}$ converges to 0 with respect to $M'_\bullet$*
3. *The completion of M with respect to $M_\bullet$ is the same as the completion of M with respect to $M'_\bullet$.*

Proof. $\{I^n M\}$ is a stable I-filtration (and assume $M'_\bullet = \{I^n M\}$). $M_\bullet$ is stable means $\exists n \forall k \geq 0$ such that $I^k M_n = M_{n+k}$. Since $M_\bullet$ is an I-filtration, we have $I^k M \subset M_k = I^{k-n} M_n \subset I^{k-n} M\ \forall k \geq n$. This implies 1. and 2. as $\{x_i\}$ Cauchy for $\{I^n M\}$ then $\{x_i\}$ is Cauchy for $\{M_\bullet\}$ since $I^n M \subset M_n$, while if $\{x_i\}$ is Cauchy for $\{M_\bullet\}$ then $\{x_i\}$ is Cauchy for $\{I^n M\}$ since $M_k \subset I^{n-k} M\ \forall k \geq n$

Then clearly 1. and 2. implies 3. $\square$

2.4 Graded rings and the Artin-Rees Lemma

Definition 2.16. A *graded ring* is a ring A together with abelian subgroups $A_n \subset A, n \in \mathbb{Z}_{\geq 0}$ such that $A = \oplus_{n\geq 0} A_n$, $1 \in A_0$, and $A_n A_m \subset A_{n+m}$. The elements of A_n in a graded ring A are called *homogeneous elements of degree n.*

Example. The polynomial ring $A = k[T_1, \ldots T_k]$ is a graded ring with $A_n = \{$homogeneous polynomials of total degree $n\}$.

If $I \subset R$ ideal, then $A = \oplus_{n\geq 0} I^n$ is a graded ring where $I^0 = R$.

Definition 2.17. If $I \subset R$ ideal, then we set $\mathrm{gr}_I R = \oplus_{n\geq 0} I^n / I^{n+1}$. This is a graded ring with multiplication $I^n/I^{n+1} \times I^m/I^{m+1} \to I^{n+m}/I^{n+m+1}$ defined by $(a + I^{n+1}, b + I^{m+1}) \mapsto ab + I^{n+m+1}$. The ring $\mathrm{gr}_I R$ is called the *associated graded ring* of $R \supset I \supset I^2 \supset \ldots$

Lemma 2.18. *If R is a Noetherian ring, $I \subset R$ an ideal, then the graded ring $A = \oplus_{n\geq 0} I^n$ is also Noetherian.*

Proof. R being Noetherian implies I is a finitely generated R-module, say by $x_1, \ldots, x_n \in I$. Then the R-algebra map $R[T_1, \ldots, T_n] \to A = \oplus_{n\geq 0} I^n$ defined by $T_i \mapsto x_i$ is surjective. (It is surjective because $x_1, \ldots, x_n$ generates I). Since R is Noetherian, Hilbert's Basis Theorem implies $R[T_1, \ldots, T_n]$ Noetherian and hence any quotient of $R[T_1, \ldots, T_n]$ is Noetherian. Hence we have $A = \oplus_{n\geq 0} I^n$ is Noetherian. $\square$

Definition 2.19. Let A be a graded ring, $A = \oplus_{n\geq 0} A_n$. Then a graded A-module is an A-module M together with subgroups $M_n \subset M$ such that $M = \oplus_{n\geq 0} M_n$ and $A_m M_n \subset M_{m+n}$.

Example. If M is an R-module with an I-filtration $M_\bullet$ then $\oplus_{n\geq 0} M_n$ is a graded $A = \oplus_{n\geq 0} I^n$-module.

Lemma 2.20. *Let R be a Noetherian ring, $I \subset R$ an ideal, M a finitely generated R-module together with an I-filtration $M = M_0 \supset M_1 \supset M_2 \supset \dots$. Then the filtration $M_\bullet$ is stable if and only if $\oplus_{n\geq 0} M_n$ is a finitely generated $A = \oplus_{n\geq 0} I^n$-module.*

Proof. "$\Rightarrow$" Assume $M_\bullet$ is a stable I-filtration . Then $\exists n \forall k \geq 0$ such that $I^k M_n = M_{n+k}$. This implies $\oplus_{n\geq 0} M_n = M_0 \oplus M_1 \oplus \dots \oplus M_{n-1} \oplus M_n \oplus IM_n \oplus I^2 M_n \oplus I^3 M_n \oplus \dots \Rightarrow \oplus_{n\geq 0} M_n$ is generated by $M_0 \oplus \dots \oplus M_n$ as A-module. Since R is Noetherian and M is finitely generated implies $M_i \subset M$ are all finitely generated. Hence $M_0 \oplus \dots \oplus M_n$ generated by finitely many elements and so $\oplus_{n\geq 0} M_n$ is generated by these finitely many elements as A-modules

"$\Leftarrow$" Assume $\oplus_{n\geq 0} M_n$ is a finitely generated $A = \oplus_{n\geq 0} I^n$-module. Let $P_K = M_0 \oplus M_1 \oplus \dots \oplus M_K \oplus IM_K \oplus I^2 M_K \oplus I^3 M_K \oplus \dots$. Now P_K is a graded A-submodule of $\oplus_{n\geq 0} M_n$, we have $P_0 \subset P_1 \subset P_2 \subset \dots \subset \oplus_{n\geq 0} M_n$ an ascending chain of A-submodules. Now R is Noetherian implies A is Noetherian by lemma 2.18. By assumption $\oplus_{n\geq 0} M_n$ is a finitely generated A-module, hence a Noetherian A-module, so the chain $P_\bullet$ has to stop, i.e., $\exists_N$ such that $P_N = P_{N+1} = P_{N+2} = \dots$. But $\cup_k P_k = \oplus_{n\geq 0} M_n$ implies $\oplus_{n\geq 0} M_n = P_N \Rightarrow M_n = I^{n-N} M_N \, \forall n \geq N$, i.e., the filtration is stable.

$\square$

Artin-Rees Lemma. *Let R be a Noetherian ring, $I \subset R$ an ideal and M a finitely generated R-module with stable I-filtration $M_\bullet$. Let $N \subset M$ be a submodule. Then the filtration $\{N \cap M_n\}$ on N is a stable I-filtration of N.*

Proof. R Noetherian, $I \subset R$ an ideal, then $A = \oplus_{i\geq 0} I^n$ is Noetherian. Recall (Lemma 2.20): $P_\bullet$ is a stable I-filtration on a finitely generated R-module P if and only if $\oplus_{n\geq 0} P_n$ is a finitely generated A-module

So $\{M_n\}$ is a stable I-filtration on M implies $\oplus_{n\geq 0} M_n$ is a finitely generated A-module. Now $\oplus_{n\geq 0} M_n \cap N \subset \oplus_{n\geq 0} M_n$ is a A-submodule. Since A is Noetherian and $\oplus_{n\geq 0} M_n$ is a finitely generated A-module, the submodule $\oplus_{n\geq 0} M_n \cap N$ is also a finitely generated A-module. Hence $\{M_n \cap N\}$ is a stable I-filtration $\square$

Theorem 2.21 (Usual formulation of Artin-Rees Lemma)**.** *Let R be a Noetherian ring, $I \subset R$ an ideal, M a finitely generated R-module and $N \subset M$ a submodule. Then $\exists K$ such that $\forall n \geq K$, $N \cap I^n = I^{n-K}(N \cap I^K M)$*

Proof. $\{I^n M\}$ is a stable I-filtration implies by Artin-Rees Lemma that $\{N \cap I^n M\}$ stable I-filtration. This means $\exists K$ such that $\forall n \geq K$, $N \cap I^n M = I^{n-K}(N \cap I^K M)$ $\square$

Theorem 2.22. *Let R be a Noetherian ring, $I \subset R$ an ideal. Let*

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$$

be an exact sequence of finitely generated R-module. Then the sequence of I-adic completions

$$0 \longrightarrow \widehat{M} \longrightarrow \widehat{N} \longrightarrow \widehat{P} \longrightarrow 0$$

is exact

Proof. $\widehat{M}, \widehat{N}, \widehat{P}$ are the completion of M, N, P with respect to the filtration $\{I^n M\}, \{I^n N\}, \{I^n P\}$. So we have the exact sequence $\forall n$

$$0 \longrightarrow M/M \cap I^n N \longrightarrow N/I^n N \longrightarrow P/I^n P \longrightarrow 0 \qquad (*)$$

Now $\{M \cap I^n N\}$ is a stable I-filtration (Artin-Rees lemma). Hence by Lemma 2.15 the completion of M with respect to $\{M \cap I^n N\}$ is the completion $\widehat{M}$ of M with respect to $I^n M$. Now $\{M/M \cap I^n N\}$ is a surjective inverse system, so by $(*)$

$$\begin{array}{ccccccc} 0 \longrightarrow & \varprojlim M/M \cap I^n N & \longrightarrow & \varprojlim N/I^n N & \longrightarrow & \varprojlim P/I^n P & \longrightarrow 0 \\ & \parallel & & \parallel & & \parallel & \\ & \widehat{M} & & \widehat{N} & & \widehat{P} & \end{array}$$

is exact $\square$

Lemma 2.23. *Let R be a Noetherian ring, $I \subset R$ an ideal, M a finitely generated R-module, $\widehat{M} = \widehat{M}_I$. Then $\widehat{R} \otimes_R M \to \widehat{M}$ defined by $\{a_i\} \otimes x \mapsto \{a_i x\}$ is an isomorphism.*

Proof. Lemma is true for $M = R$. Let M be a finitely generated R-module. Then there exists a surjective R-module homomorphism $g : R^n \twoheadrightarrow M$. Now $\ker(g)$ is finitely generated because R^n is a Noetherian R-module. Hence there exists surjective $f : R^m \twoheadrightarrow \ker(g)$. Hence we have the exact sequence

$$R^m \xrightarrow{f} R^n \xrightarrow{g} M \longrightarrow 0 \qquad (*)$$

Now tensor product is a right exact functor (i.e., it sends $(*)$ to an exact sequence). Apply $\widehat{R} \otimes_R \_\_$ to $(*)$ to obtain an exact sequence

$$\begin{tikzcd} \widehat{R} \otimes_R R^m \arrow[r, "1\otimes f"] \arrow[d, "(1)"] & \widehat{R} \otimes_R R^n \arrow[r, "g"] \arrow[d, "(2)"] & \widehat{R} \otimes_R M \arrow[r] \arrow[d] & 0 \\ \widehat{R^m} \arrow[r, "\widehat{f}"] & \widehat{R^n} \arrow[r] & \widehat{M} \arrow[r] & 0 \end{tikzcd}$$

where the second sequence is exact, by Theorem 2.22. Now $\widehat{R} \otimes_R R^m \cong \widehat{R}^m$ and $\widehat{R}^m = \widehat{R^m}$ implies that (1) and (2) are isomorphism. Hence $\operatorname{coker}(1 \otimes f) \cong \operatorname{coker}(\widehat{f}) \Rightarrow \widehat{R} \otimes_R M \cong \widehat{M}$ ☐

2.5 Flat modules and Krull's Intersection Theorem

Definition 2.24. A map of rings $R \to S$ is called *flat* if the functor R-modules $\to$ S-modules defined by $M \mapsto S \otimes_R M$ preserves exact sequence, i.e., if

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$$

is an exact sequence of R-modules then

$$0 \longrightarrow S \otimes_R M \longrightarrow S \otimes_R N \longrightarrow S \otimes_R P \longrightarrow 0$$

is an exact sequence of S-modules.

Remark. Since tensor product is right exact, so

$$S \otimes_R M \longrightarrow S \otimes_R N \longrightarrow S \otimes_R P \longrightarrow 0$$

is exact for any ring map $R \to S$. Hence $R \to S$ is flat if and only if $S \otimes_R M \to S \otimes_R N$ is injective $\forall M \to N$ injective.

Theorem 2.25. *Let R be a Noetherian ring, $I \subset R$ an ideal, and $\widehat{R} = \widehat{R}_I$. Then $R \to \widehat{R}$ defined by $x \mapsto \{x\}$ is flat.*

Proof. Let $f : M \subset N$ be an inclusion of R-modules. We need to show that $1 \otimes f : \widehat{R} \otimes_R M \to \widehat{R} \otimes_R N$ is injective. We already proved this when M, N are finitely generated R-modules (Theorem 2.22, Lemma 2.23).

Let $x \in \widehat{R} \otimes_R M$ such that $(1 \otimes f)(x) = 0$. Now $x = \sum_{i=1}^n a_i \otimes x_i$ for some $a_i \in \widehat{R}$ and $x_i \in M$. Hence $0 = (1 \otimes f)(x) = \sum_{i=1}^n a_i \otimes f(x_i) \in \widehat{R} \otimes_R N$. Recall that by construction $\widehat{R} \otimes_R N = \oplus_{\widehat{R} \times N} R / \langle \text{relations} \rangle$. This means $\sum_{i=1}^n a_i \otimes f(x_i) \in \langle \text{relations} \rangle$. Hence $\sum_{i=0}^n a_i \otimes f(x_i)$ is a finite sum of finitely many generators of $\langle \text{relations} \rangle$ involving finitely many elements in N. Let $N_0 \subset N$ be the R-submodule generated by those finitely many elements and $f(x_1), \ldots, f(x_n)$. Then $\sum_{i=0}^n a_i \otimes f(x_i) = 0 \in \widehat{R} \otimes_R N_0$, but $M \cap N_0 \subset N_0$ is injective map of finitely generated R-modules (R is Noetherian). Hence $\widehat{R} \otimes_R (M \cap N_0) \to \widehat{R} \otimes_R N_0$ is injective, and $x = \sum a_i \otimes x_i \mapsto 0$, hence $0 = x \in \widehat{R} \otimes_R (M \cap N_0) \Rightarrow 0 = x \in \widehat{R} \otimes_R M$. Hence we have showed $1 \otimes f$ is injective. ☐

Lemma 2.26. *Let R be a ring, M a finitely generated R-module and $I \subset R$ an ideal. If $IM = M$ then there exists $a \in I$ such that $(I + a)M = 0$*

Proof. If $B \in M_n(R)$, let $B^\#$ be the adjugate matrix. Then $B^\# B = BB^\# = \det B \cdot I_n$

Let $x_1, \ldots, x_n \in M$ generate M. $IM = M \Rightarrow \forall i \exists a_{ij} \in I$ such that $x_i = \sum_{j=1}^n a_{ij} x_j$. Set $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ then $x = Ax$ for $A = (a_{ij}) \in M_n(I)$. Hence $(1 - A)x = 0$, so let $(1 - A)^\#$ be the adjugate of $(1 - A)$ then $0 = (1 - A)^\#(1 - A)x = \det(1 - A) \cdot x$. But $\det(1 - A) = 1 + a$ for some $a \in I$ since $A \in M_n(I)$. Hence $(1 + a)x_i = 0 \forall i \Rightarrow (1 + a)M = 0$ ☐

Krull Intersection Theorem. *Let R be a Noetherian ring and $I \subset R$ a proper ideal. If either R is a domain or $I \subset J(R) = \bigcap_{M \subset R \text{ max ideal}} M$ (the Jacobson radical). Then $\bigcap_{n \geq 1} I^n = 0$.*

Proof. Let $N = \bigcap_{n \geq 1} I^n \subset R$. Then $\{N \cap I^k\}$ is a stable I-filtration on N by Artin-Rees lemma. Now $N \cap I^k = N$ implies by stable I-filtration that $IN = N$. Then by the previous lemma $\exists a \in I$ such that $(1+a)N = 0$ (N is finitely generated because R is Noetherian and $N \subset R$).

If R is a domain, then $1+a$ is a non-zero divisor because $1+a \neq 0$ (since $I \neq R$) hence $(1+a)N = 0 \Rightarrow N = 0$

If $I \subset J(R)$ then $1+a$ is a unit, hence $(1+a)N = 0 \Rightarrow N = 0$ □

Lemma 2.27. *Let $A = A_0 \supset A_1 \supset \dots$ and $B = B_0 \supset B_1 \supset \dots$ be filtered modules and $f : A \to B$ a map of filtered modules (that is $f(A_i) \subset B_i$).*

1. *If $gr(f) : gr(A) \to gr(B)$ is surjective, then $\widehat{f} : \widehat{A} \to \widehat{B}$ is surjective. (Recall $gr(A) = \oplus_{i \geq 0} A_i/A_{i+1}$)*
2. *If $gr(f) : gr(A) \to gr(B)$ is injective, then $\widehat{f} : \widehat{A} \to \widehat{B}$ is injective.*

Proof. Consider the commutative diagram with exact rows:

$$\begin{tikzcd} 0 \arrow[r] & A_i/A_{i+1} \arrow[r] \arrow[d, "\mathrm{gr}_i(f)"'] & A/A_{i+1} \arrow[r] \arrow[d, "\alpha_{i+1}"'] & A/A_i \arrow[r] \arrow[d, "\alpha_i"'] & 0 \quad (*) \\ 0 \arrow[r] & B_i/B_{i+1} \arrow[r] & B/B_{i+1} \arrow[r] & B/B_i \arrow[r] & 0 \end{tikzcd}$$

Therefore, $\mathrm{gr}_i(f)$ and α_i surjective (injective) imply α_{i+1} surjective (injective). Since $\mathrm{gr}_0(f) = \alpha_0 : A/A_1 = A_0/A_1 \to B_0/B_1 = B/B_1$ is surjective (injective) by assumption of 1. (respectively of 2.), we have: α_i is surjective (injective) for all $i \geq 0$.

1. We have an inverse system of exact sequence

$$0 \longrightarrow \ker(\alpha_i) \longrightarrow A/A_i \xrightarrow{\alpha_i} B/B_i \longrightarrow 0 \quad (**)$$

Now we have $\ker(\alpha_{i+1}) \to \ker(\alpha_i)$ is surjective by the Snake Lemma applied to $(*)$ and $\mathrm{coker}(\mathrm{gr}_i(f)) = 0$. This means that $\{\ker(\alpha_i)\}$ is a surjective inverse system. So by taking $\varprojlim$ of $(**)$ yields an exact sequence:

$$0 \longrightarrow \varprojlim \ker(\alpha_i) \longrightarrow \widehat{A} \xrightarrow{\widehat{f}} \widehat{B} \longrightarrow 0$$

Hence $\widehat{f} : \widehat{A} \to \widehat{B}$ is surjective.

2. Since α_i is injective $\forall i$, the map $\prod \alpha_i : \prod A/A_i \to \prod B/B_i$ is injective. As $\widehat{A}$ and $\widehat{B}$ are submodules of source and target of that map, the map $\widehat{A} \to \widehat{B}$ is injective.

□

Lemma 2.28. *Let $I \subset R$ be an ideal of a ring R which is I-adically complete. Let M be an R-module with an I-filtration $M = M_0 \supset M_1 \supset M_2 \supset \dots$ such that $\bigcap_{i \geq 0} M_i = 0$. Then if $gr(M) = \oplus_{i \geq 0} M_i/M_{i+1}$ is a finitely generated $gr_I(R) = \oplus_{i \geq 0} I^i/I^{i+1}$-module, then M itself is a finitely generated R-module.*

Proof. Let $x_1, \dots, x_n \in \mathrm{gr}(M)$ generate $\mathrm{gr}(M)$ as $\mathrm{gr}_I(R)$ -module. Without loss of generality, we can assume x_i homogeneous of degree n_i. So $x_i \in \mathrm{gr}_{n_i}(M) = M_{n_i}/M_{n_i+1}$. Lift these x_i to $y_i \in M_{n_i}$.

Claim: $y_1, \dots, y_n \in M$ generates M as R-modules

Write R_i for the R-module R equipped with the I-filtration $\underbrace{R \supset R \supset R \supset \dots \supset R}_{n_i} \supset I \supset I^2 \supset \dots$. Then consider $f_i : R_i \to M$ defined by $1 \mapsto y_i$, this is a map of filtered R-modules. Hence $f = \oplus f_i : \oplus_{i=1}^n R_i \to M$. is a map of filtered R-modules such that $\mathrm{gr}(f) = \oplus_{i=1}^n \mathrm{gr}(R_i) \to \mathrm{gr}(M)$ is surjective. (Note that $\mathrm{gr}(R_i) = \mathrm{gr}(R)(-n_i)$

where $S(r)$ graded ring with $S(r)_i = S(r+i)$) Because $\mathrm{gr}(R_i) = \mathrm{gr}(R)(-n_i) \to \mathrm{gr}(M)$ is defined by 1 (in degree n_i) maps to x_i. Then the previous lemma implies $\widehat{f} : \widehat{\oplus_{i=1}^n R_i} \to \widehat{M}$ is surjective.

$$\begin{tikzcd}
\oplus_{i=1}^n R_i \arrow[r, "f"] \arrow[d, "(1)"'] & M \arrow[d, "(2)"] \\
\underset{=\oplus_{i=1}^n \widehat{R_i}}{\widehat{\oplus_{i=1}^n R_i}} \arrow[r, "\widehat{f}"'] & \widehat{M}
\end{tikzcd}$$

The map (1) is an isomorphism, because $\widehat{R}_i = \widehat{R}_I$ since the I-filtration on R_i is stable and $R \cong \widehat{R}_I$ as R is complete. Also the map (2) is injective because $\ker = \cap_{i \geq 0} M_i = 0$. Since $\widehat{f}$ is surjective, we have (2) is surjective, hence (2) is an isomorphism. So f is surjective. ☐

Theorem 2.29. *Let R be a Noetherian ring and $I \subset R$ an ideal. Then $\widehat{R} = \widehat{R}_I$ is Noetherian.*

Proof. Let $M \subset \widehat{R}$ be an $\widehat{R}$-ideal. We need to show that M is finitely generated $\widehat{R}$-module. Equip M with the filtration $\{M \cap \widehat{I}^n\}$. Then $\mathrm{gr} M = \oplus_{n \geq 0} (M \cap \widehat{I}^n)/(M \cap \widehat{I}^{n+1}) \to \mathrm{gr}_{\widehat{I}} \widehat{R} = \oplus_{n \geq 0} \widehat{I}^n / \widehat{I}^{n+1}$ is a submodule. R is Noetherian means $\widehat{I}^n = \widehat{I^n} \,(= I^n \otimes_R \widehat{R})$, hence $\mathrm{gr}_{\widehat{I}} \widehat{R} \cong \mathrm{gr}_I R = \oplus_{n \geq 0} I^n / I^{n+1}$. Also R being Noetherian implies $\mathrm{gr}_I R$ is Noetherian, hence the submodule $\mathrm{gr} M$ is also finitely generated as $\mathrm{gr}\widehat{R}$-module.

We want to use the previous lemma, so consider $\cap_{n \geq 0} M \cap \widehat{I}^n \subset \cap_{n \geq 0} \widehat{I}^n = \ker(\widehat{R} \overset{\cong}{\to} \widehat{\widehat{R}}) = 0$. So $\mathrm{gr} M$ is a finitely generated $\mathrm{gr}\widehat{R}$-module and thus M is a finitely generated $\widehat{R}$-module, by Lemma 2.28. Hence $\widehat{R}$ is Noetherian. ☐

2.6 Hensel's Lemma

Let R be any ring, recall that $R[[T_1, \ldots, T_n]]$ is the I-adic completion of $R[T_1, \ldots, T_m]$ where $I = (T_1, \ldots, T_n) \subset R[T_1, \ldots, T_n]$.

Lemma 2.30. *Let $f : R \to S$ be a ring homomorphism. Let $I \subset S$ be an ideal such that S is I-adically complete. For any $a_1, \ldots, a_n \in I$ there exists a unique ring homomorphism $F : R[[T_1, \ldots, T_n]] \to S$ such that $T_i \mapsto a_i$ and extending f, i.e. $F(T_i) = a_i$ and the following diagram commutes:*

$$\begin{tikzcd}
R[[T_1, \ldots T_n]] \arrow[dr, "F"] & \\
R \arrow[u] \arrow[r, "f"'] & S
\end{tikzcd}$$

Proof. Existence of F: There exists ring homomorphism $F_0 : R[T_1, \ldots, T_n] \to S$ such that $T_i \to a_i$ extending f. F_0 sends $J = (T_1, \ldots, T_n) \subset R[T_1, \ldots, T_n]$ into $I \subset R$. So $F_0(J^n) \subset I^n$ means we get a commutative diagram:

$$\begin{tikzcd}
R[T_1, \ldots, T_n] \arrow[r, "F_0"] \arrow[d] & S \arrow[d, "\phi"] \\
\underset{=R[[T_1, \ldots, T_n]]}{R[\widehat{T_1, \ldots,} T_n]} \arrow[r, "\widehat{F_0}"'] & \widehat{S}
\end{tikzcd}$$

Note that the completion map $\phi : S \to \widehat{S}$ is an isomorphism because S is I-adically complete. Set $F = \phi^{-1} \circ \widehat{F_0}$. Then F extends f

F is unique: Assume F' is another extension of f as in the lemma, and let $L : R[T_1, ..., T_n] \to R[[T_1, ..., T_n]]$ be the usual embedding. The map $j : S \underset{\phi}{\overset{\cong}{\to}} \widehat{S} \subset \prod_{n \geq 1} S/I^n$ is injective. So $(*)$ $F = F' \iff j \circ F = j \circ F' \iff R[[T_1, \ldots, T_n]] \underset{\rho_n \circ F'}{\overset{\rho_n \circ F'}{\rightrightarrows}} S/I^n$ agree for all n (where $\rho_n : S \to S/I^n$).

Now, if F', F extend f such that $F(T_i) = a_i = F'(T_i)$ then $F \circ L = F' \circ L$ and the following diagram commutes:

$$\begin{tikzcd}
R[T_1, \dots T_n] \arrow[r, "L"] \arrow[d] & R[[T_1, \dots, T_n]] \arrow[r, "F", "F'"'] \arrow[d] & S \arrow[d, "\rho_n"] \\
R[T_1, \dots, T_n]/J^n \arrow[r, equal] & R[[T_1, \dots, T_n]]/\widehat{J}^n \arrow[r, "F \bmod \widehat{J}^n", "F' \bmod \widehat{J}^n"'] & S/I^n
\end{tikzcd}$$

Hence $F \mod \widehat{J}^n = F' \mod \widehat{J}^n \, \forall n \Rightarrow \rho_n \circ F = \rho_n \circ F' \underset{(*)}{\Rightarrow} F = F'$

$\square$

Definition 2.31. Let $f \in R[[T]]$, $f = a_0 + a_1 T + a_2 T^2 + \cdots = \sum_{n=0}^{\infty} a_n T^n$. Define its *derivative* $f' \in R[[T]]$ as $f' = \sum_{n=1}^{\infty} a_n \cdot n T^{n-1}$. So $f(T) = f(0) + f'(0)T + hT^2$ for some $h \in R[[T]]$.

Remark. $\mathrm{gr}_{(T)} R[[T]] = \mathrm{gr}_{(T)} R[T] = \oplus_{n \geq 0} (T^n)/(T^{n+1}) \leftarrow R[X]$ defined by $X \mapsto T \mod T^2 \in \mathrm{gr}^1_{(T)} R[[T]] = (T)/(T^2)$. This is an isomorphism because in degree n this map is $X^n \cdot R \to (T^n)/(T^{n+1})$ defined by $X^n \mapsto T^n \mod T^{n+1}$, is a map of free R-modules of rank 1 sending generator to generator.

Lemma 2.32. *Let $f \in TR[[T]]$. If $f'(0) \in R$ is a unit then the map $\phi : R[[T]] \to R[[T]]$ defined by $T \mapsto f$ is an isomorphism which sends the ideal (T) isomorphically onto itself.*

Proof. Look at $\mathrm{gr}(\phi) : \mathrm{gr} R[[T]] \to \mathrm{gr} R[[T]]$. By the above remark we get the following

$$T \longmapsto f = f'(0)T \mod T^2$$

$$\begin{tikzcd}
T \mod T^2 & \mathrm{gr} R[[T]] \arrow[r, "\mathrm{gr}(\phi)"] & \mathrm{gr} R[[T]] \\
X \arrow[u, mapsto] & R[X] \arrow[u, "\cong"] \arrow[r] & R[X] \arrow[u, "\cong"']
\end{tikzcd}$$

$$X \longmapsto f'(0) \cdot X$$

where $f = \underbrace{f(0)}_{=0} + f'(0)T + T^2 h$. Since $f'(0)$ is a unit $\Rightarrow \mathrm{gr}(\phi)$ is an isomorphism of rings. Hence $\widehat{\phi} : \widehat{R[[T]]} \to \widehat{R[[T]]}$ is an isomorphism (Lemma 2.27), but $\widehat{R[[T]]} = R[[T]]$, hence ϕ is an isomorphism. For the last claim note that $f = T(f'(0) + Th)$ for some $h \in R[[T]]$. Therefore, $\phi((T)) = (f) = (T(f'(0) + Th)) = (T)$ since $(f'(0) + Th) \in R[[T]]$ is a unit, by Lemma 2.1. $\square$

Hensel's Lemma. *Let R be a ring which is I-adically complete for some $I \subset R$. Let $f \in R[T]$ be a polynomial.*

1. *If $f(a) = 0 \mod f'(a)^2 I$ (f has an approximate solution) then $\exists b \in R$ with $f(b) = 0 \in R$ such that $b = a \mod f'(a) I$ (f has a solution near a)*

2. *If in 1. $f'(a) \in R$ is a non-zero divisor, then $b \in R$ in 1. is unique.*

Proof. 1. f is a polynomial in $R[T]$ and set $e = f'(a)$. We can write $f(a + eT) = f(a) + f'(a)eT + h(T)e^2T^2$ for some $h \in R[T]$. So $f(a + eT) = f(a) + e^2(T + h(T)T^2)$. Let $g(T) = T + h(T)T^2 \in TR[T] \subset TR[[T]]$. Then $g'(T) = 1 + T\cdot$polynomial, $g'(0) = 1 \in R^*$.

By the previous lemma, the map $\phi : R[[T]] \to R[[T]]$ defined by $T \mapsto g$ is an isomorphism such that $\phi(J) = J$ where $J = (T)$

$$f(a + eT) = f(a) + e^2 g(T) \in R[[T]] \quad (*)$$

Note that ϕ^{-1} is R-algebra homomorphism, $f \in R[T]$, so they commute. Apply ϕ^{-1} to $(*)$ and we get

$$f(a + e \cdot \phi^{-1}(T)) = f(a) + e^2 \underbrace{\phi^{-1}(g(T))}_{T} \quad (**)$$

Recall that by assumption $f(a) = 0 \mod e^2 I$, so there exists $c \in I$ such that $f(a) = -e^2 c$. Since R is complete with respect to I, we get the R-algebra homomorphism $\psi : R[[T]] \to R$ defined by $T \mapsto c$. Now apply ψ to $(**)$

$$f(a + e \cdot \psi(\phi^{-1}T)) = f(a) + e^2 \psi(T) = -e^2 c + e^2 c = 0$$

Hence $b = a + e \cdot \psi(\phi^{-1}(T)) \in R$ such that $f(b) = 0 \in R$. Now $\phi^{-1}(T) \in (T)$, hence $\psi(\phi^{-1}(T)) \in \psi(T)R = cR \subset I$, hence $b = a \mod eI$.

2. Let $b_i = a + ed_i$ for $i = 1, 2$ be two solutions of f and $d_i \in I$, so $f(b_i) = 0 \in R$.

$$f(a + eT) = f(a) + e^2 \phi(T) \in R[[T]] \quad (*)$$

Since $d_i \in I$ and R is I-adically complete, there exists a unique$R$-algebra homomorphism $\beta_i : R[[T]] \to R$ defined by $T \mapsto d_i$. Now apply β_i to $(*)$, yields

$$\underbrace{f(a + e\beta_i(T))}_{f(b_i)} = f(a) + e^2 \beta_i \phi(T) \in R$$

so we get $0 = f(b_i) = f(a) + e^2 \beta_i \phi(T)$. Hence $e^2 \beta_1 \phi(T) = e^2 \beta_2 \phi(T) \in R$, and since $e = f'(a)$ is a non-zero divisor, we have $\beta_1(\phi T) = \beta_2(\phi T)$. So the two R-algebra homomorphisms $\beta_1 \circ \phi$, $\beta_2 \circ \phi : R[[T]] \to R$ agree on T. But there exists a unique such morphism, hence $\beta_1 \circ \phi = \beta_2 \circ \phi$ as maps $R[[T]] \to R$. Recall that $\phi : R[[T]] \to R[[T]]$ was an isomorphism, so $\beta_1 = \beta_2 : R[[T]] \to R$. Hence

$$\begin{aligned} b_1 &= a + ed_1 \\ &= a + e\beta_1(T) \\ &= a + e\beta_2(T) \\ &= a + ed_2 \\ &= b_2 \end{aligned}$$

□

Example. Which units in $\mathbb{Z}_p$ ($p \in \mathbb{Z}$ prime) are squares? I.e. For which $u \in \mathbb{Z}_p^*$ does $f(T) = T^2 - u$ has a root in $\mathbb{Z}_p$?

Hensel's lemma: If $f(T) = T^2 - u$ has a root a in $\mathbb{Z}_p / f'(a)^2 p\mathbb{Z}_p = \mathbb{Z}_p / 4a^2 p\mathbb{Z}_p$ then f has a root in $\mathbb{Z}_p$. Now $f(a) = 0 \mod 4a^2 p$ means $a^2 = u \mod 4a^2 p$. Since $u \in \mathbb{Z}_p^*$ we have $a \in \mathbb{Z}_p/(2a)^2 p\mathbb{Z}_p$ is a unit which implies $a \in \mathbb{Z}_p^*$ (as both rings are local with same residue field). So we have $\mathbb{Z}_p/(2a)^2 p\mathbb{Z}_p = \mathbb{Z}_p/4p\mathbb{Z}_p$. Hence we have that $u \in \mathbb{Z}_p^*$ is a square if and only if u is a square in $\mathbb{Z}_p/4p\mathbb{Z}_p = \begin{cases} \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} & p \text{ odd} \\ \mathbb{Z}_2/8\mathbb{Z}_2 = \mathbb{Z}/8\mathbb{Z} & p = 2 \end{cases}$.

2.7 Cohen's Structure Theorem

Next we want to prove (part of) Cohen's structure theorem.

Lemma 2.33. *Let R be a ring which is complete with respect to an ideal $I \subset R$. Then*

1. $1 - \epsilon \in R^* \, \forall \epsilon \in I$

2. *$a \in R$ is a unit in R if and only if $a \in (R/I)^*$*

Proof. 1. We claim the inverse of $1 - \epsilon$ is $\sum_{i=0}^{\infty} \epsilon^i$ which is Cauchy in I-adic topology because $\epsilon \in I$. Since R is complete $\sum_{i=0}^{\infty} \epsilon^i \in R$. Then by computation we see $(1 - \epsilon) \sum_{i=0}^{\infty} \epsilon^i = 1$

2. "$\Rightarrow$" if $a \in R$ is a unit, then $a \in (R/I)^*$ because $R \to R/I$ is a ring homomorphism.

"$\Leftarrow$" if $a \in R$ is a unit $\mod I$, then $\exists b \in R$ with $ab = 1 \mod I$. So $ab = 1 - \epsilon$ for some $\epsilon \in I$. Hence by part 1, $ab \in R^*$, hence a is a unit.

□

We summarize what we have proved about the completion of local Noetherian rings.

Theorem 2.34. *Let (R, m, k) be a Noetherian local ring. Then $\widehat{R} = \widehat{R}_m$ is a local Noetherian ring with maximal ideal $\widehat{m} = \widehat{R} \otimes_R m = m\widehat{R}$ and residue field $\widehat{R}/\widehat{m} = k$.*

Proof.

- R Noetherian means $\widehat{R}$ is Noetherian (Theorem 2.29)
- $\widehat{R}$ is complete with respect to $\widehat{m^n} = m \otimes_R \widehat{R} = m\widehat{R}$ (Lemma 2.11, Lemma 2.23).
- $\widehat{R}/\widehat{m} = R/m = k$ (Lemma 2.11 part 2) is a field, hence $\widehat{m} \subset \widehat{R}$ is a maximal ideal.

So it remains to show $\hat{R}$ is a local ring, that is, $\widehat{m} = mR$ is the unique maximal ideal. This is because $a \in \widehat{R}$ is a unit in $\widehat{R}$ if and only if (by the previous lemma) $a \in (\widehat{R}/\widehat{m})^*$, if and only if $a \notin \widehat{m}$. Hence $\widehat{R}^* = \widehat{R} - \widehat{m}$, so $\widehat{m}$ is the unique maximal ideal of $\widehat{R}$. ☐

Cohen Structure Theorem. *Let (R, m, k) be a local Noetherian ring which is m-adically complete. If R contains a field then $R \cong k[[T_1, \ldots, T_n]]/I$ for some $n \in \mathbb{N}$ and I an ideal.*

Proof. We will only cover the case when $\operatorname{char} k = 0$. (The other case requires a bit more work and some Galois Theory)

Let $\Sigma = \{L \subset R, L \text{ field}\}$, and order it by inclusion. By assumption $\Sigma \neq \emptyset$. If $\mathcal{C} \subset \Sigma$ is a chain, then $\cup_{L \subset \mathcal{C}} L \subset R$ is a field. Hence by Zorn's Lemma, Σ has maximal element, so R contains a maximal field, say $L \subset R$.

Claim: The composition $L \subset R \overset{g}{\twoheadrightarrow} k = R/m$ is an isomorphism (so $L \cong K$)

Assume $L \cong g(L) \subsetneq k$ ($g|_L$ is injective because $\ker(g) = 0$ since L is a field). Choose $x \in k \setminus g(L)$. Since g is surjective, there exists $y \in R$ such that $g(y) = x$.

Case 1. Assume x is not a root of a monic polynomial $f \in g(L)[T]$. Then $y \in R$ is not a root of a monic polynomial $f \in L[T]$ $(*)$.

So we can construct $h : L[T] \to R$ by $T \mapsto y$. This map is injective because $\ker(h) = f_0 L[T]$ where $f_0 \in L[T]$ is zero or monic. Hence by $(*)$, $f_0 = 0$ so h is injective.

$$\begin{tikzcd} L[T] \arrow[r, hook, "h"] \arrow[dr, "g"'] & R \arrow[d] \\ T \mapsto x & k \end{tikzcd}$$

$g|_{L[T]}$ is injective, since x is not a root of monic polynomial. If $0 \neq f_1 \in L[T] \Rightarrow 0 \neq g(f_1) \equiv f_1 \mod m$. Hence $f_1 \notin m$, and since R is local, $f_1 \in R^*$. Hence $\operatorname{Frac}(L[T]) = L(T) \subset R$. This is a contradiction of L being the maximal field in R.

Case 2. Assume x is a root of a monic polynomial $f \in g(L)[T]$, and let f be the minimal polynomial of $x \in k$. So, f is irreducible over $g(L)$ and $F = g^{-1}(f) \in L[T] \subset R[T]$ is irreducible over L. Since $\operatorname{char} k = 0$, f is separable, so $f'(x) \neq 0$ since $F'(y) = f'(x) \mod m \neq 0$. Hence $F'(y) \notin m$, so as R is local, $F'(y) \in R^*$.

So we use Hensel's Lemma (R is complete): F has a root $\mod m = \underbrace{F'(y)^2}_{\text{unit}} m$, namely x, hence F has a root in R, say $F(z) = 0$ for some $z \in R$.

Then we can construct $L[T]/F \to R$ by $T \mapsto z$, this is injective because

$$\begin{tikzcd} L[T]/F \arrow[r, "h"] \arrow[dr] & R \arrow[d, "g"] \\ & k \end{tikzcd}$$

gh is injective as $g(F) = f$ is minimal polynomial of x. Also note $L[T]/F$ is a field since F is irreducible over L, hence we have a contradiction to L being the maximal subfield of R.

Hence the two cases above show that $L \cong k$.

R is Noetherian, means $m \subset R$ is finitely generated, say by $x_1, \ldots, x_n \in m$. Since R is complete with respect to m, we construct a unique L-algebra map $h : L[[T_1, \ldots, T_n]] \to R$ by $T_i \mapsto x_i$. Now the map $\mathrm{gr}(h)$: $\mathrm{gr}(L[[T_1, \ldots, T_n]]) \to \mathrm{gr}_m R$ is surjective because

$$\begin{aligned} \mathrm{gr}_0(h) &: \quad L \cong k \\ \mathrm{gr}_1(h) &: \quad \frac{(T_1, \ldots, T_n)}{(T_1, \ldots, T_n)^2} \to \frac{m}{m^2} \text{ defined by} T_i \mapsto x_i \end{aligned}$$

where the second map is surjective because m is generated by $x_1, \ldots, x_n$. In general $\mathrm{gr}_I(A) = \oplus_{n \geq 0} I^n / I^{n+1}$ is generated as $\mathrm{gr}_0(A) = A/I$-algebra by $\mathrm{gr}_1(A) = I/I^2$. Hence $\mathrm{gr}(h)$ is surjective.

Since $L[[T_1, \ldots, T_n]]$ and R are complete, then $h : L[[T_1, \ldots, T_n]] \to R$ is surjective, so $R = L[[T_1, \ldots, T_n]]/I$ where $I = \ker(h)$ and $L \cong k$. $\square$

Remark. If R does not contain a field, we have (without proof):

Cohen Structure Theorem. Let (R, m, k) be a complete Noetherian local ring. If R does not contain a field, then there exist a DVR V such that $R = V[[T_1, \ldots, T_n]]/I$

3 Dimension Theory

In this section we will study dimension theory of local Noetherian rings and work toward proving:

Dimension Theorem. *Let (R, m, k) be a local Noetherian ring. Then the following three numbers are equal:*

- $\dim R = \max\{n \in \mathbb{N} | \exists P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n \subset R,\ P_i \,\text{prime ideal}\}$
- $1 + \deg$ *of the Hilbert polynomial of* $gr_m R = \oplus_{n\geq 0} m^n/m^{n+1}$
- $\min\{n \in \mathbb{N} | \exists x_1, \ldots, x_n \in m : R/(x_1, \ldots, x_n) \,\text{is Artinian}\}$

3.1 Length

Recall from Commutative Algebra the following:

Fact. *Let $R \neq 0$ be a Noetherian ring, then the following are equivalent:*

1. *R is Artinian*
2. $\dim R = 0$
3. *The Jacobson Radical is nilpotent*

Definition 3.1. A *simple* R-module is a module M such that $M \neq 0$ and $0, M \subset M$ are the only submodules.

Remark. M is simple if and only if $M \cong R/m$ for some $m \subset R$ a maximal ideal.

Definition 3.2. A *composition series* of M is a finite filtration $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ such that M_i/M_{i-1} is simple $\forall i = 1, \ldots n$. We say that a module has *finite length* if it has a composition series.

Lemma 3.3 (Rings and Modules)**.** *M has finite length if and only if M is Artinian and Noetherian.*

Definition 3.4. The *length* $l(M)$ of a finite length module M is $l(M) = n$ if there exists a composition series $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$. (This does not depend on the choice of composition series, proof of this can be found in Rings and Modules)

Lemma 3.5. *Let $0 \to M_1 \to M_2 \xrightarrow{g} M_3 \to 0$ be an exact sequence of finite length modules. Then $l(M_2) = l(M_1) + l(M_3)$*

Proof. Let $0 = M_1^0 \subset M_1^1 \subset \cdots \subset M_1^r = M_1$ and $0 = M_3^0 \subset M_3^1 \subset \cdots \subset M_3^s = M_3$ be composition series of M_1 and M_3. Then $0 = M_1^0 \subset M_1^1 \subset \cdots \subset M_1^r = M_1 = g^{-1}(M_0^3) \subset g^{-1}(M_1^3) \subset \ldots g^{-1}(M_3^2) = M$ is a composition series of M of length $r + s$. ☐

Example. Let (A, m, k) be an Artinian local ring, M a finitely generated A-module. Then M is Artinian (finitely generated over A) and Noetherian (finitely generated over A which is Noetherian), hence it has finite length.

Now A being Artinian (local) implies there exists n such that $m^n = 0$ and $0 = m^n M \subset m^{n-1} M \subset \cdots \subset mM \subset M$. Now $m^i M/m^{i+1}M$ is a finite dimensional $A/m = k$ vector space. Hence $l(m^i M/m^{i+1}M) = \dim_k(m^i M/m^{i+1}M)$, which means

$$l(M) = \sum_{i\geq 0} \dim_k \left(\frac{m^i M}{m^{i+1} M} \right)$$

3.2 Hilbert Polynomial

Consider graded rings $A = \oplus_{n\geq 0} A_n$ such that:

(†) A_0 is Artinian, A_1 is a finitely generated A_0-module and A is generated as an A_0-algebra by A_1

Remark 3.6. Let A be a graded ring as in (†). If $x_1, ..., x_k \in A_1$ generate A_1 as A_0-module then the map of graded A_0-algebras $A_0[T_1, ..., T_k] \to A : T_i \mapsto x_i$ is surjective. In particular, A_n is a finitely generated A_0-module, generated by the monomials in $x_1, ..., x_k$ of total degree n.

Example. Let R be a Noetherian ring, $I \subset R$ an ideal such that R/I is Artinian. Then $\mathrm{gr}_I(R) = \oplus_{n\geq 0} I^n/I^{n+1}$ satisfies (†)

Notation. Let $M = \oplus_{n\geq 0} M_n$ be a graded $A = \oplus_{k\geq 0} A_k$-module. Then $M(i)$ is a graded A-module with $(M(i))_n = M(i+n)$.

Example. A graded A-module M is finitely generated A-module if and only there exists $\oplus_{i=1}^k A(n_i) \twoheadrightarrow M$ a surjective map of graded A-modules.

Proof. "$\Leftarrow$": $A(m_i)$ is generated by $1 \in (A(n_i))_{-n_i}$

"$\Rightarrow$": M is finitely generated say by $x_1, \dots, x_n$. Then M is generated by the finitely many homogeneous components of $x_1, \dots, x_n$. Hence, without loss of generality, we can assume x_i is homogeneous of degree d_i. Then $\oplus_{i=1}^n A(-d_i) \to M$ defined by $A(-d_i)_{d_i} \ni 1 \mapsto x_i$ is a surjective map of graded A-modules. $\square$

Remark. If A satisfies (†) and $M = \oplus_{n\geq 0} M_n$ is a finitely generated A-module, then M_n is an A_0-module of finite length l because there is a surjection $\oplus_{i=1}^l A(n_i) \twoheadrightarrow M$ of graded A-modules, and each $A(n_i)_j = A(n_i + j)$ is a finitely generated A_0-module, hence of finite length as A_0 is Artinian.

Definition 3.7. Let $A = \oplus_{n\geq 0} A_n$ be a graded ring satisfying (†) and $M = \oplus_{n\geq 0} M_n$ a finitely generated graded A-module. The *Poincare series* of M is the formal power series

$$P(M,t) = \sum_{n\geq 0} l(M_n) t^n \in \mathbb{Z}[[t]]$$

Theorem 3.8. *Let M be a finitely generated graded A-module where A satisfies (†). If $x_1, \dots, x_s$ generate A_1 as A_0-module then there exists $f(t) \in \mathbb{Z}[t]$ polynomial such that $P(M,t) = f(t)/(1-t)^s$.*

Proof. We prove this by induction on s (the number of generators of A_1 as A_0-module)

$s = 0$: This means $A = A_0$. Now M is a finitely generated A-module, means there exists a surjective of graded A-modules: $\oplus_{i=1}^l A(d_i) \twoheadrightarrow M$. Hence $M_n = 0$ for $n \gg 0$ ($n \geq \max_{1\leq i\leq l}\{-d_i\}$). Hence $P(M,t)$ is a polynomial and we can take $f(t) = P(M,t)$.

$s > 0$: Let N, Q be the kernel and cokernel of the map $M(-1) \xrightarrow{\cdot x_s} M$ of graded A-modules. So we have an exact sequence of graded A-modules: $0 \to N \to M(-1) \xrightarrow{\cdot x_s} M \to Q \to 0$. But $x_s N = 0$ and $x_s Q = 0$, so N, Q are A/x_s-modules. N (and Q) are finitely generated A (hence A/x_s) modules because A is a Noetherian ring. Length is additive with respect to short exact sequence, hence $P(N,t) - P(M(-1),t) + P(M,t) - P(Q,t) = 0$. So

$$\begin{aligned}
P(M,t) - P(M(-1),t) &= P(Q,t) - P(N,t) \\
P(M,t) - P(M(-1),t) &= \frac{f(t)}{(1-t)^{s-1}} && \text{by induction hypothesis} \\
P(M,t) - tP(M,t) &= \frac{f(t)}{(1-t)^{s-1}} && l(M(-1)_n)t^n = l(M(n-1))t^n
\end{aligned}$$

hence $P(M,t) = f(t)/(1-t)^s$. $\square$

Notation. Let M be a finitely generated graded A-module where A satisfies (†). Write $d(M)$ =order of pole of $P(M,t)$ at $t = 1$.

Theorem 3.9. *Let A satisfy (†), let $M = \oplus_{n\geq 0} M_n$ be a finitely generated graded A-module. Then there exists a polynomial $g(t) \in \mathbb{Q}[t]$ of degree $d(M) - 1$ such that there exists n_0 with $g(n) = l(M_n)$ for all $n \geq n_0$.*

Proof. By Theorem 3.8, we have $P(M,t) = f(t)/(1-t)^s$, $f(t) \in \mathbb{Z}[t]$. Cancelling common factors of $f(t)$ and $(1-t)^s$, we can assume that $P(M,t) = f(t)/(1-t)^d$ for a polynomial $f(t) = \sum_{i=0}^n a_i t^i \in \mathbb{Z}[t]$ with $f(1) \neq 0$. Then d is the order of the pole of $P(M,t)$ at $t = 1$. Now

$$\begin{aligned}
\binom{-d}{j}(-1)^j &= \frac{(-d)(-d-1)\dots(-d-j+1)}{j!}(-1)^j \\
&= \frac{(j+d-1)(j+d-2)\dots d}{j!} \\
&= \binom{j+d-1}{j} \\
&= \binom{j+d-1}{d-1}
\end{aligned}$$

Hence

$$\begin{aligned}(1-t)^{-d} &= \sum_{j=0}^{\infty}\binom{-d}{j}(-t)^j \\ &= \sum_{j=0}^{\infty}\binom{j+d-1}{d-1}t^j\end{aligned}$$

So

$$\begin{aligned}P(M,t) &= \sum_{j\geq 0, 0\leq i\leq n}\binom{j+d-1}{d-1}a_i t^{i+j} \\ &= \sum_{n\geq 0} l(M_n)t^n\end{aligned}$$

Hence we have $l(M_k) = \sum_{i=0}^{n} a_i\binom{k-i-d-1}{d-1}$ for $k \geq n$. This is a polynomial in k with leading term $\sum_{i=0}^{n} a_i \frac{k^{d-1}}{(d-1)!} = f(1)\frac{k^{d-1}}{(d-1)!} \neq 0$, since $f(1) \neq 0$. It clearly has degree $d-1$. □

Remark. If $g_1, g_2 \in \mathbb{Q}[t]$ such that $\exists n_0$ with $g_1(n) = g_2(n)\,\forall n \geq n_0$, then $g_1 = g_2 \in \mathbb{Q}[t]$. Hence there exists a unique $H(M) \in \mathbb{Q}[t]$ such that $\exists n_0$ with $H(M)(n) = l(M_n)$ for all $n \geq n_0$

Definition 3.10. The unique polynomial $H(M)$ with $H(M)(n) = l(M_n)$ for $n \gg 0$ is called the *Hilbert polynomial* of $M = \oplus_{n\geq 0}M_n$. If $I \subset R$ is an ideal such that R/I is artinian and M is a finitely generated R-module, we write $H_I(M)$ for the Hilbert polynomial of $\mathrm{gr}_I M = \bigoplus_{n\geq 0}\frac{I^nM}{I^{n+1}M}$ as a graded $\mathrm{gr}_I(R)$-module. If (R,m,k) is a local ring, we may write $H(R)$ for $H_m(R) = H(\mathrm{gr}_m R)$.

Remark 3.11. We've showed that $1 + \deg H(M) = d(M)$ (Theorem 3.9)

3.3 Characteristic Polynomial

Definition 3.12. Let (R,m,k) be a local Noetherian ring. An ideal $I \subset m$ is called *m-primary* if $m = \sqrt{I} = \{x \in R | x^n \in I \text{ for some } n\}$

Remark. $I \subset m$ is m-primary, if and only if, $m^n \subset I$ for some $n \in \mathbb{N}$, if and only if, R/I is Artinian.

Proposition 3.13. *Let (R,m,k) be a local Noetherian ring, $I \subset m$ a m-primary ideal, M a finitely generated R-module and $M = M_0 \supset M_1 \supset M_2 \supset \dots$ be a stable I-filtration. Then:*

1. *M/M_n has finite length for all $n \geq 0$*
2. *There exists $g \in \mathbb{Q}[t]$ of degree $d(\oplus_{n\geq 0}M_n/M_{n+1})$ such that $\exists n_0$ with $g(n) = l(M/M_n)\,\forall n \geq n_0$*
3. *The degree and leading coefficient of $g \in \mathbb{Q}[t]$ (from 2.) does not depend on the stable I-filtration. (Only on M and I)*

Proof. 1. $M_\bullet$ is a stable I-filtration implies $\mathrm{gr}(M_\bullet) = \oplus_{n\geq 0}M_n/M_{n+1}$ is a finitely generated $\mathrm{gr}_I(R) = \oplus_{n\geq 0}I^n/I^{n+1}$-module (Using Lemma 2.20). Hence M_n/M_{n+1} is a finitely generated R/I-module. By the above remark, I is m-primary, means R/I is Artinian, hence M_n/M_{n+1} has finite length. From the exact sequence

$$0 \longrightarrow M_n/M_{n+1} \longrightarrow M/M_{n+1} \longrightarrow M/M_n \longrightarrow 0 \qquad (*)$$

and induction on n (since $M/M_0 = 0$ has finite length), we conclude that M/M_n has finite length for all $n \geq 0$.

2. Set $g(n) = l(M/M_n)$. From $(*)$ we see that $g(n+1) - g(n) = H(\mathrm{gr}M)(n)\,\forall n \geq n_0$ (where n_0 depends on $H(M)$). Hence there exists some $c \in \mathbb{Q}$ such that $g(n) = c + \sum_{i=1}^{n-1} H(\mathrm{gr}M)(i)\ \forall n \geq n_0$. This is a polynomial of degree $1 + \deg(H(\mathrm{gr}M)) = d(\mathrm{gr}M)$ because[1] $h_d(n) = \sum_{k=1}^{n-1} k^d$ is a polynomial in n of degree $d+1$.

[1] To see this we use induction on d . For $d = 0$, then $h_d(n) = \sum_{k=1}^{n-1} 1 = n-1$, a polynomial of degree $d+1$.
Assume $d \geq 1$. Then $(k+1)^{d+1} = \sum_{i=0}^{d+1}\binom{d+1}{i}k^i$, so $\sum_{k=2}^{n} k^{d+1} = \sum_{k=1}^{n-1}(k+1)^{d+1} = \sum_{i=0}^{d+1}\binom{d+1}{i}\sum_{k=1}^{n-1}k^i = \sum_{k=1}^{n-1}k^{d+1} + \sum_{i=0}^{d}\binom{d+1}{i}h_i(n)$. Hence $n^{d+1} - 1 = \sum_{i=0}^{d}\binom{d+1}{i}h_i(n)$, so $h_d(n) = \frac{1}{d}(n^{d+1} - 1 - \sum_{i=0}^{d-1}\binom{d+1}{i}h_i(n))$. Hence by induction hypothesis, this is a polynomial of degree $d+1$.

3. Let g be as in 2. and let $\overline{g}$ be the polynomial obtained in 2. for the stable I-filtration $\{I^n M\}$. $\{M_\bullet\}$ is a stable I-filtration, hence there exists k such that $\forall n \geq k$ $I^n M \subset M_n = I^{n-k} M_k \subset I^{n-k} M$ (by Definition 2.14) So there exist surjections

$$M/I^n M \twoheadrightarrow M/M_n \twoheadrightarrow M/I^{n-k} M$$

So $l(M/I^n M) \geq l(M/M_n) \geq l(M/I^{n-k}M)$. So $\overline{g}(n) \geq g(n) \geq \overline{g}(n-k)$ for $n \gg 0$.

Note that $g = 0$, if and only if, $\overline{g} = 0$ in view of the above surjections. Therefore, $g, \overline{g}$ have the same degree and leading coefficients in this case.

So we assume $g \neq 0$. Then $\lim_{n\to\infty} \overline{g}(n)/g(n) \geq 1 \geq \lim_{n\to\infty} \overline{g}(n-k)/g(n) = \lim_{n\to\infty} \overline{g}(n)/g(n)$, hence $\lim_{n\to\infty} \overline{g}(n)/g(n) = 1$, hence g and $\overline{g}$ have the same degree and leading coefficients.

Definition 3.14. Let (R, m, k) be a Noetherian local ring, M a finitely generated R-module with stable I-filtration where $I \subset m$ is a m-primary ideal. Then the polynomial g of Proposition 3.13 part 2. is called the *characteristic polynomial* of $\{M_\bullet\}$. For $\{I^n M\}$ we write $\chi_I(M)$ for its characteristic polynomial.

□

Remark. We proved that $\deg \chi_I(M) = 1 + \deg H_I(M)$; see proof of Proposition 3.13 part 2.

Lemma 3.15. *Let (R, m, k) be a Noetherian local ring, $I \subset R$ a m-primary ideal. Then for any finitely generated R-module M we have $\deg \chi_I(M) = \deg \chi_m(M)$.*

Proof. I is m-primary, so $m^n \subset I \subset m$ by definition. Hence $m^{nk} \subset I^k \subset m^k$ and $m^{nk}M \subset I^k M \subset m^k M$. Hence there exist surjections

$$M/m^{nk}M \twoheadrightarrow M/I^k M \twoheadrightarrow M/m^k M$$

so $l(M/m^{nk}M) \geq l(M/I^k M) \geq l(M/m^k M)$, which means that

$$\chi_m(M, nk) \geq \chi_I(M, k) \geq \chi_m(M, k) \, \forall k \gg 0 \quad (*)$$

Since $\chi_m(M, k), \chi_I(M, k) \geq 0$ for $k \gg 0$, we have the leading coefficients of $\chi_m, \chi_I \geq 0$. So by $(*)$ we have $\deg \chi_m \geq \deg \chi_I \geq \deg \chi_m$ □

3.4 Dimension Theorem

Notation. Let (R, m, k) be a Noetherian local ring. Write

$$\delta(R) = \min\{n \in \mathbb{N} | \exists x_1, \ldots x_n \in m : R/(x_1, \ldots, x_n) \text{ is Artinian}\}$$

Convention for this course: The degree of the zero polynomial is -1.

Dimension Theorem. *Let (R, m, k) be a Noetherian local ring. Then the following three numbers are equal:*

$$\dim R = 1 + \deg H(gr_m R) = \delta(R)$$

Proof. The strategy of the proof is to show:

$\delta(R) \overset{(3)}{\leq} \dim R \overset{(2)}{\leq} 1 + \deg H(\mathrm{gr}_m R) \overset{(1)}{\leq} \delta(R)$

1.

Lemma 3.16. *Let (R, m, k) be a Noetherian local ring. Then $1 + \deg(H(gr_m R)) \leq \delta(R)$*

Proof. Recall (Theorem 3.13) that we have already shown that for an m-primary ideal $I \subset R$: $\deg \chi_I R = 1 + \deg H(\mathrm{gr}_I R) =$ order of pole at $t = 1$ of $P(\mathrm{gr}_I R, t)$. We also have proven (Theorem 3.8) that $P(\mathrm{gr}_I R, t) = f(t)/(1-t)^s$ where s is the number of generators of $\mathrm{gr}_I(R) = I/I^2$ as R/I-module. Nakayama's lemma shows: I is generated by s-elements as R-module. Note that order of pole at $t = 1$ is $\leq s$ (Since $f(t)$ is a polynomial). Hence $\deg \chi_I(R) \leq s = \#$generator of I. Recall (Theorem 3.13) that $\deg \chi_I(R) = \deg \chi_m(R)$, so $1 + \deg H(\mathrm{gr}_m R) = \deg \chi_m(R) = \deg \chi_I(R) \leq \#$generator of I for all m-primary ideals $I \subset R$. Hence $1 + \deg H(\mathrm{gr}_m R) \leq \delta(R)$. □

2.

Lemma 3.17. *Let (R, m, k) be a Noetherian local ring. Let $x \in m$ be a non-zero-divisor. Then $\deg H_m(R/x) \leq \deg H_m(R) - 1$.*

Proof. Since $\deg H_m = \deg \chi_m - 1$, we will show that $\deg \chi_m(R/x) \leq \deg \chi(R) - 1$. Since $x \in m$ is a non-zero-divisor, we have an exact sequence

$$0 \longrightarrow M \hookrightarrow R \longrightarrow R/x \longrightarrow 0$$

where $M = xR \cong R$ (with the isomorphism$R \to xR$ is given by $r \mapsto xr$). Set $S = R/x$. So we have exact sequences

$$0 \longrightarrow M/M \cap m^n R \longrightarrow R/m^n R \longrightarrow S/m^n S \longrightarrow 0$$

This means

$$\chi_m(R) - \chi(M_\bullet) = \chi_m(S) \ (*)$$

where $M_\bullet$ is the m-filtration $\{M \cap m^n R\}$, which is stable by the Artin-Rees lemma. By Proposition 3.13 part 3, the degree and leading coefficients of $\chi(M_\bullet)$ equals to the ones for $\chi_m(M) = \chi_m(R)$ (since $M = xR \cong R$). So using $(*)$ we have $\deg \chi_m(S) \leq \deg \chi_m(R) - 1$. □

Lemma 3.18. *Let (R, m, k) be a Noetherian local ring. Then* $\dim R \leq 1 + \deg H(R)$

Proof. We do a proof by induction on $\deg H(R) \geq -1$

Consider $\deg H(R) = -1$, this happens if and only if $H(R) = 0$. So $m^n/m(m^n) = m^n/m^{n+1} = 0$ for $n \gg 0$. By Nakayama's lemma this implies $m^n = 0$ for $n \gg 0$. Hence R is Artinian, so $\dim R = 0$. (In fact if $\dim R = 0$, then by definition R is Artinian, so $m^n = 0$ for $n \gg 0$, which trivially shows that $m^n/m^{n+1} = 0$ for $n \gg 0$. So in fact we have $H(R) = 0$ if and only if $\dim R = 0$). Hence $\dim R \leq 1 + \deg H(R)$.

Assume $\deg H(R) \geq 0$, then $\dim R \geq 1$, so there exists prime ideals $q \subsetneq p \subsetneq R$, and

$$\dim R = \max_{q \subsetneq p}\{\dim R/p\} + 1.$$

For $q \subsetneq p \subseteq R$ prime ideals, there exists $x \in p \setminus q$. Then we have surjective maps, $R/q \twoheadrightarrow R/(q, x) \twoheadrightarrow R/p$. Now R/q is a domain (since q is prime), and since $0 \neq x \in R/q$ we have x is a non-zero divisor in R/q (also $x \in p \subset m$). Hence by Lemma 3.17 and the fact $R \twoheadrightarrow R/q$, means $\mathrm{gr}_m R \twoheadrightarrow \mathrm{gr}_m R/q$ hence $H(R,t) \geq H(R/q, t) \geq 0$, $t \gg 0$, we get

$$\deg H(R/(q, x)) \leq \deg H(R/q) - 1 \leq \deg H(R) - 1$$

So by induction hypothesis (and the fact $R/(q, x) \twoheadrightarrow R/p$),

$$\dim R/p \leq \dim R/(q, x) \leq 1 + \deg H(R/(q, x)) \leq \deg H(R)$$

Hence

$$\dim R = 1 + \max_{q \subsetneq p}\{\dim R/p\} \leq 1 + \deg H(R)$$

□

Corollary 3.19. *Let (R, m, k) be a local Noetherian ring. Then* $\dim R < \infty$

Proof. $\dim R \leq 1 + \deg H(R) < \infty$ □

Remark. There are Noetherian rings of infinite dimension (Assignment III)

Corollary 3.20. *Let (R, m, k) be a Noetherian local ring. Then prime ideals in R satisfy the descending chain condition.*

Proof. If $p_0 \supsetneq p_1 \supsetneq \cdots \supsetneq p_n$ is a chain of prime ideals, then $n \leq \dim R < \infty$. □

Remark. Any (Noetherian) ring has minimal primes (either by Corollary 3.20 or by Zorn's lemma)

3.

Lemma 3.21. *Let R be a Noetherian ring. Then the set of minimal primes in R is finite.*

Proof.

Claim. Let M be a finitely generated R-module. Then there exists a filtration $0 = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_n = M$ such that $M_i/M_{i-1} \cong R/p_i$ for some prime ideals $p_i \subset R$.

Proof. Let N be any finitely generated R-module. For $x \in N$, set $\mathrm{Ann}(x) = \{a \in R | ax = 0\} = \ker(R \xrightarrow{\cdot x} N : a \mapsto ax\} \subset R$ is an ideal. Since R is Noetherian, we have that the set of ideals $\{\mathrm{Ann}(x) | x \in N, x \neq 0\}$ has a maximal element, say $\mathrm{Ann}(x) \subsetneq R$ (proper ideal since $x \neq 0$).

We claim that $\mathrm{Ann}(x)$ is a prime ideal. To see this let $ab \in \mathrm{Ann}(x), a \notin \mathrm{Ann}(x)$. Then $ax \neq 0$ and $b \in \mathrm{Ann}(ax) \supset \mathrm{Ann}(x)$ and since $\mathrm{Ann}(x)$ is maximal, $\mathrm{Ann}(x) = \mathrm{Ann}(ax) \ni b$. Hence $\mathrm{Ann}(x)$ is prime. Then $R/\mathrm{Ann}(x) \xrightarrow{\cdot x} N$ is injective, $\mathrm{Ann}(x)$ is prime. Hence $(*)$ for any finitely generated R-module N there exists a prime ideal $p \subset R$ with $R/p \subset N$.

Among all submodules P of M which have filtration $0 = P_0 \subset P_1 \subset \cdots \subset P_n = P$ with $P_i/P_{i-1} \cong R/p$, choose a maximal $P \subset M$ (Note that P exists because M is Noetherian and the set of such P is non empty by $(*)$.) If $P \neq M$ then apply $(*)$ to $N = M/P$ to find an injection $R/q \subset N := M/P$ with $q \subset R$ a prime ideal. If $g : M \to M/P$ is the quotient map then $P \subsetneq g^{-1}(N)$ and $0 = P_0 \subset P_1 \subset \cdots \subset P_n \subsetneq g^{-1}(N)$ has successive quotients isomorphic to R/q_i with $q_i \subset R$ prime ideals. This is a contradiction to the maximality of P. Hence $P = M$ and we have proven the claim. □

Claim. Let $R = M$ and $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ is a filtration with $M_i/M_{i-1} \cong R/p_i$ with $p_i \subset R$ are prime ideals. If $q \subset R$ is a minimal prime, then there exists $i \in \{1, \dots n\}$ such that $q = p_i$

Proof. $0 \neq R_q = M_q$ means there exists i with $(M_i/M_{i-1})_q \neq 0$, hence $(R/p_i)_q \neq 0$. If $(R \setminus q) \cap p_i \neq \emptyset$ then $(R/p_i)_q = 0$. Hence $(R/p_i)_q \neq 0$ means $(R \setminus q) \cap p_i = \emptyset$, so $p_i \subset q$. Since q is a minimal prime, we have $p_i = q$. □

This second claim proves the lemma. □

Prime Avoidance Lemma. *Let $I \subset R$ be an ideal, $P_1, \dots, P_n \subset R$ prime ideals. If $I \subset \cup_{i=1}^n P_i$ then there exists $i \in \{1, \dots, n\}$ such that $I \subseteq P_i$.*

Proof. See Commutative Algebra. □

Definition 3.22. Let $P \subseteq R$ be a prime ideal, with R a Noetherian ring. The *height* of P is $\mathrm{ht}(P) = \dim R_P$. Let $I \subsetneq R$ be an ideal. The height of I is $\mathrm{ht}(I) = \min_{R \supset P \supset I} \mathrm{ht}(P)$ (with P prime ideal)

Lemma 3.23. *Let (R, m, k) be a local Noetherian ring. Then $\delta(R) \leq \dim R$*

Proof. Let $\dim R = 0$, then R is Artinian and local so $m^n = 0$ for some n. Hence 0 is m-primary, and $\emptyset$ generates the m-primary ideal 0. Hence $\delta(R) = 0$

Assume now $\dim R \geq 1$, we will show:

$(*)$ For every $i = 0, \dots, d = \dim R$ there are $x_1, \dots, x_i \in m$ such that $\mathrm{ht}(x_1, \dots, x_i) \geq i$.

We will prove $(*)$ by induction on i. For $i = 0$, $\mathrm{ht}(0) = 0$.

Assume $x_1, \dots, x_i$ constructed as in $(*)$ with $i < \dim R$. Let Σ be the set of primes $p \subset R$ containing $(x_1, \dots, x_i)$ which are minimal primes of $R/(x_1, ..., x_i)$ and have $\mathrm{ht}_R(p) = i$. Now R is Noetherian, hence Σ is finite (as a subset of the finite set of minimal primes of $R/(x_1, \dots, x_i)$). If $\cup_{p \in \Sigma} p = m \Rightarrow \exists_{p \in \Sigma} m \subset p$ (by the avoidance lemma). But this implies $m = p$, since m is maximal, which leads to the contraction that $\mathrm{ht}(m) = \dim R > i = \mathrm{ht}(p)$. Hence there exists $x_{i+1} \in m \setminus \cup_{p \in \Sigma} p$.

If $q \subset R$ is a prime ideal such that $q \supset (x_1, \dots, x_{i+1})$ then $\mathrm{ht}(q) \geq i$ (since $\mathrm{ht}(x_1, \dots, x_i) \geq i$), but $\mathrm{ht}(q) \neq i$, otherwise $q \in \Sigma$ but $x_{i+1} \in q \setminus \cup p, p \in \Sigma$. Hence $\mathrm{ht}(q) \geq i + 1$ implying $\mathrm{ht}(x_1, \dots, x_{i+1}) \geq i + 1$, thus proving $(*)$

So there exists $x_1, \dots, x_d \in m$ such that $\mathrm{ht}(x_1, \dots, x_d) \geq d$ where $d = \dim R$. Hence m is the only prime ideal containing $x_1, \dots, x_d$ because m is the only prime ideal p with $\mathrm{ht}(p) = d$. Hence $R/(x_1, \dots, x_d)$ has exactly one prime ideal, namely m. Hence $\dim R/(x_1,\dots,x_d)=0$, that is $R/(x_1,\dots,x_d)$ is Artinian, so $(x_1,\dots,x_d)$ is m-primary and $\delta(R)\le d=\dim R$. ☐

This finishes the proof of the Dimension Theorem. ☐

Corollary 3.24. *Let (R,m,k) be a Noetherian local ring, let $\widehat{R}$ be its m-adic completion. Then* $\dim R=\dim\widehat{R}$

Proof. We have $\mathrm{gr}_m R=\mathrm{gr}_{m\widehat{R}}\widehat{R}$. Then $H(\mathrm{gr}_m R)=H(\mathrm{gr}_{m\widehat{R}}\widehat{R})$, so by the Dimension Theorem $\dim R=\dim\widehat{R}$ ☐

Corollary 3.25. *Let (R,m,k) be a local Noetherian ring, and $x\in m$ be a non-zero divisor. Then* $\dim R/x=\dim R-1$.

Proof. By Lemma 3.17, we have $\deg H(R/x)\le\deg H(R)-1$ (and hence by the Dimension Theorem $\dim R/x\le\dim R-1$)

Let $n=\dim R/x$, then there exists $y_1,\dots,y_n\in m$ such that $R/(x,y_1,\dots,y_n)$ is Artinian (by the Dimension Theorem for R/x). So $x,y_1,\dots,y_n$ generates a m-primary ideal in R. Hence we have $\dim R=\delta(R)\le n+1=\dim R/x+1$ ☐

Krull's Principal Ideal Theorem. *Let R be a Noetherian ring. Let $x_1,\dots,x_n\in R$ such that $(x_1,\dots,x_n)\ne R$. Then* $\mathrm{ht}(x_1,\dots,x_n)\le n$.

Proof. Let $p\subset R$ be a prime ideal minimal over $(x_1,\dots,x_n)$. Then $x_1,\dots,x_n$ generates a p-primary ideal in R_p because $\dim R_p/(x_1,\dots,x_n)=0$ as p is minimal over $x_1,\dots,x_n$. Hence $\mathrm{ht}(x_1,\dots,x_n)\le\dim R_p=\delta(R_p)\le n$. ☐

3.5 Faithfully Flat and Going Down.

Recall: A map of rings $A\to B$ is called flat if the functor (A-modules $\to$ B-modules defined by $M\mapsto B\otimes_A M$) preserves exact sequences.

Definition 3.26. A map of rings $A\to B$ is called *faithfully flat* if $A\to B$ is flat and for all $M\in A$-modules, $B\otimes_A M=0$ if and only if $M=0$.

Remark. If $f:A\to B$ is faithfully flat then f is injective because $B\otimes_A\ker(f)=0$, and hence $\ker(f)=0$.

Example. Of flatness

1. $S\subset A$ is a multiplicatively closed subset then $A\to S^{-1}A$ is flat (but rarely faithfully flat)
2. If $f:A\to B$ is flat, and $A\to C$ any ring homomorphism then the map $C\to C\otimes_A B$ defined by $c\mapsto c\otimes 1$ is also flat

$$\begin{tikzcd} A \arrow[r, "\text{flat}", "f"'] \arrow[d] & B \arrow[d] \\ C \arrow[r, "\text{flat}"] & C\otimes_A B \end{tikzcd}$$

   To see this: The functor C-modules $\to$ $C\otimes_A B$-modules defined by $M_C\mapsto M_C\otimes_C(C\otimes_A B)\cong M_A\otimes_A B$ is exact where M_C and M_A denote M considered as a C, respectively A-module.
3. $A\to A[T]$ is faithfully flat because for $M\in A$-modules, we have $M\otimes_A A[T]\cong\oplus_{i\in\mathbb{N}}M$, and direct sums preserves exact sequences.

Definition 3.27. A *local map* of (local) rings $f:(A,m,K)\to(B,n,L)$ is a ring homomorphism $f:A\to B$ such that $f(m)\subset n$.

Example. If $f:A\to B$ is any ring homomorphism, $q\subseteq B$ is prime and set $p=f^{-1}(q)$. Then $A_p\to B_q$ is a local map of rings.

Lemma 3.28. *Let $f:(A,m,K)\to(B,n,L)$ be a local map of rings. If $f:A\to B$ is flat, then f is faithfully flat.*

Proof. Let M be an A-module such that $B \otimes_A M = 0$

First assume M is finitely generated. Consider the commutative diagram of rings

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d] & B \arrow[d] \\ K = A/m \arrow[r, "f"] & L = B/n \end{tikzcd}$$

Since $f : K \to L$ is a map of fields, f is injective and L is a non-zero vector space over K, we have $K \to L$ is faithfully flat. $0 = L \otimes_B (B \otimes_A M) = L \otimes_A M = L \otimes_K (K \otimes_A M)$, so $M/mM = A/m \otimes_A M = K \otimes_A M = 0$ (since $K \to L$ is faithfully flat). Hence by Nakayama's Lemma (using the fact M is finitely generated) we have $M = 0$.

For general M, let $x \in M$, then $Rx \hookrightarrow M$ is a submodule. $A \hookrightarrow B$ is flat, hence $B \otimes_A Rx \hookrightarrow B \otimes_A M = 0$ is injective, i.e., $B \otimes_A Rx = 0$. Since Rx is finitely generated $Rx = 0$, so $0 = x \in M\, \forall x \in M$. Hence $M = 0$ ☐

Remark. If $f : A \to B$ is flat, $q \subset B$ is prime and define $p = f^{-1}(q) \subset A$. Then $A_p \to B_q$ is also flat, hence faithfully flat.

Definition 3.29. Let $f : A \to B$ be a ring homomorphism. Then $f : A \to B$ has the *going down property* if for all $q_1 \subset B$ prime ideals, $p_1 = f^{-1}(q_1) \subset A$ and $p_0 \subset p_1$ prime in A, there exists $q_0 \subset B$ primes, such that $q_0 \subset q_1$ and $p_0 = f^{-1}(q_0)$

Notation. If R is a ring, define $\operatorname{Spec} R = \{p \subset R | p \text{ prime ideal}\}$

Proposition 3.30. *Let $f : A \to B$ be a flat map of rings.*

1. *If f is faithfully flat, then* $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ *defined by $q \mapsto f^{-1}(q)$ is surjective.*
2. *$f : A \to B$ has the going down property*

Proof. 1. Let $p \subset A$ be a prime ideal. The primes in B contracting to p are (in bijection with) the primes in $B \otimes_A k(p)$ where $k(p) = \operatorname{Frac}(A/p) = A_p/pA_p$ (See Commutative Algebra or the argument below)

Consider

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "g"] & B \arrow[d, "\overline{g}"] \\ k(p) \arrow[r, "\overline{f}"] & B \otimes_A k(p) \end{tikzcd}$$

Since f is faithfully flat and $k(p) \neq 0$, we have $B \otimes_A k(p)$ is a non-zero ring. Take a prime $q \subsetneq B \otimes_A k(p)$ then $\overline{g}^{-1}(q) \subset B$ is a prime ideal. So $f^{-1}(\overline{g}^{-1}(q)) = g^{-1}(\underbrace{\overline{f}^{-1}(q)}_{=0}) = p$, hence $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is surjective.

2. Let $q_1 \subset B$ be a prime ideal, and $p_0 \subset p_1 = f^{-1}(q_1) \subset A$ be prime ideals. Now $A_{p_1} \to B_{q_1}$ is a flat local map of rings, hence $A_{p_1} \to B_{q_1}$is faithfully flat. By part 1. $\operatorname{Spec}(B_{q_1}) = \{q \subset B | q \subset q_1\} \to \operatorname{Spec}(A_{p_1}) = \{p \subset A | p \subset p_1\}$ is surjective. Now $p_0 \in \operatorname{Spec}(A_{p_1})$, so there exists $q_0 \subset q_1$ such that $f^{-1}(q_0) = p_0$.

☐

Definition 3.31. Let (R, m, k) be a local Noetherian ring of dimension $d = \dim R$. A *system of parameters* for R is a set $x_1, \dots, x_d \in m$ such that $R/(x_1, \dots, x_d)$ is Artinian.

Remark. System of parameters exists by the Dimension Theorem.

Theorem 3.32. *Let $f : (A, m, K) \to (B, n, L)$ be a local map of local Noetherian rings. Then*

1. $\dim A + \dim(B/mB) \geq \dim B$
2. *Furthermore if f has going down property (for instance f is flat) then we actually have equality.*

Proof. 1. Let $x_1, \dots, x_r \in m$ be a system of parameters for A (so $r = \dim A$), and let $\overline{y}_1, \dots, \overline{y}_s \in n/mB$ be a system of parameters for B/mB. Let $y_1, \dots, y_s \in n$ be such that $y_i = \overline{y_i} \in B/mB$.

Claim. $x_1, \dots, x_r, y_1, \dots, y_s \in n$ generates an n-primary ideal.

By definition of system of parameters there exists $c \in \mathbb{N}$ such that $m^c \subset (x_1, \dots, x_r)$ and $n^d \subset (y_1, \dots, y_s) + mB$ for some $d \in \mathbb{N}$. Hence $n^{cd} \subset (y_1, \dots y_s) + m^c B \subset (y_1, \dots, y_s, x_1, \dots, x_r)$.

Then the claim proves $\dim B \leq r + s = \dim A + \dim B/mB$, by the Dimension Theorem.

2. A and B/mB are local Noetherian rings, let $r = \dim A$ and $s = \dim B/mB$. There exists chains of prime ideals $p_0 \subsetneq \cdots \subsetneq p_r \subset A$, $q_0 \subsetneq \cdots \subsetneq q_s \subset B$ such that $mB \subset q_0$ and $q_0/mB \subsetneq \cdots \subsetneq q_s/mB \subset B/mB$ is a chain of prime ideals. Now A is local Noetherian of dimension r, so $p_r = m = f^{-1}(q_0)$ because $m = f^{-1}(mB) \subset \underbrace{f^{-1}(q_0)}_{\text{prime ideal}} \subset m$. By going down for $f : A \to B$ there is a chain of prime ideals $q_0 \supsetneq \overline{p_{r-1}} \supsetneq \overline{p_{r-2}} \supsetneq \cdots \supsetneq \overline{p_o}$ in B such that $f^{-1}(\overline{p_i}) = p_i$. Hence we have a chain of prime ideals of length $r + s$, namely $\overline{p_0} \subsetneq \cdots \subsetneq \overline{p_{r-1}} \subsetneq q_0 \subsetneq \cdots \subsetneq q_s \subset B$. Hence $\dim B \geq r + s = \dim A + \dim B/mB$

□

Remark.

$$\begin{tikzcd}
\operatorname{Spec} B/mB \arrow[d] & \subset & \operatorname{Spec} B \arrow[d] \\
\{m\} & \subset & \operatorname{Spec} A
\end{tikzcd}$$

$\operatorname{Spec} B/mB$ is the fibre of the map $\operatorname{Spec} B \to \operatorname{Spec} A : q \mapsto f^{-1}(q)$ over $m \in \operatorname{Spec} A$. In this sense, Theorem 3.32 says that the dimension of base plus dimension of fibre is greater or equal the dimension of the total space.

Theorem 3.33. *Let A be a Noetherian ring. Then* $\dim A[T] = 1 + \dim A$.

Proof. "$\geq$" Let $p_0 \subsetneq \cdots \subsetneq p_n \subset A$ be a chain of prime ideals. Then $p_0[T] \subsetneq p_1[T] \subsetneq \cdots \subsetneq p_n[T] \subsetneq (T, p_n[T]) \subset A[T]$ is a chain of prime ideals in $A[T]$. (Since $p \subset A$ is prime then $p[T] \subset A[T]$ is prime since $A[T]/p[T] \cong (A/p)[T]$ and A/p is a domain. Similarly $(T, p[T]) \subset A[T]$ is prime because $A[T]/(T, p[T]) \cong A/p$). Hence we have found a chain of length $n + 1$. Hence $\dim A[T] \geq 1 + \dim A$

"$\leq$" The map $A \hookrightarrow A[T]$ is faithfully flat. Let $q \subset A[T]$ be a prime ideal and $p = A \cap q$. Then $A_p \to A[T]_q$ is a local flat (and hence faithful flat) map of Noetherian rings, hence $A_p \to A[T]_q$ has the going down property. By Theorem 3.32 we have $\dim A[T]_q = \dim A_p + \dim {}^{A[T]_q}/_{pA[T]_q}$ $(*)$.

Since $A \setminus p \subset A[T] \setminus q$ we have

$$\frac{A[T]_q}{pA[T]_q} = \left(\frac{A_p[T]}{pA_p[T]} \right)_q = (k(p)[T])_q$$

where $k(p) = (A/pA)_p$ =Fraction field of A/pA. Hence $k(p)[T]$ is a PID, so every non-zero prime ideal is maximal, so $1 = \dim k(p)[T] = \max_q k(p)[T]_q$. So $\dim k(p)[T]_q \leq 1$. So by $(*)$ $\dim A[T]_q \leq \dim A_p + 1$ for all prime ideals $q \subset A[T]$. Hence $\dim A[T] \leq 1 + \dim A$.

□

3.6 Dimension and Integral Extensions

Recall (from Commutative Algebra): Let $A \subset B$ be an extension of rings, and let $I \subset A$ be an ideal. Then $x \in B$ is called *integral over I* if $x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$ for some $a_1, \dots, a_n \in I$, $n \in \mathbb{N}$. The extension $A \subset B$ is called *integral* if every $x \in B$ is integral over A.

Lemma 3.34 (/**Definition**). *Let $A \subset B$ be an extension of rings. Then $x \in B$ is integral over A if and only if $A[x] \subset B$ (sub A-algebra of B generated by $x \in B$) is a finitely generated A-module. In particular, the set of elements in B that are integral over A is a sub A-algebra over A, called the* integral closure of A in B

Proof. See Commutative Algebra (Theorem 4.2) □

Definition 3.35. A domain A is called *normal* (or *integrally closed*) if A is integrally closed in its field of fractions.

Example. A is a UFD implies A is normal

Proposition 3.36. *Let $A \subset B$ be an integral extension of rings. Then:*

1. *The map* $\operatorname{Spec} B \to \operatorname{Spec} A$ *defined by* $p \mapsto p \cap A$ *is surjective.*

2. $q \subset B$ *is a maximal ideal if and only if* $A \cap q \subset A$ *is a maximal ideal*

3. *If* A *is Artinian and* B *Noetherian then* B *is Artinian*

4. *"Going up" holds (we won't need this so not stated)*

Proof. See Commutative Algebra:

1. Theorem 4.12 (part 1.)
2. Lemma 4.11
3. Uses part 1.
4. The "Going up" Theorem

$\square$

Goal: If $A \hookrightarrow B$ is an integral extension of domains with A normal. Then "going down" holds.

Lemma 3.37. *Let* $A \subset B$ *be an extension of rings. Let* C *be the integral closure of* A *in* B. *Let* $I \subset A$ *be an ideal. Then the closure of* I *in* B *(i.e., the set of* $b \in B$ *that are integral over* I*) is* $\sqrt{IC}$ *(the radical of* IC*). In particular, the integral closure of* I *in* B *is closed under taking sums and products.*

Proof. Let $J \subset B$ be the integral closure of I in B. We want to show that $J = \sqrt{IC}$.

"$\subset$" Let $x \in J$, then there exists $x^n + a_1x^{n-1} + \cdots + a_n = 0$ with $a_1, \ldots, a_n \in I$. Hence x is integral over A and $x \in C$. Since $x^n = -(a_1x^{n-1} + \cdots + a_n) \in IC$, we have $x \in \sqrt{IC}$.

"$\supset$" Let $x \in \sqrt{IC}$, then $x^n \in IC$ for some $n \in \mathbb{N}$. Hence $x^n = a_1y_1 + \cdots + a_ny_n$ with $a_i \in I$ and $y_i \in C$. Now $y_1, \ldots, y_n$ are integral over A, then by Lemma 3.34, $M = A[y_1, \ldots, y_n]$ is a finitely generated A-module. Now $x^nM \subset IM$. If M is generated by $b_1, \ldots, b_m$ as an A-module then x^nb_i is an I-linear combination of $b_1, \ldots, b_n$. So there exists a matrix $\Phi \in M_m(I)$ such that $x^nb = \Phi b$ (where $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$). Hence $(\mathrm{id}_m x^n - \Phi)b = 0$, so $\det(\mathrm{id}_m x^n - \Phi)b = 0$ (by multiplying with adjugate matrix of $(\mathrm{id}_m x^n - \Phi)$. Since $1 \in M = A[y_1, ..., y_n]$ is a linear combination of the b_i's, we have $\det(\mathrm{id}_m x^n - \Phi) = 0$, hence expanding the determinant, we get x is integral over I.

$\square$

Lemma 3.38. *Let* $A \subset B$ *be an extension of domains, assume* A *is normal. Let* $I \subset A$ *be an ideal. If* $x \in B$ *is integral over* I *then the minimal polynomial of* $x \in F(B)$ *=Fraction field of* B *over* $F(A)$ *has all coefficients in* $\sqrt{I}$.

Proof. Let $f(T) = T^n + a_1T^{n-1} + \cdots + a_n$ be the minimal polynomial of $x \in F(B)$ over $F(A)$. We need to show that $a_1, \ldots, a_n \in \sqrt{I}$. We know $x \in B$ is integral over I, so by definition there exists $g(T) = T^m + b_1T^{m-1} + \cdots + b_m$ with $b_i \in I$ and $g(x) = 0$. Since f is the minimal polynomial and $f(x) = g(x) = 0$, we have $f|g$. Let $L \supset F(B)$ be a field extension containing all roots $x_1, \ldots, x_n$ of f (and say $x = x_1$). Since $f|g$, we have $g(x_i) = 0$ for all x_i, so x_i is integral over I. Since $a_1, \ldots, a_n$ are sums of the products of $x_1, \ldots, x_n$, they are integral over I (Lemma 3.37). Now apply Lemma 3.37 to the extension $A \subset F(A)$. Then $C = A$ since A is normal, so $a_1, \ldots, a_n \in \sqrt{I}$. $\square$

The "going down" theorem for integral extensions. *Let* $A \subset B$ *be an integral extension of domains and assume* A *is normal. Then* $A \subset B$ *has the going down property, i.e.,* $\forall q_0 \subset B$ *prime,* $p_1 \subset p_0 = A \cap q_0$ *there exists* $q_1 \subset q_0 \subset B$ *prime such that* $p_1 = A \cap q_1$.

Proof. Consider the following commutative diagram of rings

$$\begin{tikzcd} & A_{p_0} \arrow[r, hook] \arrow[d, "\lambda"] & B_{q_0} \arrow[d, "\overline{\lambda}"] & \\ k(p_1) \arrow[r, equal] & \left(\frac{A_{p_0}}{p_1A_{p_0}}\right)_{p_1} \arrow[r, "j"] & \left(\frac{B_{q_0}}{p_1B_{q_0}}\right)_{p_1} \arrow[r, equal] & B_{q_0} \otimes_A k(p_1) \end{tikzcd}$$

If $B_{q_0} \otimes_A k(p_1) \neq 0$ then it has a prime ideal, and any of its prime ideals $\overline{q}_1$ corresponds to a prime ideal $q_1 = \overline{\lambda}^{-1}(\overline{q}_1) \subset Bq_0$, hence a prime ideal q_1 of B with $q_1 \subset q_0$. Now $q_1 \cap A_{p_0} = \lambda^{-1}(\underbrace{j^{-1}\overline{q_1}}_{=0\, k \text{ field}}) = p_1$, hence we have going down property.

So we need to show that $B_{q_0} \otimes_A k(p_1) \neq 0$. We show this using the following claim.

Claim. $p_1 = p_1 B_{q_0} \cap A$

This claim will prove $B_{q_0} \otimes_A k(p_1) \neq 0$, since the claim implies $p_1 A_{p_0} = p_1 B_{q_0} \cap A_{p_0}$, so considering the commutative diagram

$$\begin{tikzcd} A_{p_0} \arrow[r, hook] \arrow[d] & B_{q_0} \arrow[d] \\ \frac{A_{p_0}}{p_1 A_{p_0}} \arrow[r, hook, "\text{injective by claim}"'] & \frac{B_{q_0}}{p_1 B_{q_0}} \end{tikzcd}$$

localizing at $A \setminus p_1$ the map $k(p_1) = \left(\frac{A_{p_0}}{p_1 A_{p_0}}\right)_{p_1} \hookrightarrow \left(\frac{B_{q_0}}{p_1 B_{q_0}}\right)_{p_1} = B_{q_0} \otimes_A k(p_1)$ is still injective. Since $k(p_1) \neq 0$, we have $B_{q_0} \otimes_A k(p_1) \neq 0$

Proof of claim. We have $p_1 \subset p_1 B_{q_0} \cap A$. To prove the other inclusion, let $x \in p_1 B_{q_0} \cap A$, then $x = \frac{y}{s}$ with $y \in p_1 B$, $s \in B \setminus q_0$. Since B is integral over A, we have B is the integral closure of A in B, so by Lemma 3.37, the integral closure of p_1 in B is $\sqrt{p_1 B}$. Now $y \in p_1 B \subset \sqrt{p_1 B}$ means y is integral over p_1. Hence by Lemma 3.38, the minimal polynomial of $y \in F(B)$ =field of fraction of B over $F(A)$, $f(T) = T^n + a_1 T^{n-1} + \cdots + a_n$ has all coefficients $a_1, \ldots, a_n \in p_1$.

Now $s = \frac{y}{x} \in F(B)$, $0 = f(y) = y^n + a_1 y^{n-1} + \cdots + a_k = 0$ hence $0 = s^n x^n + a_1 s^{n-1} x^{n-1} + \cdots + a_n = 0$, hence $s^n + \frac{a_1}{x} s^{n-1} + \cdots + \frac{a_n}{x^n} = 0$. So $g(T) = T^n + \frac{a_1}{x} T^{n-1} + \cdots + \frac{a_n}{x^n}$ is the minimal polynomial of s over $F(A)$ because any factorisation of g yields a factorisation of f as $0 \neq x \in A \subset F(A)$. Since $s \in B$ integral over A, by Lemma 3.38, we have all coefficients $\frac{a_i}{x^i} \in A$. If $x \notin p_1$, since

$$\underbrace{\frac{a_i}{x^i}}_{\in A} \cdot \underbrace{x^i}_{\in A \setminus p_1} = a_i \in p_1,$$

we have $\frac{a_i}{x^i} \in p_1$ for all i. Hence s is integral over p_1, so (by Lemma 3.37) $s \in \sqrt{p_1 B} \subset \sqrt{q_0} = q_0$. This is a contradiction to $s \in B \setminus q_0$. Hence $x \in p_1$. ☐

☐

Theorem 3.39. *Let $A \subset B$ be an integral extension of Noetherian domains with A normal. Then $\forall n \subset B$ maximal ideal, $m = A \cap n$, we have $\dim B_n = \dim A_m$ and $\dim B = \dim A$.*

Proof. By assumption and the previous theorem, the map $A \to B$ has the "going down" property. Hence $A_m \to B_n$ has the going down property. So by the Theorem 3.32, we have $\dim A_m + \dim B_n / m B_n = \dim B_n$. Since $A \subset B$ is an integral extension, we have $p \subset B$ is maximal, if and only if, $A \cap p \subset A$ is a maximal ideal. Hence $B_n / m B_n$ has a unique maximal ideal $n B_n / m B_n$. Hence $\dim B_n / m B_n = 0$, so $\dim B_n = \dim A_m$.

Since for all $m \subset A$ maximal, there exists $n \subset B$ such that $m = A \cap n$, we have $\dim A = \sup_{m \subset A \max} \dim A_m = \sup_{n \subset B \max} \dim B_n = \dim B$. ☐

Definition 3.40. Let k be a field. An *affine k-algebra* is a k-algebra A which is isomorphic to $A \cong k[X_1, \ldots, X_n]/I$ as k-algebras. An *affine ring* is an affine k-algebra for some field k.

Noether Normalisation. *Let A be an affine k-algebra. Then there exists an integral extension $k[X_1, \ldots, X_n] \subset A$ where $k[X_1, \ldots, X_n]$ is the polynomial ring in n-variables with coefficients in k.*

Proof. We will only give a proof in the case k is infinite. We will use the following lemma:

Lemma 3.41. *Let k be an infinite field. Let $f \in k[X_1, \ldots, X_n]$, $f \neq 0$. Then there exists $c_1, \ldots, c_n \in k$ such that $f(c_1, \ldots, c_n) \neq 0$.*

Proof. Induction on n. For $n = 0$, we are done.

For $n = 1$, if $0 \neq f \in k[X]$ has degree d, then f has at most d roots. Since $\#k = \infty$, there exists $c \in k$ such that $f(c) \neq 0$.

Assume $n \geq 2$. Write $f \in k[X_1, \dots, X_n]$ as $f = g_d X_n^d + g_{d-1} X_n^{d-1} + \dots + g_0$ where $g_i \in k[X_1, \dots, X_{n-1}]$, with $g_d \neq 0$. By our induction hypothesis, there exists $c_1, \dots, c_{n-1}$ such that $g_d(c_1, \dots, c_{n-1}) \neq 0$. Then $0 \neq f(c_1, \dots, c_{n-1}, X_n) \in k[X_n]$. By the case $n = 1$, there exists $c_n \in k$ such that $f(c_1, \dots, c_n) \neq 0$. $\square$

To finish the proof of Noether Normalization, let A be an affine k-algebra. Then A is generated by $x_1, \dots, x_n \in A$ as a k-algebra. We will prove the theorem by induction on n. If $n = 0$, then $A = k$ so we are done.

Assume $n \geq 1$. By assumption the map $p : k[T_1, \dots, T_n] \twoheadrightarrow A$ defined by $T_i \mapsto x_i$ is surjective. If p is injective then p is an isomorphism and we are done. Assume p is not injective, let $0 \neq f \in \ker p \subset k[T_1, \dots, T_n]$. Let $d =$total degree of f. Write $f = f_d + f_{d-1} + \dots + f_0$ with f_i homogeneous of degree i. Now $0 \neq f_d \in k[T_1, \dots, T_n]$ and $\#k = \infty$ implies by the lemma that there exists $c_1, \dots, c_n \in k$ such that $f_d(c_1, \dots, c_n) \neq 0$. Since f_d is homogeneous $0 \neq f_d(c_1, \dots, c_n) = c_n^d f(\frac{c_1}{c_n}, \dots, \frac{c_{n-1}}{c_n}, 1)$, by replacing c_i with $\frac{c_i}{c_n}$ we can assume $c_n = 1$.

Set $y_i = x_i - c_i x_n$, hence $x_i = y_i + c_i x_n$ ($c_n = 1, y_n = 0$). Since $f \in \ker(p)$, we have $0 = f(x_1, \dots, x_n) = f(y_1 + c_1 x_n, \dots, y_n + c_n x_n) = f_d(c_1, \dots, c_n) x_n^d + g_{d-1} x_n^{d-1} + \dots + g_0 \quad (*)$, where $g_i \in k[y_1, \dots, y_{n-1}]$ (Since $y_n = 0$). By choice of $c_1, \dots, c_n$ we have $0 \neq f(c_1, \dots, c_n) \in k$. Hence by $(*)$ x_n is integral over $k[y_1, \dots, y_{n-1}]$ and $k[y_1, \dots, y_{n-1}] \subset k[y_1, \dots, y_{n-1}, x_n] = k[x_1, \dots, x_n] = A$ is an integral extension. By induction hypothesis there exists an integral extension $k[T_1, \dots, T_m] \subset k[y_1, \dots, y_{n-1}]$ with $k[T_1, \dots, T_m]$ polynomial ring. Hence $k[T_1, \dots, T_m] \subset A$ is integral. $\square$

Theorem 3.42. *Let k be a field and A an affine k-algebra which is a domain. Then for all maximal ideals $m \subset A$ we have* $\dim A = \dim A_m = \operatorname{Tr}\deg_k F(A)$ *where* $F(A)$ *=field of fraction of A.*

Proof. We split the proof in several cases:

Case 1. $A = k[T_1, \dots, T_n]$ and $m = (T_1, \dots, T_n)$. So $\dim A = n$, $\dim A_m = 1 + \underbrace{\deg H\mathrm{gr}_m A}_{n-1} = n$ and $\operatorname{Tr}\deg_k k(T_1, \dots, T_n) = n$.

Case 2. $k = \overline{k}$ is algebraically closed, $m \subset k[T_1, \dots, T_n]$ any maximal ideal. By the Nullstellensatz Theorem ($k = \overline{k}$), we have $m = (T_1 - a_1, \dots, T_n - a_n)$ for some $a_1, \dots, a_n \in k$. So $k[X_1, \dots, X_n] \to k[T_1, \dots, T_n]$ defined by $X_i \mapsto T_i - a_i$ is an isomorphism sending $(X_1, ..., X_n)$ to m. Then by 1, we have $\dim(A) = n$, $\dim A_m = \dim k[X_1, \dots, X_n]_{(X_1, \dots, X_n)} = n$ and $\operatorname{Tr}\deg_k k(T_1, \dots, T_n) = n$.

Case 3. Let $A = k[T_1, \dots, T_n]$ and $m \subset A$ any maximal ideal. Then $A = k[T_1, \dots, T_n] \to \overline{k}[T_1, \dots, T_n] = B$ is an integral extension of domains with A normal ($k[T_1, \dots, T_n]$ being a UFD implies A normal). Hence for all $m \subset A$ there exists a maximal ideal $p \subset B$ such that $m = p \cap A$ and $\dim A_m = \dim B_p$, by Theorem 3.39. So by 2. we have $\dim A_m = n, \dim A = n$ and $\operatorname{Tr}\deg_k k(T_1, \dots, T_n) = n$

Case 4. A is any affine k-algebra which is a domain. By Noether normalisation there exists an integral extension $B = k[T_1, \dots, T_n] \subset A$. Since $k[T_1, \dots, T_n]$ is normal domain, for all maximal ideals $m \subset A$, $p = B \cap m$ we have $\dim A_m = \dim B_p = n$ (by part 3. and Theorem 3.39). Hence $\dim A = \sup_{m \subset A \max} A_m = n$. Since $B \subset A$ is an integral extension, we have $F(B) \subset F(A)$ are algebraic extension of fields, so $n = \operatorname{Tr}\deg_k F(B) = \operatorname{Tr}\deg_k F(A)$.

$\square$

3.7 Groebner basis and an algorithmic computation of the Hilbert Polynomial

Let k be a field and $S = k[x_1, \dots, x_n]$ the polynomial ring in n variables with coefficients in k.

Definition 3.43. A polynomial $f \in S$ is called *monomial* if $f = x_1^{\alpha_1} \dots x_n^{\alpha_n}$ for some $\alpha_i \in \mathbb{N}$.

Notation. If $\alpha = (\alpha_1, \dots, \alpha_n)$ we may write x^α for $x_1^{\alpha_1} \dots x_n^{\alpha_n}$.

Definition 3.44. A *monomial ideal* in S, is an ideal $I \subset S$ that is generated by monomials.

Lemma 3.45. *Any monomial ideal in $S = k[x_1, \dots, x_n]$ is generated by a finite number of monomials.*

Proof. Let $I \subset S$ be a monomial ideal, let $\Sigma \subset I$ be the set of monomials in I. So $I = \langle \Sigma \rangle$ (i.e., it is generated by Σ). Assume I cannot be generated by a finite number of monomials. Construct $J_n = (x^{\alpha_1}, \dots, x^{\alpha_n}) \subset I$ such that $J_i \subsetneq J_{i+1}$ as follows:

- $J_0 = 0$.
- Assume J_n is constructed. Since $J_n \neq I$ (as I is not generated by a finite number of monomials). There exists $x^{\alpha_{n+1}} \in \Sigma$ such that $x^{\alpha_{n+1}} \notin J_n$. Then $J_n \subsetneq J_{n+1}(x^{\alpha_1}, \dots, x^{\alpha_n})$

So we can construct $J_0 \subsetneq J_1 \subsetneq \cdots \subsetneq I$ which contradicts the ACC as S is Noetherian. Hence I is generated by a finite number of monomials. □

Remark. If $I = (x^{\alpha_1}, \dots, x^{\alpha_n}) \subset S$ is an ideal generated by monomials x^{α_i}, then a monomial $x^\beta \in I$ if and only if, there exists $i = 1, \dots, n$ such that $x^{\alpha_i} | x^\beta$.

The monomials in I form a k-basis of I.

Definition 3.46. Let x^α, x^β be monomials. Then the *least common multiple* of x^α, x^β is $\operatorname{lcm}(x^\alpha, x^\beta) = x_1^{\max(\alpha_1,\beta_1)} \dots x_n^{\max(\alpha_n,\beta_n)}$

Lemma 3.47. *The intersection of two monomial ideals is a monomial ideal. More precisely, if $f_1, \dots, f_n$, $g_1, \dots, g_m$ are monomials then $(f_1, \dots, f_n) \cap (g_1, \dots, g_m) = (\operatorname{lcm}(f_i, g_j) | i = 1, \dots, n,\ j = 1, \dots m)$*

Proof. Let $I = (f_1, \dots, f_n)$ and $J = (g_1, \dots, g_m)$. Let Σ_I =monomials in I, this is a k-basis of I. Similarly let Σ_J =monomials in J, this is a k-basis of J. S has a k-basis of all monomials ideals. Hence $I \cap J$ has a k-basis $\Sigma_I \cap \Sigma_J$. Hence $I \cap J = (\Sigma_I \cap \Sigma_J)$ is a monomial ideal.

Let h be a monomial then:

- $h \in \Sigma_I$ if and only if there exists $f_i | h$
- $h \in \Sigma_J$ if and only if there exists $g_j | h$

Hence $h \in \Sigma_I \cap \Sigma_J$ if and only if there exists i and j such that $f_i | h$ and $g_j | h$, if and only if, there exists i, j with $\operatorname{lcm}(f_i, g_j) | h$. Hence $I \cap J = (\operatorname{lcm}(f_i, g_j))$. □

3.7.1 Algorithm for computing $H(S/I)$ where $I \subset S$ is a monomial ideal.

Recall: $H(k[x_1, \dots, x_s], t) = \binom{t+s-1}{s-1}$ (exercise sheet).

Algorithm 1. Let $I = (f_1, \dots, f_n)$ be generated by monomials $f_1, \dots, f_n$. We have an exact sequence of graded modules

$$S(-i) \xrightarrow{f_n} S/(f_1, \dots, f_{n-1}) \longrightarrow S/I \longrightarrow 0$$

where $i = \deg(f_n)$. Now $S(-i) \cong f_n S$ by multiplication by f_n. Now the kernel of the map $f_n S \to S/(f_1, \dots, f_n)$ is $(f_n) \cap (f_1, \dots, f_n) = (\operatorname{lcm}(f_1, f_n), \dots, \operatorname{lcm}(f_{n-1}, f_n))$. So using the isomorphism $S(-i) \overset{\cdot f_n}{\to} f_n S$ we have

$$J = \ker\left(S(-i) \overset{\cdot f_n}{\to} \frac{S}{f_1, \dots, f_{n-1}}\right) = \left(\frac{1}{f_n} \operatorname{lcm}(f_1, f_n), \dots, \frac{1}{f_n} \operatorname{lcm}(f_{n-1}, f_n)\right)$$

Hence we have a short exact sequence of graded S-modules:

$$0 \longrightarrow S/J(-i) \longrightarrow S/I' \longrightarrow S/I \longrightarrow 0$$

where $I' = (f_1, \dots, f_{n-1})$. Hence

$$H(S/I, t) = H(S/I', t) - H(S/J, t - i)$$

Since J and I' have fewer monomial generators than I, this process will eventually stop. The computation of $H(S/I, t)$ is recursively reduced to the computation of Hilbert polynomials of polynomial rings.

Remark.

- We can assume $f_i \nmid f_j$ for $i \neq j$ by removing redundant generators.
- If f_n contains the highest degree of variable among $f_1, \dots, f_n$, then the generators of the ideal $J = (\frac{1}{f_n} \operatorname{lcm}(f_i, f_n))$ do not contain that variable.

Our next goal is to compute $H(S/I)$ when I is homogeneous but not necessarily monomial

Definition 3.48. A *monomial order* on $S = k[x_1, \dots, x_n]$ is a total order $\preceq$ on the set of monomials in S such that

1. $x^\alpha \preceq x^\beta$ implies $x^\alpha x^\gamma \preceq x^\beta x^\gamma$ for all x^γ
2. Any non-empty set of monomials has a minimal element

Recall: A total order on Σ is a partial order $\preceq$ such that for all $x, y \in \Sigma$ we have $x \preceq y$ or $y \preceq x$

Remark. If $x^\alpha | x^\beta$ then $x^\alpha \preceq x^\beta$ for any monomial oder $\preceq$. This is because the smallest monomial is $1 = x^0$ and thus $1 \preceq x^{\beta-\alpha} \Rightarrow x^\alpha \preceq x^{\beta-\alpha}x^\alpha = x^\beta$. To see that 1 is indeed the smallest monomial, let x^α be the smallest monomial. Then $x^\alpha \preceq 1 \Rightarrow x^\alpha \cdot x^\alpha \preceq x^\alpha \Rightarrow x^\alpha \cdot x^\alpha = x^\alpha$ by minimality of x^α, hence $x^\alpha = 1$.

Example. Lexicographic order: $\preceq_{\text{lex}}$, is defined as $x^\alpha \prec_{\text{lex}} x^\beta$ if and only if the first non-zero component from the left of $\beta - \alpha$ is positive.

For example: $x_1^2 x_3 x_4^2 \prec_{\text{lex}} x_1^2 x_2 x_3^5$ since $(2,1,5,0) - (2,0,1,2) = (0, \underline{1}, 4, -2)$.

Definition 3.49. Fix a monomial order $\prec$ on S. For $0 \neq f \in S = K[x_1, \ldots, x_n]$, $f = \sum_\alpha c_\alpha x^\alpha$. The *leading monomial* of f is $\text{LM}(f) = x^\beta$ were $x^\beta = \max\{x^\alpha | c_\alpha \neq 0\}$.

The *leading term* of $f = \sum_\alpha c_\alpha x^\alpha$ is $\text{LT}(f) = c_\beta x^\beta$ where $x^\beta = \text{LM}(f)$. By convention $\text{LT}(0) = 0$

For example, let $f = 4x_1^2 x_3 x_5 + 3x_1^2 x_3^2$ and $\prec = \prec_{\text{lex}}$. Then $\text{LM}(f) = x_1^2 x_3^2$ and $\text{LT}(f) = 3x_1^2 x_3^2$.

Definition 3.50. Let $I \subset S$ be an ideal. The *ideal of leading terms* of I is the ideal $\text{LT}(I) = (\text{LT}(g) | g \in I)$, the ideal generated by $\text{LT}(g)$ with $g \in I$. Note that $\text{LT}(I)$ is a monomial ideal.

Definition 3.51. Fix a monomial order $\prec$ on $S = k[x_1, \ldots, x_n]$. Let $I \subset S$ be an ideal, and $f \in S$. A *normal form* of f (with respect to I and $\prec$) is a polynomial $\text{NF}(f) = \sum_{x^\alpha \notin \text{LT}(I)} c_\alpha x^\alpha$ such that $\text{NF}(f) \equiv f \mod I$. Note that $0 = \sum_\emptyset$ is in normal form.

Theorem 3.52. *Fix a monomial order $\prec$ on $S = k[x_1, \ldots, x_n]$ and an ideal $I \subset S$. Then every $f \in S$ has a unique normal form (with respect to $\prec$ and I)*

Proof. Existence of NF: Let $\Sigma = \{f \in S | f \text{ has no normal form}\}$. Want to show that $\Sigma = \emptyset$.

Assume $\Sigma \neq \emptyset$, we know from definition that $0 \notin \Sigma$. Choose $f \in \Sigma$ with $\text{LM}(f) = \min_{g \in \Sigma} \text{LM}(g)$.

If $\text{LM}(f) \in \text{LT}(I)$, then there exists $g \in I$ such that $\text{LT}(f) = \text{LT}(g)$. If $f - g = 0$ then $\text{NF}(f) = 0$ because $f = g \equiv 0 \mod I$. If $f - g \neq 0$, then $\text{LM}(f-g) < \text{LM}(f)$, hence $f - g$ has a normal form by minimality of $\text{LM}(f)$. So $\text{NF}(f) = \text{NF}(f-g) \equiv f - g \equiv f \mod I$. Both being contradiction to $f \in \Sigma$.

On the other hand if $\text{LM}(f) \notin \text{LT}(I)$ then $f = \text{LT}(f) + h$ where $h = f - \text{LT}(f)$. We have $\text{LM}(h) \lneq \text{LM}(f)$ or $h = 0$, hence by minimality of f, h has a normal form $\text{NF}(h)$. Then $\text{NF}(f) = \text{LT}(f) + \text{NF}(h)$ is a normal form of f, contradicting $f \in \Sigma$, hence $\Sigma = \emptyset$, and every $f \in S$ has a normal form.

Uniqueness of NF: Assume $\text{NF}(f) \neq \text{NF}'(f)$ are two normal forms of f, that is $\text{NF}(f) = \sum_{x^\alpha \notin \text{LT}(I)} c_\alpha x^\alpha$, $\text{NF}(f) = \sum_{x^\alpha \notin \text{LT}(1)} c'_\alpha x^\alpha$ and $f \equiv \text{NF}(f) \equiv \text{NF'}(f) \mod I$. Consider $0 \neq g = \text{NF}(f) - \text{NF}'(f) = \sum_{\alpha \notin \text{LT}(I)} (c_\alpha - c'_\alpha) x^\alpha \equiv 0 \mod I$, hence $g \in I$. So $\text{LM}(g) \in \text{LT}(I)$ but all monomials x^α with non-zero coefficient $c_\alpha - c'_\alpha$ occurring in g are not in $\text{LT}(I)$. Hence we have a contradiction, and so $\text{NF}(f) = \text{NF}'(f)$. ☐

Corollary 3.53. *The monomials $x^\alpha \notin LT(I)$ forms a k-basis of S/I*

Proof. Direct consequence of the theorem ☐

Theorem 3.54. *Let $I \subset S = k[x_1, \ldots, x_n]$ be a homogeneous ideal. Fix a monomial order $\prec$ on S. Then S/I and $S/LT(I)$ have the same Hilbert polynomial and the same Poincaré series.*

Note. $\text{LT}(I)$ is a monomial ideal, so there exists an algorithm (Algorithm 1) for computing $H(S/\text{LT}(I), t)$ (provided we know a set of monomial generators of $\text{LT}(I)$)

Proof. For $f \in S$, let $f = \sum c_\alpha x^\alpha$ then $f_i = \sum_{|\alpha|=i} c_\alpha x^\alpha$ is the homogeneous degree i part of f where $|\alpha| = \alpha_1 + \cdots + \alpha_n$. So $f = \sum_{i \geq 0} f_i$. $I \subset S$ is homogeneous if and only if for all $f \in I$ we have $f_i \in I \, \forall i \geq 0$. If f is homogeneous of degree i, then $\text{NF}(f)_i$ is a normal form of f, and hence $\text{NF}(f)$ is homogeneous of degree i (by uniqueness of normal form). Hence for all $f \in S_i =$ degree i homogeneous polynomial, there exists a unique expression $\text{NF}(f) = \sum_{x^\alpha \notin \text{LT}(I), |\alpha| = i} c_\alpha x^\alpha \equiv f \mod I_i$. So S_i/I_i has k-basis $\{x^\alpha \notin \text{LT}(I) | |\alpha| = i\}$ but this is also a k-basis for $S_i/\text{LT}(I)_i$. Hence $\dim_k S_i/I_i = \dim_k S_i/\text{LT}(I)_i = \forall i$. In particular, S/I and $S/\text{LT}(I)$ have the same Hilbert polynomial and Poincaré series. ☐

We have the natural questions,

1. Given generators $f_1, \ldots f_n$ of $I \subset S$ and $g \in S$, how can we decide if $g \in I$?
2. Recall $H(S/I) = H(S/\text{LT}(I))$ for I homogeneous ideals of S. How do we find a finite list of monomial generators for $\text{LT}(I)$ given a list of generators for I?

3.7.2 Division Algorithm

Algorithm 2 (Division Algorithm). Let $I=(f_1,\dots,f_n)\subset S=k[x_1,\dots,x_s]$ be an ideal. Fix a monomial order $\prec$ on S. Let $g\in S$. Set $r_0=g$ and assume $r_l\in S$ is defined.

If $r_l=0$ or $\mathrm{LM}(f_i)\nmid \mathrm{LM}(r_l)$ $\forall i=1,...,n$ then STOP. Otherwise choose f_i such that $\mathrm{LM}(f_i)|\mathrm{LM}(r_l)$. Set

$$r_{l+1}=r_l-f_i\cdot\frac{\mathrm{LM}(r_l)}{\mathrm{LT}(f_i)}\qquad (*_l)$$

Repeat.

Note $r_{l+1}=0$ or $\mathrm{LM}(r_{l+1})\lneq \mathrm{LM}(r_l)$ because $\mathrm{LT}(r_l)=\mathrm{LT}(f_i\cdot\frac{r_l}{\mathrm{LT}(f_i)})$. Since $\prec$ is a monomial order, the division algorithm eventually stops, say at step l, with either

- $r_l=0$ then by $(*_1),\dots,(*_l)$ we have $g=r_0=\sum_{i=1}^h h_if_i$ for some $h_i\in S$ with $\mathrm{LM}(h_if_i)\le\mathrm{LM}(g)$.
- $r_l\neq0$ then $\mathrm{LM}(f_i)\nmid\mathrm{LM}(r_l)$ for all i, that is $\mathrm{LM}(r_l)\notin(\mathrm{LM}(f_1),\dots,\mathrm{LM}(f_n))$.

r_l is called *remainder of g on division by $f_1,...,f_n$*.

Definition 3.55. Let $S=k[x_1,\dots,x_n]$ and $\prec$ a monomial order on S. Let $I\subset S$ be an ideal, then a *Groebner basis* for I (with respect to $\prec$) is a finite set, $f_1,\dots,f_n\in I$ such that $\mathrm{LT}(I)=(\mathrm{LM}(f_1),\dots,\mathrm{LM}(f_n))$.

Theorem 3.56. *Fix a monomial order $\prec$ on $S=k[x_1,...,x_s]$ and let $f_1,\dots,f_n\in I$ be a Groebner basis for the ideal $I\subset S$. Let $g\in S$, then $g\in I$ if and only if the division algorithm yields remainder 0 on division by $f_1,\dots,f_n$*

Proof. "$\Leftarrow$": If $r_l=0$, then $f=\sum h_if_i$.

"$\Rightarrow$": Recall that the division algorithm stops with $r_l=0$ or $\mathrm{LM}(r_l)\notin(\mathrm{LM}(f_1),\dots,\mathrm{LM}(f_n))=\mathrm{LT}(I)$ since $f_1,\dots,f_n$ are a Groebner basis. If $g\in I$, then $r_i\in I$ for all i, in particular, $\mathrm{LM}(r_l)\in\mathrm{LT}(I)$. Hence $r_l=0$. ☐

Corollary 3.57. *If $f_1,\dots,f_n\in I$ is a Groebner basis for I then $I=(f_1,\dots,f_n)$.*

Proof. Every $g\in I$ gives remainder 0, on application of the division algorithm. Hence $g=\sum h_if_i\in(f_1\dots,f_n)$. ☐

Theorem 3.58 (Buchberger's Criterion). *Fix a monomial order $\prec$ on $S=k[x_1,\dots,x_n]$. Let $I=(f_1,\dots,f_s)\subset S$ be an ideal. Set*

$$S_{ij}=S(f_i,f_j)=f_i\frac{\mathrm{lcm}(\mathrm{LM}(f_i),\mathrm{LM}(f_j))}{\mathrm{LT}(f_i)}-f_j\frac{\mathrm{lcm}(\mathrm{LM}(f_i),\mathrm{LM}(f_j))}{\mathrm{LT}(f_j)}$$

for $i<j$, $i,j=1,\dots,s$. Then the following are equivalent:

1. *$f_1,\dots,f_s$ are a Groebner basis for $I=(f_1,\dots,f_s)$*
2. *For all $i<j$, $i,j\in1,\dots,s$ we have S_{ij} yields remainder 0 on application of the division algorithm by $f_1,\dots,f_s$.*

Proof. 1. $\Rightarrow$2. is clear since $S_{i,j}\in I=(f_1,\dots,f_s)$. Hence since $f_1,\dots,f_s$ is a Groebner basis, we have S_{ij} yields remainder 0 on application of division algorithm (Thoerem 3.56).

2. $\Rightarrow$1, : $I=(f_1,\dots,f_s)$. We have to show $(\mathrm{LM}(f_1),\dots,\mathrm{LM}(f_s))=\mathrm{LT(I)}$. Assume $J=(\mathrm{LM}(f_1),\dots,\mathrm{LM}(f_s))\subsetneq\mathrm{LT}(I)$. Let

$$x^\delta=\min_{\prec}\left\{\max_{i=1,\dots,s}\mathrm{LM}(h_if_i)|\exists g\in I,\mathrm{LT}(g)\notin J,g=\sum_{i=1}^s h_if_i\right\}$$

Let

$$l=\min\left\{\#\{i=1,\dots,s|\mathrm{LM}(h_if_i)=x^\delta\}|g\in I,\mathrm{LT}(g)\notin J,g=\sum_{i=1}^s h_if_i,\ \max_{i=1,\dots,s}\mathrm{LM}(h_if_i)=x^\delta\right\}$$

Choose $g\in I$ reaizing x^δ and l. That is, $\mathrm{LT}(g)\notin J$ such that $g=\sum_{i=1}^s h_if_i$, $x^\delta=\max_{i=1,\dots,s}\mathrm{LM}(h_if_i)$ and $\#\{i=1,\dots,s|\mathrm{LM}(h_if_i)=x^\delta\}=l$. By renumbering, we can assume $\mathrm{LM}(h_1f_1),\dots,\mathrm{LM}(h_lf_l)=x^\delta$ and $\mathrm{LM}(h_if_i)<x^\delta$ for $i=l+1,\dots,s$. Now $\mathrm{LM}(g)\le\mathrm{LM}(h_if_i)\le x^\delta\ \forall i=1,\dots,s$. If $\mathrm{LM}(g)=x^\delta=\mathrm{LM}(h_1f_1)=\mathrm{LM}(h_1)\mathrm{LM}(f_1)$, then $\mathrm{LM}(f_1)|\mathrm{LM}(g)$, hence $\mathrm{LT}(g)\in J$ which is a contradiction to our g.

Since $\mathrm{LT}(g)\notin J$, we have $\mathrm{LM}(g)\lneq x^\delta$ and $l\ge2$. Consider

$$S_{12}=f_1\frac{\mathrm{lcm}(\mathrm{LM}(f_1),\mathrm{LM}(f_2))}{\mathrm{LT}(f_1)}-f_2\frac{\mathrm{lcm}(\mathrm{LM}(f_1),\mathrm{LM}(f_2))}{\mathrm{LT}(f_2)}\qquad(a)$$

By assumption, S_{12} has remainder 0 on division by $f_1, \dots, f_s$. Hence, the division algorithm yields

$$S_{12} = \sum_{i=1}^{s} t_i f_i \quad (b)$$

with $\mathrm{LM}(t_i f_i) \le \mathrm{LM}(S_{12}) < \mathrm{lcm}(\mathrm{LM}(f_i), \mathrm{LM}(f_j))$. So by $(a), (b)$ we get

$$-f_1 \frac{\mathrm{lcm}(\mathrm{LM}(f_1), \mathrm{LM}(f_2))}{\mathrm{LT}(f_1)} + f_2 \frac{\mathrm{lcm}(\mathrm{LM}(f_1), \mathrm{LM}(f_2))}{\mathrm{LT}(f_2)} + \sum_{i=1}^{s} t_i f_i = 0 \quad (c)$$

Recall (d) $g = \sum_{i=1}^{s} h_i f_i, \mathrm{LM}(h_i f_i) \le x^\delta, \quad \underbrace{\mathrm{LM}(h_1 f_1) = \mathrm{LM}(h_2 f_2) = x^\delta}_{\Rightarrow \mathrm{LM}(f_i) | x^\delta \Rightarrow \mathrm{lcm} \le x^\delta \Rightarrow x^\delta = \mathrm{lcm} \cdot x^\alpha, \ i=1,2}$.

Multiply (c) with $x^\alpha \cdot \mathrm{LC}(h_1) \cdot \mathrm{LC}(f_1)$ (where LC stands for leading coefficient) and add (d) to obtain

$$\begin{aligned}
g = {} & h_1 f_1 - f_1 \frac{\mathrm{lcm}(\mathrm{LM}(f_1), \mathrm{LM}(f_2))}{\mathrm{LT}(f_1)} x^\alpha \cdot \mathrm{LC}(h_1) \cdot \mathrm{LC}(f_1) + x^\alpha \cdot \mathrm{LC}(h_1) \cdot \mathrm{LC}(f_1) t_1 f_1 && \leftarrow \mathrm{LM} < x^\delta \\
& + h_2 f_2 + f_2 \frac{\mathrm{lcm}(\mathrm{LM}(f_1), \mathrm{LM}(f_2))}{\mathrm{LT}(f_2)} x^\alpha \cdot \mathrm{LC}(h_1) \cdot \mathrm{LC}(f_1) + x^\alpha \cdot \mathrm{LC}(h_1) \cdot \mathrm{LC}(f_1) t_2 f_2 && \leftarrow \mathrm{LM} \le x^\delta \\
& + h_3 f_3 + x^\alpha \cdot \mathrm{LC}(h_1) \cdot \mathrm{LC}(f_1) t_3 f_3 && \leftarrow \mathrm{LM} \le x^\delta \\
& + \vdots && \vdots \\
& + h_l f_l + x^\alpha \cdot \mathrm{LC}(h_1) \cdot \mathrm{LC}(f_1) t_l f_l && \leftarrow \mathrm{LM} \le x^\delta \\
& + h_{l+1} f_{l+1} + x^\alpha \cdot \mathrm{LC}(h_1) \cdot \mathrm{LC}(f_1) t_{l+1} f_{l+1} && \leftarrow \mathrm{LM} < x^\delta \\
& + \vdots && \vdots \\
& + h_s f_s + x^\alpha \cdot \mathrm{LC}(h_1) \cdot \mathrm{LC}(f_1) t_s f_s && \leftarrow \mathrm{LM} < x^\delta
\end{aligned}$$

This is an expression of $g = \sum \widetilde{h}_i f_i$ with $\mathrm{LM}(\widetilde{h_1} f_1) < x^\delta$, $\mathrm{LM}(\widetilde{h}_i f_i) = x^\delta$ for $i = 2, \dots l$, and $\mathrm{LM}(\widetilde{h_1} f_1) < x^\delta$ for $i = l+1, \dots, s$. This contradicts the choice of g (the minimality of l).

Hence $J = (\mathrm{LM}(f_1), \dots, \mathrm{LM}(f_s)) = \mathrm{LT}(I)$. □

3.7.3 Buchberger's Algorithm for finding a Groebner basis

Let $I = (f_1, \dots, f_n) \subset k[x_1, \dots, x_s]$, and let $S_{ij} = f_i \frac{\mathrm{lcm}(\mathrm{LM}(f_i), \mathrm{LM}(f_j))}{\mathrm{LT}(f_i)} - f_j \frac{\mathrm{lcm}(\mathrm{LM}(f_i), \mathrm{LM}(f_j))}{\mathrm{LT}(f_j)}$ as before.

Algorithm 3 (Buchberger's Algorithm). If all remainders r_{ij} obtained by applying the division algorithm to S_{ij} are 0 then STOP (then $f_1, \dots, f_n$ is a Groebner basis for I)

Otherwise, add r_{ij} to the list of generators of I and repeat.

The algorithm stops eventually because if $r_{ij} \neq 0$ then $r_{ij} \in I$ (Since $S_{ij} \in I$) but $\mathrm{LT}(r_{ij}) \notin (\mathrm{LT}(f_1), \dots, \mathrm{LT}(f_n)) \subset \mathrm{LT}(I)$. Since $\mathrm{LT}(I) \subset S$ is a Noetherian Ideal, the algorithm has to stop. By Theorem 3.58, the resulting list of generators for I is a Groebner basis for I.

Example. Let us find a Groebner basis for $I = (x^2 + yz, xy + z^2) \subset k[x, y, z] = S$ with respect to $\prec_{\mathrm{lex}}$ $(x \succ y \succ z)$. Compute $H(S/I)$, $P(S/I, t)$.

i	1	2	3	4
f_i	$x^2 + yz$	$xy + z^2$	$-y^2 z + xz^2$	$y^3 z + z^4$
$\mathrm{LM}(f_i)$	x^2	xy	xz^2	$y^3 z$

- $S_{12} = (x^2 + yz)y - (xy + z^2)x = y^2 z - xz^2$ has $\mathrm{LM} = xz^2$ which is not divisible by $\mathrm{LM}(f_i)$, $i = 1, 2$. So we add S_{12} to the list of generators.
- $S_{13} = (x^2 + yz)z^2 - (xz^2 - y^2 z)x = yz^3 + xy^2 z = (xy + z^2)yz$, so it has remainder 0.
- $S_{23} = (xy + z^2)z^2 - (xz^2 - y^2 z)y = z^4 + y^3 z$ has $\mathrm{LM} = y^3 z$ which is not divisible by $\mathrm{LM}(f_i)$, $i = 1, 2, 3$. So we add S_{23} to the list of generators.
- S_{14}, S_{24} and S_{34} all lead to remainder 0.

Hence $\{x^2+yx, xy+z^2, xz^2-y^2z, y^3z+z^4\}$ is a Groebner basis for I. We know that $H(S/I)=H(S/\mathrm{LT}(I))$ and $P(S/I,t)=P(S/\mathrm{LT}(I),t)$ and we have $\mathrm{LT}(I)=(x^2,xy,xz^2,y^3z)$.

To compute $H(S/\mathrm{LT}(I))$, $P(S/\mathrm{LT}(I),t)$ we recall from the beginning of section 3.7.1 the exact sequence of graded S-modules

$$0 \longrightarrow S/J(-i) \xrightarrow{f_n} S/(f_1,\dots,f_{n-1}) \longrightarrow S/I \longrightarrow 0$$

and so we start with the exact sequence

$$0 \longrightarrow \frac{S}{(y,z^2,y^3z)}(-2) \xrightarrow{x^2} \frac{S}{(xy,xz^2,y^3z)} \longrightarrow \frac{S}{\mathrm{LT}(I)} \longrightarrow 0$$

and note that the first two graded S-modules have fewer relations. If we keep repeating we end up with $H(S/\mathrm{LT}(I))=2$.

Our next goal is: Let $I\subset m=(x_1,\dots,x_s)\subset k[x_1,\dots,x_s]=S$ and let $R=S/I$. Recall that $\dim R_m = 1+\deg H(\mathrm{gr}_m R)$. We want to find a homogeneous ideal $J\subset S$ such that $\mathrm{gr}_m R = S/J$ and generators for J. This will allow us to compute $H(\mathrm{gr}_m R)$ in view of Algorithms 1 and 3 and Theorem 3.54.

Notation.

- Let $f=x_1^{\alpha_1}\dots x_s^{\alpha_s}$, then the total degree of f is denoted $|f|=\alpha_1+\dots+\alpha_s$
- $g\in S=k[x_1,\dots,x_s]$ is homogeneous of degree i if $g=\sum_{|x^\alpha|=i} c_\alpha x^\alpha$.
- $S_i=\{$ homogeneous of polynomial of degree $i\}$ then $S=\oplus_{i=1}^\infty S_i$
- Every $g\in S$ has a unique expression as $g=\sum_{i=1}^n g_i$ with $g_i\in S_i$.
- For $0\neq g\in S$ write $g=g_0+g_1+\dots$ with $g_i\in S_i$, let $g_{\mathrm{bot}}=g_{\mathrm{bottom}}=g_l$ where $l=\min\{i|g_i\neq 0\}$. If $g=0$ set $g_{\mathrm{bot}}=0$. e.g., $(x^2y^3z+x^2y+z^3)_{\mathrm{bot}}=x^2y+z^3$

If $m=(x_1,\dots,x_s)\subset S=k[x_1,\dots,x_s]$, then $m^i=\{g\in S|g=0, \text{ or } \deg(g_{\mathrm{bot}})\geq i\}$. Hence $m^i/(m^{i+1})$ has k-basis the monomials of degree i.

The map $k[x_1,\dots,x_s]=S\to \mathrm{gr}_m S=\oplus m^i/m^{i+1}$ defined by $x_j\mapsto x_j \mod m$ in degree 1, is a ring isomorphism with inverse in degree i: $m^i/m^{i+1}\to S_i$ defined by $g\mapsto g_i$.

Let $I\subset m\subset S$ be any ideal, $R=S/I$. Let $J=\ker(S\cong \mathrm{gr}_m(S)\twoheadrightarrow \mathrm{gr}_m(R))$. Then $\mathrm{gr}_m(R)=S/J$ where $J=\oplus_{i=0}^\infty J_i$ and $J_i=\ker(S_i\cong \underbrace{\mathrm{gr}_m(S)_i}_{m^i/m^{i+1}}\twoheadrightarrow \underbrace{\mathrm{gr}_m(R)_i}_{m_R^i/m_R^{i+1}})$. Here $m_R=m/I\subset S/I$ is the maximal ideal of R. This has i-th power $m_R^i=(m^i+I)/I$. So $m_R^i/m_R^{i+1}=(m^i+I)/(m^{i+1}+I)=m^i/((m^{i+1}+I)\cap m^i)$. Hence

$$\begin{aligned} J_i &= \ker(S_i\cong m^i/m^{i+1}\twoheadrightarrow m^i/((m^{i+1}+I)\cap m^i)\\ &= ((m^{i+1}+I)\cap m^i)/m^{i+1}\\ &= \{g+f|\deg(g_{\mathrm{bot}})\geq i+1, f\in I, \deg(f_{\mathrm{bot}})\geq i\}/m^{i+1}\\ &= \{f\in I|\deg(f_{\mathrm{bot}})=i\}\end{aligned}$$

So $J=\oplus_{i=0}^\infty J_i$ and hence $J=\{f_{\mathrm{bot}}|f\in I\}$

Definition 3.59. The *homogenisation* of $f=\sum_\alpha c_\alpha x^\alpha\in S=k[x_1,...,x_s]$ is the polynomial $F\in S[x_0]=k[x_0,x_1,\dots,x_s]$ defined by $F=\sum_\alpha c_\alpha x_0^{|f|-|\alpha|}x^\alpha=\sum_\alpha c_\alpha x^{|f|}\left(\frac{x}{x_0}\right)^\alpha = x_0^{|f|}f(\frac{x_1}{x_0},\dots,\frac{x_s}{s_0})$.

A monomial order on $S[x_0]$ *refines the order by degree in* x_0 if $x^\alpha\prec x^\beta$ (where $\alpha=(\alpha_0,\dots,\alpha_s),\beta=(\beta_0,\dots,\beta_s)$) implies $\alpha_0\leq\beta_0$.

Example. The homogenisation of $f=x_1^2x_2+x_2^5x_3$ is $F=x_0^3x_1^2x_2+x_2^5x_3$.

The lexicographic order on $S[x_0]$ with $x_0\succ x_1\succ\dots\succ x_n$ refines the order by degree in x_0.

Theorem 3.60. *Let k be a field, $S=k[x_1,\dots,x_s]$, $I=(f_1,\dots,f_n)\subset S$ an ideal such that $I\subset m=(x_1,\dots,x_s)$, and $R=S/I$. Let $F_1,\dots,F_n\in S[x_0]$ be the homogenisation of $f_1,\dots,f_n$. Let $G_1,\dots,G_r$ be a Groebner basis for the ideal $(F_1,\dots,F_n)\subset S[x_0]$ with respect to a monomial order on $S[x_0]$ that refines the order by degree in x_0. Then*

$$gr_m R\cong \frac{S}{((g_1)_{\mathrm{bot}},\dots,(g_r)_{\mathrm{bot}})}$$

where $g_i=G_i(1,x_1,\dots,x_s)$.

Proof. Recall that we showed above $\mathrm{gr}_m R \cong S/J$ where $J = (f_{\mathrm{bot}} | f \in I)$. Hence we need to show that for $0 \neq g \in I$ we have $g_{\mathrm{bot}} \in ((g_1)_{\mathrm{bot}}, \ldots, (g_r)_{\mathrm{bot}})$.

Note if $P \in S[x_0]$ is homogeneous then $P = x_0^b p(1, x_1, \ldots, x_s)_{\mathrm{bot}} + \text{lower degree } x_0 \text{ terms} \quad (*)$. Let $0 \neq g \in I$, then $g = \sum_{i=1}^n h_i f_i$ for some $h_i \in S$. Let G and H_i be the homogenisation of g and h_i.

$$\begin{aligned} G &= x_0^{|g|} g\left(\frac{x_1}{x_0}, \ldots, \frac{x_s}{x_0}\right) \\ &= x_0^{|g|} \sum_{i=1}^n h_i \left(\frac{x_1}{x_0}, \ldots \frac{x_s}{x_0}\right) f_i \left(\frac{x_1}{x_0}, \ldots \frac{x_s}{x_0}\right) \\ &= x_0^{|g|} \sum_{i=1}^n \frac{1}{x_0^{|h_i + f_i|}} H_i F_i \end{aligned}$$

Hence there exists $a, a_i \in \mathbb{N}$ such that $Gx_0^{\alpha} = \sum x_0^{\alpha_i} H_i F_i \in (F_1, \ldots, F_n)$. But if $G_1, \ldots, G_r$ is a Groebner basis for $(F_1, \ldots, F_n)$, we have $Gx_0^a = \sum P_i G_i$ $(\dagger)$ for some $P_i \in S[x_0]$ such that $\mathrm{LM}(P_i G_i) \leq \mathrm{LM}(Gx_0^a)$ $(**)$ by the division algorithm. So by $(*)$ we have $Gx_0^a = x_0^b \underbrace{G(1, x_1, \ldots, x_s)_{\mathrm{bot}}}_{g_{\mathrm{bot}}} + \text{lower degree terms in } x_0$. Since the monomial order $\prec$ refines the order by degree in x_0, we have $(**)$ implies $b \geq \deg_{x_0}(P_i G_i)$. Then from $(\dagger)$, we have $x_0^b g_{\mathrm{bot}} = \sum_{b = \deg_{x_0}(P_i G_i)} x_0^b \underbrace{P_1(1, x_1, \ldots x_s)_{\mathrm{bot}}}_{p_i} \underbrace{G_i(1, x_1, \ldots, x_s)_{\mathrm{bot}}}_{(g_i)_{\mathrm{bot}}}$. This means $g_{\mathrm{bot}} = \sum p_i \cdot (g_i)_{\mathrm{bot}} \in ((g_1)_{\mathrm{bot}}, \ldots, (g_r)_{\mathrm{bot}})$ $\square$

4 Smooth and Etale Extensions

4.1 Derivations and the Module of Kähler Differentials

Definition 4.1. Let A be an R-algebra, and M an A-module. An *R-derivation of M* is an R-linear map $\delta : A \to M$ satisfying the Leibniz rule: $\delta(ab) = a\delta(b) + b\delta(a) \, \forall a, b \in A$.

Example. Let $A = R[x_1, \dots, x_s]$ be the polynomial ring in s variables. Then for $i = 1, \dots, s$ define $\frac{\partial}{\partial x_i} : A \to A$ on the monomials (which form an R-basis) as $\frac{\partial}{\partial x_i}(x_1^{\alpha_1} \dots x_s^{\alpha_s}) = \alpha_i x_1^{\alpha_1} \dots x_{i-1}^{\alpha_{i-1}} \underline{x_i^{\alpha_i - 1}} x_{i+1}^{\alpha_{i+1}} \dots x_s^{\alpha_s}$ and extended it R-linearly to a map $A \to A$. Then $\frac{\partial}{\partial x_i}$ is an R-derivation. (Check $\frac{\partial}{\partial x_i}(x^\alpha x^\beta) = x^\alpha \frac{\partial}{\partial x_i} x^\beta + x^\beta \frac{\partial}{\partial x_i} x^\alpha$) .

Remark. If $f : M \to N$ is an A-module, $g : B \to A$ is an R-algebra homomorphism and $\delta : A \to M$ an R-derivation then $f\delta : A \to N$ and $\delta g : B \to M$ are R-derivations.

Notation. Write $\mathrm{Der}_R(A, M)$ for the set of R-derivations $A \to M$.

Remark. $\mathrm{Der}_R(A, M)$ is an A-module as follows: If $\delta, \delta' \in \mathrm{Der}_R(A, M)$ then $\forall a, b \in A$ we have $a\delta + b\delta' : A \to M$ is an R-derivation. This makes $\mathrm{Der}_R(A, M)$ into an A-module.

Lemma 4.2. *Assume $\delta : A \to M$ which is $\mathbb{Z}$-linear and satisfies the Leibniz rule. Then δ is R-linear if and only if $\delta(r \cdot 1) = 0 \, \forall r \in R$.*

Proof. We have $\delta(1) = \delta(1 \cdot 1) = 1 \cdot \delta(1) + 1 \cdot \delta(1)$ by Leibniz rule, hence $\delta(1) = 0$.
"$\Rightarrow$": $\delta(r \cdot 1) = r\delta(1) = 0$
"$\Leftarrow$": $\delta(r \cdot a) = a\delta(r \cdot 1) + r\delta(a) = 0 + r\delta(a)$ □

Definition 4.3. Let A be an R-algebra. The *universal R-derivation,* the module of Kaehler differentials, is an A-module $\Omega_{A/R}$ together with an R-derivation $d : A \to \Omega_{A/R}$ such that for every R-derivation $\delta : A \to M$ there is a $(*)$ unique A-module map $f : \Omega_{A/R} \to M$ such that $\delta = f \circ d$.

Note. $(*)$ is equivalent to $\mathrm{Hom}_R(\Omega_{A/R}, M) \cong \mathrm{Der}_R(A, M)$ defined by $f \mapsto f \circ d$.

Lemma 4.4. *The universal R-derivation $(\Omega_{A/R}, d)$ is unique in the sense that if (Ω', d') also satisfies $(*)$ then there is a unique A-module isomorphism $f : \Omega_{A/R} \to \Omega'$ such that $f \circ d = d'$.*

Proof. Exercise □

Lemma 4.5 (Construction of $\Omega_{A/R}$)**.** *Let A be an R-algebra, then the universal R-derivation $(\Omega_{A/R}, d)$ exists.*

Proof. Construction of $(\Omega_{A/R}, d)$: Let $F = \oplus_{a \in A} A da$ be the free A-module with basis the symbols da for $a \in A$. We have a map of sets $d : A \to F$ defined by $a \mapsto da$. We want to impose the relations that ensure R-linearity and the Leibniz rule. We therefore define the following sets:

$dR =$ $\{dr \cdot 1 | r \in R\}$

Linearity:= $\{d(a + b) - da - db | a, b \in A\}$

Leibniz:= $\{d(ab) - adb - bda | a, b \in A\}$

Set

$$\Omega_{A/R} = \frac{F}{A \cdot dR, A \cdot (\text{Linearity}), A \cdot (\text{Leibniz})}$$

where for a subet S of a module M, we denote by $A \cdot S$ the A-submodule generated by S. The quotient $\Omega_{A/R}$ is an A-module equipped with a map $d : A \to \Omega_{A/R}$ defined by $a \mapsto da$, which is an R-derivation and satisfies the condition $(*)$ to be the universal $R-$derivation (exercise) □

Remark. (Functoriality): If $f : A \to B$ is an R-algebra map, we have a well-defined A-module map $\Omega_{A/R} \to \Omega_{B/R}$ defined by $da \mapsto df(a)$, and hence and induced B-module map $B \otimes_A \Omega_{A/R} \to \Omega_{B/R}$ defined by $b \otimes da \mapsto dbf(a)$.

Example. Let $A = R[T_1, \dots, T_n]$. Then $\Omega_{A/R} = \oplus_{i=1}^n A dT_i$, free A-module with basis $dT_1, \dots, dT_n$ equipped with the R-derivation $d : A \to \Omega_{A/R}$ defined by $f \mapsto \sum_{i=1}^n \frac{\partial f}{\partial T_i} dT_i$

Proof of Example. We already saw that $\frac{\partial}{\partial T_i} : A \to A$ is an R-derivation, hence $d : A \to \Omega_{A/R}$ is an R-derivation.

Let $\delta : A \to M$ be an R-derivation. Then $\delta(f) = \sum_{i=1}^n \frac{\partial f}{\partial T_i}\delta(T_i)$ because both sides are R-derivations, which agree on the set $T_i, \dots, T_n$ generating A as R-algebra. Hence there exists a unique A-module map $\phi : \Omega_{A/R} = \oplus_{i=1}^n AdT_i \to M$ sending $dT_i \mapsto \delta(T_i)$, such that $\phi \circ d = \delta$. □

Yoneda Lemma. *Let $f : M \to N$ be an A-module homomorphism. Then f is an isomorphism, if and only if for all A-module P, $\hom_R(N,P) \to \hom_R(M,P)$ defined by $g \mapsto g \circ f$ is an isomorphism.*

Proof. "⇒" is clear.

"⇐". Choose $P = M$, then there exists $g \in \hom_R(N,M)$ such that $gf = 1$. Since $fgf = f = \mathrm{id}_N f$, choosing $P = N$ yields $fg = 1$. Hence f is an isomorphism with inverse g. □

Lemma 4.6. *Let A be an R-algebra, $S \subset A$ a multiplicative subset. Then $S^{-1}\Omega_{A/R} \to \Omega_{S^{-1}A/R}$ defined by $\frac{da}{s} \mapsto \frac{da}{s}$ is an isomorphism of $S^{-1}A$-modules.*

Proof. Let M be an $S^{-1}A$-module. Then $\mathrm{Der}_R(S^{-1}A, M) \to \mathrm{Der}_R(A,M)$ defined by $\delta \mapsto (A \to S^{-1}A \xrightarrow{\delta} M)$ is an isomorphism with inverse $\mathrm{Der}_R(A,M) \to \mathrm{Der}_R(S^{-1}A, M)$ defined by $(\delta : A \to M) \mapsto \delta'$ where $\delta'\left(\frac{a}{s}\right) = \frac{1}{s}\delta(a) - \frac{1}{s^2}a\delta(s)$. One checks that δ' is a well-defined R-derivation defining the inverse. Then:

$$\begin{aligned} \mathrm{Hom}_{S^{-1}A}(\Omega_{S^{-1}A/R}, M) &= \mathrm{Der}_R(S^{-1}A, M) \\ &\cong \mathrm{Der}_R(A, M) \\ &= \mathrm{Hom}_A(\Omega_{A/R}, M) \\ &= \mathrm{Hom}_{S^{-1}A}(S^{-1}\Omega_{A/R}, M), \end{aligned}$$

the isomorphism of hom-sets being induced by the map $S^{-1}\Omega_{A/R} \to \Omega_{S^{-1}A/R}$ in the Lemma. By the Yoneda Lemma, this implies $\Omega_{S^{-1}A/R} \cong S^{-1}\Omega_{A/R}$ □

Lemma 4.7. *Let A, B be R-algebras. Then $A \otimes_R \Omega_{B/R} \to \Omega_{A \otimes_R B/A}$ defined by $da \mapsto d(a \otimes 1)$ is an isomorphism of $A \otimes_R B$-modules.*

Proof. Consider the following commutative diagram of rings

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "g"'] & A \arrow[d, "\overline{g}"] \\ B \arrow[r, "\overline{f}"'] & A \otimes_R B \end{tikzcd}$$

Let M be an $A \otimes_R B$-module. Then the map $\mathrm{Der}_A(A \otimes_R B, M) \to \mathrm{Der}_R(B, M)$ defined by $\delta \mapsto \delta \circ f$ is an isomorphism with inverse, $\mathrm{Der}_R(B,M) \to \mathrm{Der}_A(A \otimes_R B, M)$ defined by $(\delta : B \to M) \mapsto (A \otimes_R B \overset{1 \otimes \delta}{\to} A \otimes_R M \overset{\text{multi}}{\to} M)$. As in the previous lemma, Yoneda implies $\Omega_{A \otimes_R B/A} \cong A \otimes_R \Omega_{B/R}$, because for all $A \otimes_R B$-modules M

$$\begin{aligned} \mathrm{Hom}_{A \otimes_R B}(\Omega_{A \otimes B/A}, M) &= \mathrm{Der}_A(A \otimes_R B, M) \\ &= \mathrm{Der}_R(B, M) \\ &= \mathrm{Hom}_A(\Omega_{B/R}, M) \\ &= \mathrm{Hom}_{A \otimes_R B}(A \otimes_R \Omega_{B/R}, M) \end{aligned}$$

□

1st Fundamental Exact Sequence. *Let $R \to A \to B$ be maps of rings. Then the following is an exact sequence of B-modules:*

$$B \otimes_A \Omega_{A/R} \xrightarrow{g} \Omega_{B/R} \longrightarrow \Omega_{B/A} \longrightarrow 0$$

$$b \otimes da \longmapsto b \cdot df(a) \; ; \; db \longmapsto db$$

Proof. $\mathrm{im}(g) = BdA$,

$$\begin{aligned}
\mathrm{coker}(g) &= \frac{\Omega_{B/R}}{\mathrm{im}(g)} \\
&= \frac{\Omega_{B/R}}{BdA} \\
&= \frac{\oplus_{b\in B} db}{B\cdot dR, B\cdot\ (\text{linearity}), B\cdot\ (\text{Leibniz}), B\cdot dA} \\
&= \Omega_{B/A}
\end{aligned}$$

□

2nd Fundamental Exact Sequence. *Consider $R \to A \to B = A/I$ maps of rings, where $I \subset A$ is an ideal. Then the following is an exact sequence of B-modules:*

$$I/I^2 \xrightarrow{d} B \otimes_A \Omega_{A/R} \longrightarrow \Omega_{B/R} \longrightarrow 0$$

$$a \longmapsto 1 \otimes da\ ;\ b \otimes da \longmapsto bda$$

Remark. $1 \otimes d(I^2) = 0 \subset B \otimes_A \Omega_{A/R}$. This is because for $x, y \in I \subset A$, $1 \otimes d(xy) = 1 \otimes xdy + 1 \otimes ydx = x \otimes dy + y \otimes dx = 0 \in A/I \otimes \Omega_{A/R}$ as $x, y = 0 \in A/I$. Therefore, the first map of the exact sequence is well-defined. Furtheremore, since $I(I/I^2) = 0$, the A-module I/I^2 is in fact an A/I-module and the sequence is a sequence of A/I-modules.

Proof. The image of the first map in the sequence is the B-submodule generated by dI, that is, $\mathrm{im}(d) = B \cdot dI$.

$$\begin{aligned}
\mathrm{coker}(d) &= \frac{B \otimes_A \Omega_{A/R}}{\mathrm{im}(d)} \\
&= \frac{B \otimes_A \Omega_{A/R}}{BdI} \\
&= \frac{B \otimes_A \left(\frac{\oplus_{a\in A} Ada}{AdR, A\,\text{linearity}, A\,\text{Leibniz}}\right)}{BdI} \\
&= \frac{\otimes_{a\in A} Bda}{BdR, B\,\text{linearity}, B\,\text{Leibniz}, BdI} && B\text{ linearity and } BdI \Rightarrow dx = dy \text{ if } x = y \mod I \\
&= \frac{\oplus_{b\in B} Bdb}{BdR, B\,\text{linearity}, B\,\text{Leibniz}} \\
&= \Omega_{B/R}
\end{aligned}$$

□

Remark. Assume $B = R[x_1, \dots, x_s]/(f_1, \dots, f_r)$, with $I = (f_1, \dots, f_r) \subset A := R[x_1, \dots, x_s]$. Then by the 2nd fundamental exact sequence we have an exact sequence of B-modules

$$I/I^2 \longrightarrow B \otimes_A \Omega_{A/R} \longrightarrow \Omega_{B/R} \longrightarrow 0$$

where $\Omega_{A/R} = \oplus_{i=1}^s Adx_i$, so $B \otimes_A \Omega_{A/R} = \oplus_{i=1}^s Bdx_i$. Now I is generated by $f_1, \dots, f_r$ as A-module. Since I/I^2 generated by $f_1, \dots, f_r$ as A-module and I/I^2 is generated by $f_1, \dots, f_r$ as $B = A/I$-module, the map $B^r = \oplus_{j=1}^r Be_j \twoheadrightarrow I/I^2$ defined by $e_j \mapsto f_j$ is surjective. So

$$\begin{tikzcd}
& I/I^2 \arrow[dr, "1\otimes d"] & & & \\
B^r \arrow[ur, two heads] \arrow[rr, "J(f)"'] & & B^s \arrow[r] & \Omega_{B/R} \arrow[r] & 0
\end{tikzcd}$$

is an exact sequence, where $J(f) = \left(\frac{\partial f_i}{\partial x_j}\right) \in M_{sr}(B)$. This is called the *Jacobi matrix* of $f = (f_1, \dots, f_r)$

Example. Let $B = k[x, y, z]/(x^2y, x^3 + z^2)$, then $\Omega_{B/k} = \mathrm{coker}(J : B^2 \to B^3)$ where $J = J(x^2y, x^3 + z^2) = \begin{pmatrix} 2xy & 3x^2 \\ x^2 & 0 \\ 0 & 2z \end{pmatrix}$.

4.2 Formally smooth and étale Extensions

Definition 4.8. A ring homomorphism $f : R \to A$ is called

- *formally smooth* if

  $(*)$ for all rings C, ideals $J \subset C$ with $J^2 = 0$, ring maps $g : R \to C, \overline{g} : A \to C/J$ such that $\overline{g}f = \overline{f}g$ where $\overline{f} : C \to C/J$ the quotient map,

  there exists a ring map $G : A \to C$ such that $Gf = g$, $\overline{f}G = \overline{g}$. (That is the diagram below commutes in each triangle)

$$\begin{tikzcd} R \arrow[r, "g"] \arrow[d, "f"'] & C \arrow[d, "\overline{f}"] \\ A \arrow[r, "\overline{g}"'] \arrow[ur, dashed, "\exists G"] & C/J \end{tikzcd}$$

- *formally étale* if $(*)$, there exists a <u>unique</u> ring map $G : A \to C$ such that $Gf = g$, $\overline{f}G = \overline{g}$
- It has *finite presentation* if it is $f : R \to R[x_1, \dots, x_s]/(f_1, \dots, f_r)$
- *smooth* (respectively *étale*) if it is formally smooth (respectively formally étale) and of finite presentation

Example 4.9. Let $R \to A, R \to B$ be ring homomorphism. If $R \to A$ is formally smooth/formally étale/finite presentation/smooth/étale, then so is $B \to A \otimes_R B$ defined by $b \mapsto 1 \otimes b$

$$\begin{tikzcd} R \arrow[r] \arrow[d] & B \arrow[d] \\ A \arrow[r] & A \otimes_R B \end{tikzcd}$$

We show this in the case of formally étale (The other follows the same logic). Assume $h_0 : R \to A$ is formally étale. Let $h : C \to C/J$ be the quotient map where $J \subset C$ an ideal with $J^2 = 0$. Given a commutative diagram of rings

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "h_0"'] & B \arrow[r, "g"] \arrow[d, "h_1"'] & C \arrow[d, "h"] \\ A \arrow[r, "\overline{f}"'] & A \otimes_R B \arrow[r, "\overline{g}"'] & C/J \end{tikzcd}$$

We know h_0 is formally étale, so there exists a unique $F : A \to C$ such that $hgf = Fh_0$, $hF = \overline{g}\overline{f}$. By the universal property of tensor product, there exists a unique $G : A \otimes_R B \to C$ such that $h_1 G = g$ and $\overline{f}G = F$. This G is the unique $G : A \otimes_R B \to C$ such that $h_1 G = g$, $hG = \overline{g}$

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "h_0"'] & B \arrow[r, "g"] \arrow[d, "h_1"'] & C \arrow[d, "h"] \\ A \arrow[r, "\overline{f}"'] \arrow[urr, dashed, "\exists! F"] & A \otimes_R B \arrow[r, "\overline{g}"'] \arrow[ur, dashed, "\exists! G"] & C/J \end{tikzcd}$$

Lemma 4.10. *Given $R \xrightarrow{f} A \xrightarrow{g} B$ be maps of rings. If f and g are formally smooth/formally étale/finite presentation/smooth/étale, then so is $g \circ f$*

Proof. Exercise, follows the same work as in the example ☐

Example. $R \to A = R[x_1, \dots, x_s]$ is smooth. It clearly is of finite presentation. Let $h : C \to C/J$ with $J \subset C$ an ideal such that $J^2 = 0$. Given the commutative diagram of rings

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "g"'] & C \arrow[d, "h"] \\ A = R[x_1, \dots, x_s] \arrow[r, "\overline{f}"'] & C/J \end{tikzcd}$$

choose $c_i \in C$ such that $h(c_i) = \overline{f}(x_i)$ (h is surjective). Define $F : A = R[x_1, \ldots, x_s] \to C$ as the R-algebra map $x_i \mapsto c_i$. Then $Fg = f$ and $hF = \overline{f}$.

Example 4.11. Let $S \subset R$ be a multiplicative subset, then $R \to S^{-1}R$ is formally étale. To see this, consider a commutative diagram of rings

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "g"'] & C \arrow[d, "h"] \\ S^{-1}R \arrow[r, "\overline{f}"'] & C/J \end{tikzcd}$$

where $J^2 = 0$. Since $J^2 = 0$, an element $x \in C$ is a unit if and only if x is a unit in C/J. For all $s \in S$, $hf(s) = \overline{f}\underbrace{g(s)}_{\text{unit}}$ units in C/J implies $f(s) \in C$ is a unit. Hence there exists unique $F : S^{-1}R \to C$ defined by $\frac{r}{s} \mapsto f(s)^{-1}f(r)$, making the diagram commute.

Remark 4.12. In general, the map $R \to S^{-1}R$ is not of finite presentation and hence is not étale. For instance, $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-algebra as any finite set of elements in $\mathbb{Q}$ only involves a finite number of primes in the denominators and the same is true for the algebra generated by these finitely many elements.

However, $R \to R_f = R[T]/(fT-1)$ is of finite presentation and formally étale, hence étale for any $f \in R$.

Example 4.13. $A \times B \to A$ defined by $(a, b) \mapsto a$ is étale. Note that $A = (A \times B)_{(1,0)}$ =localisation of $A \times B$ at $(1, 0) \in A \times B$.

Lemma 4.14. *A map of rings $f : R \to A$ is formally étale if and only if f is formally smooth and $\Omega_{A/R} = 0$*

Proof. If f is étale then f is smooth. Assume f is formally smooth, we will show that f is formally étale if and only if $\Omega_{A/R} = 0$.

Consider a commutative diagram of rings

$$\begin{tikzcd} R \arrow[r, "g"] \arrow[d, "f"'] & C \arrow[d, "\overline{f}"] \\ A \arrow[r, "\overline{g}"'] \arrow[ur, dashed, "G_0"] & C/J \end{tikzcd} \qquad (*)$$

where $J \subset C$ is an ideal such that $J^2 = 0$. Then f is formally smooth means there exists $G_0 : A \to C$ making $(*)$ commute. There exists a bijection of sets between

$$\mathrm{Der}_R(A, J) \leftrightarrow \{G : A \to C \text{ ring map making } (*) \text{ commute}\}$$

defined by $(\delta : A \to J) \mapsto (G_0 - \delta)$ one way and $G \mapsto (G - G_0 : A \to J)$ the other way. (Check that they are inverses of each other)

f is étale means the right hand side of the bijection is a singleton set, and hence $\mathrm{Der}_R(A, J) = 0$ for all $J \subset C$ ideal and $J^2 = 0$. But $\mathrm{Der}_R(A, J)$ is the set $\mathrm{Hom}_A(\Omega_{A/R}, J)$ (†). For any A-module M define an A-algebra $C = A \oplus M$ with multiplication $C \times C \to C$ defined by $((a, x), (b, y)) \mapsto (a, x)(b, y) = (ab, bx + ay)$, with $M \subset C$ an ideal such that $M^2 = 0$. So by (†) we have $\mathrm{Hom}_A(\Omega_{A/R}, M) = 0$, so choose $M = \Omega_{A/R}$, showing $\Omega_{A/R} = 0$.

Assume $\Omega_{A/R} = 0$, then the left hand side of the bijection is a singleton set, because $\mathrm{Der}_R(A, J) = \mathrm{Hom}_A(\underbrace{\Omega_{A/R}}_{0}, J)$.

Hence by the bijection, there exists a unique $G : A \to C$ making $(*)$ commute, so $f : R \to A$ is formally étale. □

Lemma 4.15. *Let B be an R-algebra, $J \subset B$ an ideal such that $J^2 = 0$. Then $p : B \to B/J$ has a section as R-algebras (i.e., there exists an R-algebra map $s : B/J \to B$ such that $ps = 1$) if and only if $\delta : J \to B/J \otimes_B \Omega_{B/R}$, defined by $b \mapsto 1 \otimes db$, has a retraction as B/J-modules (that is, there exists a B/J-module map $\pi : B/J \otimes_B \Omega_{B/R} \to J$, such that $\pi\delta = 1$)*

Proof. "⇒": Assume $p : B \to B/J$ has an R-algebra section $s : B/J \to B$. Consider the map $(1 - sp) : B \to B$, this has image in J since $p(1 - sp) = p - \underbrace{ps}_{1}p = 0$. Hence we have a map $\partial = (1 - sp) : B \to J$. Check that this is an R-derivation. Hence there exists a unique B-module map $\Omega_{B/R} \to J$ defined by $db \mapsto \partial b = (b - sp(b))$, since

$J(J)=0$ we obtain a B/J-module map $\pi : B/J \otimes_B \Omega_{B/R} \to J$ defined by $c \otimes db \mapsto c\partial b = c \cdot (b - sp(b))$. Check that π is a retract of $\delta : J \to B/J \otimes_R \Omega_{B/R}$ as in the lemma.

"$\Leftarrow$": Let $\pi : B/J \otimes_B \Omega_{B/R} \to J$ be a B/J-module map such that $\pi\delta = 1$. We have the universal derivation $d : B \to \Omega_{B/R}$ giving us the composition:

$$\begin{tikzcd} B \arrow[r] & B/J \otimes_B \Omega_{B/R} \arrow[r, "\pi"] & J \\ b \arrow[r, mapsto] & 1 \otimes db & \end{tikzcd}$$

Call this composition $g : B \to J$. As π is a retract of δ, we have $g(b) = b$ for all $b \in J$. Hence consider the map $(1-g) : B \to B$, this is zero on J. One checks that $(1-g) : B \to B$ is an R-algebra map. Hence we obtain an R-algebra map $B/J \to B$ defined by $b \mapsto b - g(b)$. This is an R-algebra section of $p : B \to B/J$. □

Proposition 4.16. *Let $R \to A$ be a ring map, $I \subset A$ an ideal. Let $B = A/I$. Assume $R \to A$ is formally smooth. Then the following are equivalent:*

1. *$R \to B = A/I$ is formally smooth*
2. *$A/I^2 \to A/I$ has an R-algebra section*
3. *$I/I^2 \to B \otimes_A \Omega_{A/R}$ defined by $a \mapsto 1 \otimes da$, has a retraction as B-modules.*

Proof. $1 \Rightarrow 2$ This is by definition of formal smoothness:

$$\begin{tikzcd} R \arrow[r] \arrow[d] & A/I^2 \arrow[d] \\ A/I \arrow[r, "\mathrm{id}"'] \arrow[ur, dashed, "\exists"] & A/I \end{tikzcd}$$

$2 \Rightarrow 1$ Consider a commutative diagram of rings

$$\begin{tikzcd} R \arrow[r, "h"] \arrow[d, "f"'] & C \arrow[ddd, "\overline{g}"] \\ A \arrow[d, "g_1"'] \arrow[ur, dashed, "H"] & \\ A/I^2 \arrow[d, "g_2"'] \arrow[uur, dashed, "\overline{H}"'] & \\ A/I \arrow[r, "\overline{h}"'] & C/J \end{tikzcd}$$

where $J \subset C$ is an ideal with $J^2 = 0$. Now $R \to A$ is formally smooth, so there exists $H : A \to C$ making the diagram commutes. Now $H(I) \subset J$ (since $\overline{g}H = \overline{h}g_2g_1$). Since $J^2 = 0$, we have $H(I^2) = 0$, hence there exists a unique $\overline{H} : A/I^2 \to C$ such that $\overline{H}g_1 = H$ and $\overline{h}g_2 = \overline{g}\overline{H}$. By assumption g_2 has an R-algebra section $s : A/I \to A/I^2$, hence $\overline{H}s : A/I \to C$ is an R-algebra map making the lower triangle commute. Hence we have $R \to A/I$ is formally smooth.

$2 \iff 3$ Consider the second fundamental exact sequence for $R \to A \to A/I^2$. Then we get an exact sequence of A/I^2-modules:

$$I^2/I^4 \longrightarrow A/I^2 \otimes_A \Omega_{A/R} \longrightarrow \Omega_{(A/I^2)/R} \longrightarrow 0$$

tensor this sequence with $A/I \otimes_A$ _to obtain the exact sequence, with the first map being 0:

$$A/I \otimes_A I^2/I^4 \xrightarrow{0} A/I \otimes_A \Omega_{A/R} \xrightarrow{\cong} A/I \otimes_A \Omega_{(A/I^2)/R} \longrightarrow 0$$

hence we obtain an isomorphism

$$\begin{tikzcd} A/I \otimes_A \Omega_{A/R} \arrow[r, "\cong"] & A/I \otimes_A \Omega_{(A/I^2)/R} \\ I/I^2 \arrow[u, "\alpha=1\otimes d"] \arrow[ur, "\beta=1\otimes d"'] & \end{tikzcd}$$

Then by Lemma 4.15, 2 is true if and only if β has a retraction, which happens if and only if α has a retraction.

$\square$

Remark 4.17. In view of the second fundamental exact sequence, the equivalence $1 \Leftrightarrow 3$ in Proposition 4.16 can be reformulated as follows. Assume $R \to A$ formally smooth. Then $R \to B = A/I$ is formally smooth if and only if the sequence

$$0 \to I/I^2 \to B \otimes_A \Omega_{A/R} \to \Omega_{B/R} \to 0$$

is split exact.

Definition 4.18. An R-module P is called *projective* if there exists an R-module Q and an isomorphism of R-modules $P \oplus Q \cong \oplus_I R$. (That is P is a direct summand of a free module)

Proposition 4.19. *Let $R \to A$ be a smooth map of rings. Then $\Omega_{A/R}$ is a finitely generated projective A-module.*

Proof. Case 1. $A = R[T_1, \ldots, T_n]$. Then $\Omega_{A/R} = \oplus_{i=1}^n A dT_i \cong A^n$.

Case 2. $R \to A$ smooth, means $R \to A$ has a finite presentation, so $A = R[T_1, \ldots, T_n]/I = S/I$ where $I = (f_1, \ldots, f_s)$. By the second fundamental exact sequence we have that

$$\begin{tikzcd} 0 \arrow[r] & I/I^2 \arrow[r, shift right, "\sigma"'] & A \otimes_S \Omega_{S/R} \arrow[l, shift right, dashed, "\exists \rho"'] \arrow[r, "\pi"] & \Omega_{A/R} \arrow[r] & 0 \end{tikzcd}$$

is exact and by smoothness, there exists ρ such that $\rho\sigma = 1$. Hence using Case 1 we have $A^n = A \otimes_S \Omega_{S/R} \overset{(\pi,\rho)}{\to} \Omega_{A/R} \oplus I/I^2$ is an isomorphism of A-modules.

$\square$

Definition 4.20. Let $K \subset L$ be a finite field extension. An element $x \in L$ is called *separable over K* if the minimal polynomial of x over K has no multiple roots (in an algebraic closure $\overline{K}$ of K). The field L is called *separable* over K if every $x \in L$ is separable.

A field K is called *perfect* if all its finite field extensions are separable.

Example. All finite fields, algebraically closed fields and all fields of characteristic 0 are perfect.

Criterion. *Let $K \subset L$ be a finite field extension, this is separable if and only if $L \cong K[T]/f$ with f and f' (the derivative of f) coprime in $K[T]$ (this is covered in Galois Theory)*

Proposition 4.21. *Let $K \subset L$ be a finite field extension. Then $K \subset L$ étale if and only $K \subset L$ is separable.*

Proof. "$\Leftarrow$": $K \subset L$ is separable implies, using the criterion, $L \cong K[T]/f$ with $(f, f') = K[T]$. By the second fundamental exact sequence for $K \to K[T] \to L \cong K[T]/f$ we have an exact sequence of L-vector spaces

$$(f)/(f^2) \xrightarrow{f \mapsto f'dT} \underbrace{L \otimes_{K[T]} \Omega_{K[T]/K}}_{=LdT} \longrightarrow \Omega_{L/K} \longrightarrow 0 \qquad (*)$$

Now $(f)/(f^2)$ is generated by f as L-module. So

$$\begin{tikzcd} L \arrow[r, two heads] & (f)/(f^2) \arrow[r] & LdT \\ 1 \arrow[r, mapsto] & f \arrow[r, mapsto] & f'dT \end{tikzcd}$$

is a composition which is an isomorphism because $(f', f) = K[T]$ implies $(f')L = L$, hence $f' \in L$ is a unit. So $L \to (f)/(f^2)$ is also injective and hence an isomorphism. Hence, $(f)/(f^2) \to L \otimes_{K[T]} \Omega_{K[T]/K}$ is an isomorphism and thus has a retraction, and $\Omega_{L/K} = 0$. So $K \subset L$ is smooth and $\Omega_{L/K} = 0$, meaning $K \subset L$ is étale.

"$\Rightarrow$" Assume $K \subset L$ is étale, and L is not separable over K. Then there exists $a \in L$ such that the minimal polynomial $f \in K[T]$ of a over K has multiple roots, i.e., $f = (T-a)^n g \in \overline{K}[T]$, where $\overline{K}$ is the algebraic closure of K, $n \geq 2$ and $f \in K[T]$ is irreducible. Then $K \subset K[T]/f = E \subset L$ is an extension of fields. Tensoring this by $1 \otimes_K \overline{K}$ to get $\overline{K} \subset E \otimes_K \overline{K} \subset L \otimes_K \overline{K}$. But we have $E \otimes_K \overline{K} = \overline{K}[T]/f = \overline{K}[T]/(T-a)^n g$ contains a non-zero nilpotent element, namely $T - a \in \overline{K}[T]/(T-a)^n g$ since $n \geq 2$. Hence $L \otimes_K \overline{K}$ has a non-zero nilpotent elements.

Since $K \subset L$ is étale, we have $\overline{K} \subset L \otimes_K \overline{K} = A$ is étale (Example 4.9), and A is a finite dimensional $\overline{K}$-vector space. Hence A is Artinian, so $A = \prod_{i=1}^{l} A_i$ where A_i are local finite dimensional $\overline{K}$-algebra. Since A has a non-zero nilpotent element, not all of A_i are fields, so say A_1 has maximal ideal $0 \neq m \subset A$. Recall that $\prod_{i=1}^{l} A_i \to A_1$ is étale (Example 4.13), so $\overline{K} \to A_1$ is étale as a composition of étale maps. We have

$$\begin{tikzcd} \overline{K} \arrow[r, "\text{étale}"] \arrow[rr, bend right, "\text{id=étale}"'] & A_1 \arrow[r] & A_1/m = \overline{K} \end{tikzcd}$$

(we have $A_1/m = \overline{K}$ since A_1/m is a finite field extension of $\overline{K}$ which is algebraically closed), so by the second fundamental exact sequence we have

$$0 \longrightarrow m/m^2 \rightleftarrows \overline{K} \otimes_{A_1} \underbrace{\Omega_{A_1/R}}_{0\,(\overline{K} \to A_1 \text{ étale})} \longrightarrow \underbrace{\Omega_{\overline{K}/\overline{K}}}_{0\,(\overline{K} \subset \overline{K} \text{ étale})} \longrightarrow 0$$

is split exact. So $m/m^2 = 0$ and by Nakayama, this means $m = 0$, which is a contradiction. So A_1 has no non-zero nilpotent element. $\square$

4.3 Smoothness and Regularity

Definition 4.22. A Noetherian local ring (R, m, k) is called *regular* if $\dim_k m/m^2 = \dim R$

Lemma 4.23. *Let k be a field. Then for all $m \subset S = k[T_1, \dots, T_n]$ maximal ideals, S_m is a regular local ring.*

Proof. Case 1. $k \subset S/m = S_m/m$ is separable (it is a finite field extension by Hilbert's Nullstellensatz). In particular $k \subset S/m = L$ is étale. So

$$\begin{tikzcd} K \arrow[r, "\text{smooth}"] \arrow[rr, bend right, "\text{étale}"'] & S \arrow[r] & S/m = L \end{tikzcd}$$

so by the second fundamental sequence, we have the split exact sequence

$$0 \longrightarrow m/m^2 \longrightarrow \underbrace{L \otimes_S \Omega_{S/K}}_{\oplus_{i=1}^{n} L dT_i = L^n} \longrightarrow \underbrace{\Omega_{L/K}}_{0\,(K \subset L \text{ étale})} \longrightarrow 0$$

Hence $m/m^2 \cong L^n$ as L-modules, so $\dim_L m/m^2 = n = \dim S_m$, hence S_m is regular.

Case 2. $k \subset S/m = L$ is arbitrary. We use the

Black box Theorem 1. *Let $A \to B$ be a faithful flat map of local rings. If B is regular then so is A.*

Remark 4.24. The theorem follows from Serre's theorem (proved in MA 4H8 "Ring Theory") that a local noetherian ring is regular if and only if it has finite projective dimension; see Assignment sheet IV.

To finish the proof of Lemma 4.23, let $\overline{S} = \overline{k}[T_1, \dots, T_n]$, then $S \subset \overline{S}$ is an integral extension. Choose $\overline{m} \subset \overline{S}$ a maximal ideal such that $m = S \cap \overline{m}$. Then $S \to \overline{S}$ is faithfully flat ($K \to \overline{K}$ is), so $S_m \to \overline{S}_{\overline{m}}$ is (faithfully) flat. By case 1 we have $\overline{S}_{\overline{m}}$ is regular and hence S_m is regular.

$\square$

Lemma 4.25. *Let (R, m, k) be a Noetherian local ring, and $x_1, ..., x_s \in m$. Then $\dim R \leq s + \dim R/(x_1, ..., x_s)$.*

Proof. Let $y_1, ..., y_d \in R$ be a system of parameters for $R/(x_1, ..., x_s)$. So, $d = \dim R/(x_1, ..., x_s)$ and $R/(x_1, ..., x_s, y_1, ..., y_d)$ is Artinian. Then $(x_1, ..., x_s, y_1, ..., y_d) \subset R$ is an m-primary ideal. By the Dimension Theorem, we have $\dim R \leq s + d$. $\square$

Lemma 4.26. *Let (R, m, k) be a regular local ring of dimension $\dim R = n$. If $x_1, \dots, x_s \in m$ are linearly independent in the k-vector space m/m^2 (so $s \leq n$), then $S = R/(x_1, \dots, x_s)$ is regular of dimension $n - s$*

Proof. Let $m_s \subset S$ be the maximal ideal, $m_s = m/(x_1, \dots, x_s)$. We have an exact sequence of k-vector space:

$$(x_1, \dots, x_s)m/m^2 \longrightarrow m/m^2 \longrightarrow m_s/m_s^2 \longrightarrow 0$$

Now the first map is injective since $x_1, \dots, x_s$ are linearly independent in m/m^2. Hence $\dim_k m_s/m_s^2 = \dim_k m/m^2 - \dim_k(x_1, \dots, x_s)m/m^2 = n-s$. From the Dimension Theorem, we have $\dim S \leq \dim_k m_s/m_s^2 = n-s$. From Lemma 4.25 we have $\dim S \geq \dim R - s = n-s$, hence $\dim S = n-s = \dim_k m_s/m_s^2$ and S is regular of dimension $n-s$. □

Definition 4.27. Let $f : R \to A$ be a ring map such that A is finitely presented over R. Let $m \subset A$ be a maximal ideal. Then we call f *smooth at* m if $R \to A_m$ is formally smooth.

Remark. Write $A = R[T_1, \dots, T_s]/I$ with $I = (f_1, \dots, f_n)$, $m \subset A$ maximal ideal. Write $S = R[T_1, \dots, T_s]$, so $A = S/I$. Let $m_s =$ maximal ideal $\subset S$ such that $m_s/I = m$. Now $R \to S$ is smooth, $S \to S_{m_s}$ is formally étale, hence $R \to S$ is smooth at m_s. Then $R \to A$ is smooth at m if and only if the second fundamental sequence for $R \to S_{m_s} \to A_m$:

$$0 \longrightarrow (I/I^2)_m \longrightarrow A_m \otimes_S \Omega_{S/R} \longrightarrow (\Omega_{A/R})_m \longrightarrow 0$$

is split exact. (Note $\Omega_{A/R} = (\Omega_{A_m/R})_m$, by Lemma 4.6)

Remark. If $R \to A$ has finite presentation, then $R \to A$ is smooth if and only if $R \to A$ is smooth at all $m \subset A$ maximal ideal.

Proof. "$\Rightarrow$" $A \to A_m$ is formally étale (Example 4.11).

"$\Leftarrow$" Write $A = S/I$, $S = R[T_1, \dots, T_s]$, $I = (f_1, \dots, f_n)$. Then for all maximal ideals $m \subset A$, the second fundamental sequence

$$0 \longrightarrow (I/I^2)_m \longrightarrow (A \otimes_R \Omega_{S/R})_m \longrightarrow (\Omega_{A/R})_m \longrightarrow 0$$

is split exact. Hence, the sequence

$$0 \longrightarrow I/I^2 \longrightarrow A \otimes_R \Omega_{S/R} \longrightarrow \Omega_{A/R} \longrightarrow 0 \qquad (*)$$

is exact. Moreover, from the split exact sequence above, $(\Omega_{A/R})_m$ is projective as it is a direct summand of $(A \otimes_R \Omega_{S/R})_m = A_m^s$ which is free. Since $\Omega_{A/R} = \operatorname{coker}(J(f) : A^n \to A^s)$ is a finitely presented A-module (as A is a finitely presented R-algebra) and projective (actually free as A_m local) at m for all $m \subset A$ maximal ideals, the A-module $\Omega_{A/R}$ is projective. In particular, the exact sequence $(*)$ is split exact as any surjection onto a projective module splits. So $R \to A$ is smooth. □

Proposition 4.28. *Let (R, m, k) be a regular local ring. Then R is a domain.*

Sketch of proof. If (R, m, k) is Noetherian local, then R is regular if and only if $\operatorname{gr}_m R \cong k[x_1, \dots, x_s]$.

Let (R, m, k) be Noetherian local. If $\operatorname{gr}_m R$ is a domain, then R is a domain. □

Theorem 4.29. *Let k be a field, A a finitely generated k-algebra. Let $m \subset A$ be a maximal ideal. Let $L = A/m$. Assume that $k \to L$ is separable. Then $k \to A$ is smooth at m, if and only if, A_m is regular. In this case, $(\Omega_{A/k})_m$ is a free A_m-module of rank equal to* $\dim A_m$.

Proof. Write $A = S/I$ where $S = k[T_1, \dots, T_s]$ and let $m_s \subset S$ be the maximal ideal such that $m = m_s/I$.

"$\Rightarrow$" $k \to A$ smooth at m implies

$$0 \longrightarrow (I/I^2)_m \longrightarrow A_m \otimes_S \Omega_{S/k} \longrightarrow (\Omega_{A/k})_m \longrightarrow 0$$

is split exact. So applying $- \otimes_A L$ to this exact sequence we get

$$0 \longrightarrow I/I^2 \otimes_A L \longrightarrow \underbrace{L \otimes_S \Omega_{S/k}}_{=L^s} \longrightarrow \Omega_{A/k} \otimes_A L \longrightarrow 0 \qquad (*)$$

is split exact. Now $k \to L$ is separable and hence étale, so by the second fundamental sequence applied to

$$\begin{tikzcd} k \arrow[r, "\text{smooth}"] \arrow[rr, bend right, "\text{étale}"'] & A_m \arrow[r] & L \end{tikzcd}$$

we get a split exact sequence

$$0 \longrightarrow m/m^2 \xrightarrow{\cong} L \otimes_A \Omega_{A/k} \longrightarrow \underbrace{\Omega_{L/k}}_{0\,(k\to L\text{ étale})} \longrightarrow 0 \qquad (\dagger)$$

Hence $m/m^2 \cong L \otimes_A \Omega_{A/k}$ as L-vector spaces. Let $n = \dim_L m/m^2$. By the Dimension Theorem $\dim A_m \leq n$. Now $(*)$ and $(\dagger)$ imply $\dim_L \underbrace{I/I^2 \otimes_A L}_{I_m/I_m^2 \otimes_{A_m} L} = s - n$. So by Nakayama, I_m is generated as A_m-module by $s - n$ elements. Lemma 4.25 implies $\dim A_m = \dim S_{m_S}/I_m \geq \dim S_m - (s-n) = n$. With the inequality $\dim A_m \leq n$ above, this implies $\dim A_m = n = \dim_L m/m^2$, and A_m is regular.

"$\Leftarrow$" Assume A_m is regular. Let $n = \dim A_m$, then $\dim_L m/m^2 = n$. We have

$$0 \longrightarrow I/(I \cap m_s^2) \longrightarrow m_s/m_s^2 \longrightarrow m/m^2 \longrightarrow 0$$

is an exact sequence of L-vector spaces. Hence there exists $f_1, \ldots, f_{s-n} \in I$ which form basis for the L-vector space $I/(I \cap m_S^2)$. So $f_1, \ldots, f_{s-n}$ are linearly independent in m_s/m_s^2. Let $J = (f_1, \ldots, f_{s-n})$ then S_{m_s}/J is a regular ring of dimension $s - (s-n) = n$ (since S_{m_s} is regular of dimension s). Furthermore $\phi : S_{m_s}/J \twoheadrightarrow A_m$ is a surjection of regular rings (hence of domains). Since the two domains have the same dimension, namely n, and ϕ is surjective, we have ϕ is an isomorphism (Otherwise $\ker \phi \neq 0$ and S_m/J has a prime ideal, namely 0 which doesn't correspond to a prime ideal in A_m. In particular any chain of primes in A_m gives - by taking preimages- a chain of primes in S_m/J of the same length that can be made longer by adding the 0 prime ideal). Hence $I_m = J = (f_1, \ldots, f_{s-n})$. By the second fundamental exact sequence for $K \to S_{m_s} \to A_m$ we have the exact sequence.

$$\begin{tikzcd}
(I/I^2)_m \arrow[r] & \underbrace{(A \otimes_S \Omega_{S/k})_m}_{A_m^s} \arrow[r] & (\Omega_{A/k})_m \arrow[r] & 0 \\
A_m^{s-n} \arrow[u, "e_i \mapsto f_i"] \arrow[ur, "J(f)"'] & & &
\end{tikzcd}$$

where $J(f)$ is the Jacobian matrix of $(f_1, \ldots, f_{s-n})$. Applying $- \otimes_{A_m} L$ gives the exact sequence

$$L^{s-n} \xrightarrow{J(f)\otimes L} L^s \longrightarrow L \otimes_A \Omega_{A/k} \longrightarrow 0 \qquad (**)$$

Using the second fundamental sequence for

$$\begin{tikzcd}
k \arrow[r] \arrow[rr, bend right, "\text{étale}"'] & A_m \arrow[r] & L
\end{tikzcd}$$

gives the exact sequence

$$m/m^2 \longrightarrow (\Omega_{A/k}) \otimes_A L \longrightarrow \underbrace{\Omega_{L/k}}_{0\,(k\to L\text{ étale})} \longrightarrow 0$$

We have $n = \dim_L m/m^2 \geq \dim_L \Omega_{A/k} \otimes L \geq_{\text{by }(**)} s - (s-n) \geq n$, hence $\dim_L \Omega_{A/k} \otimes L = n$. So the first map in (**) is injective, and thus, the map $J(f) \otimes L$ has a $s - n \times s - n$ invertible submatrix. It follows that $J(f) : A_m^{s-n} \to A_m^s$ has a $s - n \times s - n$ invertible submatrix (For a local ring (R, m, k), a matrix $M \in M_n(R)$ is invertible if and only if $M \mod m \in M_n(k)$ is invertible. This is because invertibility is equivalent to $\det M$ being a unit, and $r \in R$ is a unit iff $r \mod m$ is a unit in k). So $J(f)$ is injective and has a retraction. Hence $A_m^{s-n} \overset{\cong}{\twoheadrightarrow} (I/I^2)_m$ is an isomorphism and the second fundamental exact sequence for $K \to S_{m_s} \to A_m$ is split exact. Hence $k \to A$ is smooth at m.

$\square$

Corollary 4.30. *Let k be a perfect field and A a finitely generated k-algebra. Let $m \subset A$ be a maximal ideal. Then $k \to A$ is smooth at m if and only if A_m is regular. In particular, $k \to A$ is smooth if and only if A_m is regular for every maximal ideal $m \subset A$.*

Theorem 4.31. *Let k be a field, A a finitely generated k algebra, $m \subset A$ a maximal ideal and $L = A/m$. Then $k \to A$ is smooth at m, if and only if, A_m is regular and $\dim_L \Omega_{A/k} \otimes_A L = \dim A_m$*

Proof. The proof was not given in the lectures. But since it is short, it is included here for completeness' sake.

$\Rightarrow$ Let $\bar{k}$ be an algebraic closure of k. By Example 4.9, since $k \to A$ is smooth at $m \subset A$, the map $\bar{k} \to \overline{A} = A \otimes_k \bar{k}$ is smooth at every maximal ideal $\overline{m} \subset \overline{A}$ of $\overline{A}$ with $m = A \cap \overline{m}$ (such maximal ideals $\overline{m}$ exist since $A \subset \overline{A}$ is an integral extension). By Theorem 4.29, $\overline{A}_{\overline{m}}$ is regular, and $\Omega_{\overline{A}_{\overline{m}}/\bar{k}}$ is a free $\overline{A}_{\overline{m}}$-module of rank equal $\dim \overline{A}_{\overline{m}}$. Since $A \to \overline{A}$ is flat (as $k \to \bar{k}$ is), the local map of rings $A_m \to \overline{A}_{\overline{m}}$ is faithfully flat. Black Box Theorem 1 therefore implies that A_m is also regular, and Theorem 3.32 implies that $\dim A_m = \dim \overline{A}_{\overline{m}}$. Let $\overline{L} = \overline{A}/\overline{m}$. This is a field extension of $L = A/m$. From Lemmas 4.6 and 4.7 we have $\Omega_{\overline{A}/\bar{k}} \cong \Omega_{A/k} \otimes_A \overline{A}$ and thus, $\Omega_{\overline{A}_{\overline{m}}/\bar{k}} \otimes_{\overline{A}} \overline{L} \cong \Omega_{\overline{A}/\bar{k}} \otimes_{\overline{A}} \overline{L} \cong \Omega_{A/k} \otimes_A \overline{L} \cong (\Omega_{A_m/k} \otimes_A L) \otimes_L \overline{L}$. Therefore, using Theorem 4.29 again, we have $\dim A_m = \dim \overline{A}_{\overline{m}} = \dim_{\overline{L}} \Omega_{\overline{A}_{\overline{m}}/\bar{k}} \otimes_{\overline{A}} \overline{L} = \dim_L \Omega_{A_m/k} \otimes_A L$.

$\Leftarrow$ The proof of this implication is the same as the implication "$\Leftarrow$" of Theorem 4.29 using the additional hypothesis $\dim A_m = \dim_L \Omega_{A_m/k} \otimes_A L$.

$\square$

Theorem 4.32 (MA4H8)**.** *If (A, m, k) is regular, then for all prime ideal $p \subset A$ we have A_p is regular.*