Yanqi Lake Lectures on Algebra

/ Wen-Wei Li

$$\supset \operatorname{Spec}(B_{\mathfrak{q}'}) \xrightarrow{\varphi^{\sharp}_{\mathfrak{p}'}} \supset \operatorname{Spec}(A_{\mathfrak{p}'})$$

Part 3

Commutative rings
Completions
Dimension theory

中国科学院大学
University of Chinese Academy of Sciences

Yanqi Lake Lectures on Algebra

Part 3

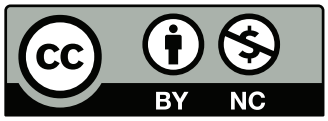
Wen-Wei Li
Chinese Academy of Sciences

中国科学院大学
University of Chinese Academy of Sciences

Version: 2019-06-14

The cover page uses the fonts *Bebas Neue* and *League Gothique*, both licensed under the SIL Open Font License.

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/.



Contents

Introduction 1

1 Warming up 3
- 1.1 Review on ring theory . . . 3
- 1.2 Localization of rings and modules . . . 5
- 1.3 Radicals and Nakayama's lemma . . . 9
- 1.4 Noetherian and Artinian rings . . . 11
- 1.5 What is commutative algebra? . . . 12

2 Primary decompositions 15
- 2.1 The support of a module . . . 15
- 2.2 Associated primes . . . 16
- 2.3 Primary and coprimary modules . . . 18
- 2.4 Primary decomposition: the main theorem . . . 19
- 2.5 Examples and remarks . . . 21

3 Integral dependence, Nullstellensatz and flatness 25
- 3.1 Integral extensions . . . 25
- 3.2 Nullstellensatz . . . 28
- 3.3 Flatness: the first glance . . . 30
- 3.4 Structure of flat modules . . . 33
- 3.5 Faithful flatness and surjectivity . . . 36

4 Going-up, going-down, gradings and filtrations 39
- 4.1 Going-up and going-down . . . 39
- 4.2 Subsets in the spectrum . . . 42
- 4.3 Graded rings and modules . . . 45
- 4.4 Filtrations . . . 46
- 4.5 Theorems of Artin–Rees and Krull . . . 48

5 From completions to dimensions 51
- 5.1 Completions . . . 51
- 5.2 Further properties of completion . . . 55
- 5.3 Hilbert–Samuel polynomials . . . 56
- 5.4 Definition of Krull dimension . . . 58
- 5.5 Krull's theorems and regularity . . . 63

6 Dimension of finitely generated algebras **65**
6.1 Dimensions in fibers 65
6.2 Calculation for polynomial algebras 67
6.3 Noether normalization and its consequences 68

7 Serre's criterion for normality and depth **73**
7.1 Review of discrete valuation rings 73
7.2 Auxiliary results on the total fraction ring 74
7.3 On normality 76
7.4 Serre's criterion 77
7.5 Introduction to depth 78

8 Some aspects of Koszul complexes **83**
8.1 Preparations in homological algebra 83
8.2 Auxiliary results on depth 85
8.3 Koszul complexes and depth 86

Bibliography **91**

Index **93**

Introduction

In the beginning, these lecture notes were prepared for the graduate course *Algebra III* (ID: 011M4002Y) in Spring 2016, University of the Chinese Academy of Sciences. For some reasons, it took place in the Yuquanlu campus instead of the Yanqi Lake campus as it should be.

The course is a sequel to Algebra I (fields, modules and representations) and II (homological algebra). The topic of this Part III is commutative algebra, or more precisely *commutative ring theory*. Each "Lecture" in these notes took roughly one week, say approximately four hours of lecture, but the materials were only partially covered. My initial intention was to give a traditional course on commutative algebra as proposed by the syllabus prescribed by UCAS. For various reasons, my plan failed. For example, there are too few discussions on depth, regular sequences and Cohen–Macaulay modules, too few applications of completions, and the computational aspects haven't been touched. Moreover, the homological aspect of commutative algebra is almost nonexistent in these notes, namely the Auslander–Buchsbaum Formula, the properties of regular local rings, etc. Last but not least, the exercises herein are scarcely sufficient.

These notes were also used for the Enhanced Program for Graduate Study held at the Beijing International Center of Mathematical Research, Peking University, during Spring 2019 (course ID: 00102057).

As the title suggests, some backgrounds from the Part I are presumed, namely the basic notions of rings, modules and their chain conditions, as well as familiarity with tensor products and some Galois theory. We occasionally presume some basic knowledge of homological algebra, such as the functors Tor_i and Ext^i.

Sometimes I made free use of the language of derived categories. This was indeed covered in the preceding course *Algebra II*, and it should be common sense for the future generations.

As the reader might have observed, these notes were prepared in a rush; certain paragraphs have not been proofread yet and many proofs are silly. I am very grateful to the students for various corrections and improvements, and I will try to polish these notes in the future.

Conventions

Throughout these lectures, we consider only associative rings with unit 1, and the rings and algebras are assumed to be commutative and nonzero unless otherwise specified. The ideal generated by elements $x_1, x_2, \ldots$ in a ring R is denoted by $(x_1, x_2, \ldots)$ or sometimes $\langle x_1, x_2, \ldots \rangle$; the R-algebra of polynomials in variables $X, Y, \ldots$ with coefficients in

R is denoted by $R[X, Y, \ldots]$. We write $R^\times$ for the group of invertible elements in a ring R. A ring without zero-divisors except 0 is called an integral domain, or simply a domain. The localization of a ring R with respect to a multiplicative subset S will be written as $R[S^{-1}]$.

For any sets E, F, let $E \setminus F := \{x \in E : x \notin F\}$. The cardinality of E is denoted by $|E|$.

The usual logical connectives such as $\exists$, $\forall$, $\wedge$, $\vee$ and so forth will occasionally be used. Writing $A := B$ means that the expression A is defined to be B.

We will use the standard notations $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ to denote the set of integers, of rational numbers, etc. Sans serif fonts are reserved for categories, such as Ab (abelian groups) and Ring.

When denoting morphisms in a category by arrows, monomorphisms (resp. epimorphisms, isomorphisms) will be indicated $\hookrightarrow$ (resp. $\twoheadrightarrow$, $\xrightarrow{\sim}$).

Possible references

The reader is expected to have basic familiarity with groups, rings and modules, as covered in my lecture notes on Algebra I. We will make use of some really elementary homological algebra as our course proceeds — so keep calm.

Our main references will be [11] and [8]. The Bourbaki volumes [5, 3] serve as our ultimate source. The readers are also encouraged to consult the relevant materials in Stacks Project.

《教授生涯》, 李桦, 木刻版画, 1948 年.

Lecture 1

Warming up

The reader might be familiar with most of the materials in this lecture. Our goal is to fix notation and present the basic structural results on Noetherian and Artinian rings or modules, including the celebrated Nakayama's Lemma which will be used repeatedly.

1.1 Review on ring theory

Let R be a ring, supposed to be commutative with unit $1 \neq 0$ as customary. Recall that an ideal $I \subsetneq R$ is called

- *prime*, if $ab \in I \iff (a \in I) \vee (b \in I)$;
- *maximal*, if I is maximal among the proper ideals of R with respect to inclusion.

Recall the following standard facts

- I is prime if and only if R/I is an integral domain, i.e. has no zero divisors except 0;
- I is maximal if and only if R/I is a field; in particular, maximal ideals are prime;
- every proper ideal I is contained in a maximal ideal (an application of Zorn's Lemma).

Definition 1.1.1 (Local rings)**.** The ring R is called *local* if it has a unique maximal ideal, *semi-local* if it has only finitely many maximal ideals.

Let $\mathfrak{m}$ be the maximal ideal of a local ring R. We call $R/\mathfrak{m}$ the *residue field* of R. A local homomorphism between local rings $\varphi : R_1 \to R_2$ is a ring homomorphism such that $\varphi(\mathfrak{m}_1) \subset \mathfrak{m}_2$. Consequently, local homomorphisms induce embeddings on the level of residue fields.

Sometimes we denote a local ring by the pair $(R, \mathfrak{m})$.

Remark 1.1.2. Let R be a local ring with maximal ideal $\mathfrak{m}$, then $R^\times = R \setminus \mathfrak{m}$. The is easily seen as follows. An element $x \in R$ is invertible if and only if $Rx = R$. Note that $Rx = R$ is equivalent to that x is not contained in any maximal ideal, and the only maximal ideal is $\mathfrak{m}$.

Throughout these lectures, we shall write

$$\begin{aligned}\mathrm{Spec}(R) &:= \{\text{prime ideals of } R\},\\ \mathrm{MaxSpec}(R) &:= \{\text{maximal ideals of } R\}.\end{aligned}$$

They are called the *spectrum* and the *maximal spectrum* of R, respectively. The upshot is that $\mathrm{Spec}(R)$ comes with a natural topology.

Definition 1.1.3 (Zariski topology)**.** For any ideal $\mathfrak{a} \subset R$, set $V(\mathfrak{a}) := \{\mathfrak{p} \in \mathrm{Spec}(R) : \mathfrak{p} \supset \mathfrak{a}\}$. Then there is a topology on $\mathrm{Spec}(R)$, called the *Zariski topology*, whose closed subset are precisely $V(\mathfrak{a})$, for various ideals $\mathfrak{a}$.

Indeed, we only have to prove the family of subsets $\{V(\mathfrak{a}) : \mathfrak{a} \subset R\}$ is closed under finite union and arbitrary intersections. It boils down to the easy observation that $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{ab})$ (check this!) and $\bigcap_{\mathfrak{a}\in\mathcal{A}} V(\mathfrak{a}) = V\left(\sum_{\mathfrak{a}\in\mathcal{A}} \mathfrak{a}\right)$, where $\mathcal{A}$ is any family of ideals.

Given a ring homomorphism $\varphi : R_1 \to R_2$, if $I \subset R_2$ is an ideal, then $\varphi^{-1}(I) \subset R_1$ is also an ideal.

Proposition 1.1.4. *Given φ as above, it induces a continuous map*

$$\begin{aligned}\varphi^\sharp : \mathrm{Spec}(R_2) &\longrightarrow \mathrm{Spec}(R_1)\\ \mathfrak{p} &\longmapsto \varphi^{-1}(\mathfrak{p})\end{aligned}$$

with respect to the Zariski topologies on spectra.

Proof. Clearly, $ab \in \varphi^{-1}(\mathfrak{p})$ is equivalent to $\varphi(a)\varphi(b) \in \mathfrak{p}$, which is in turn equivalent to $(\varphi(a) \in \mathfrak{p}) \vee (\varphi(b) \in \mathfrak{p})$ when $\mathfrak{p}$ is prime.

To show the continuity of $\varphi^\sharp$, observe that for any ideal $\mathfrak{a} \subset R_1$ and $\mathfrak{p} \in \mathrm{Spec}(R_2)$, we have $\varphi^{-1}(\mathfrak{p}) \supset \mathfrak{a}$ if and only if $\mathfrak{p} \supset \varphi(\mathfrak{a})$, i.e. $\mathfrak{p} \in V(\varphi(\mathfrak{a})R_2)$. Hence the preimage of closed subsets are still closed. □

More operations on spectra:

- Take R_1 to be a subring of R_2 and φ be the inclusion map, the map above becomes $\mathfrak{p} \mapsto \mathfrak{p} \cap R_1$.
- Take $\varphi : R \twoheadrightarrow R/I$ to be a quotient homomorphism, then φ^{-1} is the usual bijection from $\mathrm{Spec}(R/I)$ onto $V(I)$.
- In general, φ^{-1} does not induce $\mathrm{MaxSpec}(R_2) \to \mathrm{MaxSpec}(R_1)$, as illustrated in the case $\varphi : \mathbb{Z} \hookrightarrow \mathbb{Q}$.

At this stage, we can prove a handy result concerning prime ideals.

Proposition 1.1.5 (Prime avoidance)**.** *Let I and $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be ideals of R such that $I \subset \bigcup_{i=1}^n \mathfrak{p}_i$. Suppose that*

- *either R contains an infinite field, or*
- *at most two of the ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are non-prime,*

then there exists $1 \le i \le n$ such that $I \subset \mathfrak{p}_i$.

Proof. If R contains an infinite field F, the ideals are automatically F-vector subspaces of R. Since $I = \bigcup_{i=1}^{r} I \cap \mathfrak{p}_i$ whereas an F-vector space cannot be covered by finitely many proper subspaces, there must exist some i with $I \cap \mathfrak{p}_i = I$.

Under the second assumption, let us argue by induction on n that $\forall i\ I \not\subset \mathfrak{p}_i$ implies $I \not\subset \bigcup_{i=1}^{n} \mathfrak{p}_i$. The case $n = 1$ is trivial. When $n \geq 2$, by induction we may choose, for each i, an element $x_i \in I \setminus \bigcup_{j\neq i} \mathfrak{p}_j$. Suppose on the contrary that $I \subset \bigcup_{j=1}^{n} \mathfrak{p}_j$, then we would have $x_i \in \mathfrak{p}_i$, for all $i = 1, \dots, n$.

When $n = 2$ we have $x_1 + x_2 \notin \mathfrak{p}_1 \cup \mathfrak{p}_2$ and $x_1 + x_2 \in I$, a contradiction. When $n > 2$, we may assume $\mathfrak{p}_1$ is prime, therefore

$$x_1 + \prod_{j=2}^{n} x_j \notin \bigcup_{i=1}^{n} \mathfrak{p}_i,$$

again a contradiction. □

Exercise 1.1.6. The following construction from [8, Exercise 3.17] shows that the assumptions of Proposition 1.1.5 cannot be weakened. Take $R = (\mathbb{Z}/2\mathbb{Z})[X, Y]/(X, Y)^2$, which has a basis $\{1, X, Y\}$ (modulo $(X, Y)^2$) as a $\mathbb{Z}/2\mathbb{Z}$-vector space. Show that the image $\mathfrak{m}$ of (X, Y) in R is the unique prime ideal, and can be expressed as a union of three ideals properly contained in $\mathfrak{m}$.

1.2 Localization of rings and modules

Let S be a *multiplicative subset* of R, which means that (a) $1 \in S$, (b) S is closed under multiplication, and (c) $0 \notin S$. The *localization* of R with respect to S is the ring $R[S^{-1}]$ formed by classes $[r, s]$ with $r \in R$, $s \in S$, modulo the equivalence relation

$$[r, s] = [r', s'] \iff \exists t \in S,\ (rs' - r's)t = 0.$$

You should regard $[r, s]$ as a token for r/s; the ring structure of $R[S^{-1}]$ is therefore evident. In brief, localization amounts to formally inverting the elements of S, whence the notation $R[S^{-1}]$. Note that condition (c) guarantees $R[S^{-1}] \neq \{0\}$.

Exercise 1.2.1. Given R and S, show that $r \mapsto r/1$ yields a natural homomorphism $R \to R[S^{-1}]$ and show that its kernel equals $\{r : \exists s \in S,\ sr = 0\}$.

The universal property of $R \to R[S^{-1}]$ can be stated using commutative diagrams as follows.

$$\forall \begin{cases} \varphi : R \to R' : \text{ ring homomorphism} \\ \text{s.t. } \varphi(S) \subset (R')^{\times} \end{cases}, \qquad \begin{array}{ccc} R & \longrightarrow & R[S^{-1}] \\ & \searrow^{\varphi} & \downarrow \exists! \\ & & R' \end{array}$$

Consequently, if $S \subset R^\times$ then $R \simeq R[S^{-1}]$ canonically. Furthermore, the homomorphism $R \to R[S^{-1}]$ induces a bijection

$$\begin{array}{ccc} \mathrm{Spec}(R[S^{-1}]) & \xleftrightarrow{1:1} & \{\mathfrak{p} \in \mathrm{Spec}(R) : \mathfrak{p} \cap S = \emptyset\} \subset \mathrm{Spec}(R) \\ \mathfrak{p}R[S^{-1}] = \{r/s : r \in \mathfrak{p},\ s \in S\} & \longleftarrow\!\shortmid & \mathfrak{p} \\ \mathfrak{q} & \longmapsto & \text{its preimage.} \end{array} \tag{1–1}$$

Exercise 1.2.2. Check the properties above.

Let us review some important instances of the localization procedure.

1. Take S to be the subset of non zero-divisors of R. This is easily seen to be a multiplicative subset (check it!) and $K(R) := R[S^{-1}]$ is called the *total fraction ring* of R. The reader is invited to check that $R \to K(R)$ is the "biggest localization" such that the natural homomorphism $R \to R[S^{-1}]$ is injective. Hint: state this in terms of universal properties.

   When R is an integral domain, we shall take $S := R \setminus \{0\}$; in this case the total fraction ring $\mathrm{Frac}(R) := K(R)$ is the well-known *field of fractions* of R.

2. Take any $\mathfrak{p} \in \mathrm{Spec}(R)$ and $S := R \setminus \mathfrak{p}$. From the definition of prime ideals, one infers that S is a multiplicative subset of R. The corresponding localization is denoted by $R \to R_\mathfrak{p} := R[S^{-1}]$. We see from (1–1) that

   $$\mathrm{MaxSpec}(R_\mathfrak{p}) = \{\mathfrak{p}R_\mathfrak{p}\};$$

   in particular, $R_\mathfrak{p}$ is a local ring with maximal ideal $\mathfrak{p}R_\mathfrak{p}$. This is the standard way to produce local rings; we say that $R_\mathfrak{p}$ is the localization of R at the prime $\mathfrak{p}$.

3. Suppose $f \in R$ is not nilpotent, that is, $f^n \neq 0$ for every n. Take $S := \{f^n : n \geq 0\}$. The corresponding localization is denoted by the self-explanatory notation $R \to R[f^{-1}]$.

Exercise 1.2.3. Describe the following localizations explicitly.

(a) $R = \mathbb{Z}$, and we localize at the prime ideal (p) where p is a prime number.

(b) $R = \mathbb{C}[X_1, \dots, X_n]$ and we localize at the maximal ideal generated by $X_1, \dots, X_n$.

(c) $R = \mathbb{C}[\![X]\!]$ (the ring of formal power series) and $S := \{X^n : n \geq 0\}$.

Exercise 1.2.4. Prove that $R[X]/(fX - 1) \xrightarrow{\sim} R[f^{-1}]$ by mapping $X \mapsto f^{-1}$. Hint: use the universal property.

Always let $S \subset R$ be a multiplicative subset. The localization $M[S^{-1}]$ of an R-module M can be defined in the manner above, namely as the set of equivalence classes $[m, s]$ with $m \in M$ and $s \in S$, such that

$$[m, s] = [m', s'] \iff \exists t \in S,\ t(s'm - sm') = 0.$$

As in the case of rings, we shall write m/s instead of $[m,s]$. It is an $R[S^{-1}]$-module, equipped with a natural homomorphism $M \to M[S^{-1}]$ of R-modules. This yields a functor: for any homomorphism $f : M \to N$ we have a natural $f[S^{-1}] : M[S^{-1}] \to N[S^{-1}]$, mapping m/s to $f(m)/s$; furthermore $f[S^{-1}] \circ g[S^{-1}] = (f \circ g)[S^{-1}]$ whenever composition makes sense.

A slicker interpretation is to use the natural isomorphism $M[S^{-1}] \xrightarrow{\sim} R[S^{-1}] \underset{R}{\otimes} M$ which maps m/s to $(1/s) \otimes m$. Hereafter, we shall identify $M[S^{-1}]$ and $R[S^{-1}] \underset{R}{\otimes} M$ without further comments.

In the same vein, we may define $M[f^{-1}]$ and $M_{\mathfrak{p}}$, for non-nilpotent $f \in R$ and $\mathfrak{p} \in \operatorname{Spec}(R)$ respectively. Localization "commutes" with several standard operation on modules, which we sketch below. The details are left to the reader.

- ◇ For R-modules M, N, we have a natural isomorphism of $R[S^{-1}]$-modules

$$(M \underset{R}{\otimes} N)[S^{-1}] \simeq M[S^{-1}] \underset{R[S^{-1}]}{\otimes} N[S^{-1}],$$
$$(M \oplus N)[S^{-1}] \simeq M[S^{-1}] \oplus N[S^{-1}].$$

  Same for arbitrary direct sums. This is easily seen by viewing $M[S^{-1}]$ as $M \otimes_R R[S^{-1}]$.

- ◇ Note that $\operatorname{Hom}_R(M,N)$ is also an R-module: simply set $(rf)(m) = r \cdot f(m)$ for any $f \in \operatorname{Hom}_R(M,N)$. There is a natural homomorphism

$$\operatorname{Hom}_R(M,N)[S^{-1}] \to \operatorname{Hom}_{R[S^{-1}]}\left(M[S^{-1}], N[S^{-1}]\right) \tag{1–2}$$

  sending $s^{-1} \otimes \varphi$ to $s^{-1}\varphi : m/t \mapsto \varphi(m)/st$. It is clearly an isomorphism for $M = R$, thus also for $M = R^a$ where $a \in \mathbb{Z}_{\geq 0}$, but this is not the case in general, as there is no uniform bound for the "denominators" for any given $\psi : M[S^{-1}] \to N[S^{-1}]$ — some finiteness condition is needed. Let us assume M to be *finitely presented*, i.e. there is an exact sequence

$$R^a \to R^b \to M \to 0, \quad a, b \in \mathbb{Z}_{\geq 0}.$$

  In this case (1–2) is an isomorphism, as easily seen from the commutative diagram with exact rows:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \operatorname{Hom}(M,N)[S^{-1}] & \longrightarrow & \operatorname{Hom}(R^b,N)[S^{-1}] & \longrightarrow & \operatorname{Hom}(R^a,N)[S^{-1}] \\
 & & \downarrow & & \downarrow \simeq & & \downarrow \simeq \\
0 & \to & \operatorname{Hom}(M[S^{-1}],N[S^{-1}]) & \to & \operatorname{Hom}(R[S^{-1}]^b,N[S^{-1}]) & \to & \operatorname{Hom}(R[S^{-1}]^a,N[S^{-1}])
\end{array}$$

  Here we used the fact that localization preserves exactness: see the Proposition 1.2.5 below.

- ◇ Let $\varphi : R \to R'$ be a ring homomorphism and $S \subset R$ be a multiplicative subset, so that $S' := \varphi(S) \subset R'$ is also multiplicative. View R' as an R-module, then we

have

$$\underbrace{R'[(S')^{-1}]}_{\text{as ring}} \xrightarrow{\sim} \underbrace{R'[S^{-1}]}_{\text{as module}} = R[S^{-1}] \underset{R}{\otimes} R'$$

$$r'/\varphi(s) \longmapsto (1/s) \otimes r'$$

$$r'\varphi(r)/\varphi(s) \longmapsfrom (r/s) \otimes r'$$

- ◇ As a special case, take φ to be a quotient homomorphism $R \to R/I$, we get a natural isomorphism

$$(R/I)[(S')^{-1}] \simeq R[S^{-1}] \underset{R}{\otimes} (R/I) = \frac{R[S^{-1}]}{I[S^{-1}]}$$

from the right exactness of $\otimes$.

We prove an easy yet fundamental property of localizations, namely they are exact functors.

Proposition 1.2.5 (Exactness of localization)**.** *Let S be any multiplicative subset of R. If*

$$\cdots \to M_i \xrightarrow{f_i} M_{i+1} \to \cdots$$

is an exact sequence of R-modules, then

$$\cdots \to M_i[S^{-1}] \xrightarrow{f_i[S^{-1}]} M_{i+1}[S^{-1}] \to \cdots$$

is also exact.

Proof. By homological common sense, we are reduced to the exact sequences (i) $0 \to M' \to M \to M''$ (i.e. left exactness), (ii) $M' \to M \to M'' \to 0$ (i.e. right exactness). The case (ii) is known for tensor products in general.

As for (i), note that for every homomorphism $g : M \to M''$,

$$\begin{aligned}\ker\left(g[S^{-1}]\right) &= \left\{\frac{y}{s} \in M[S^{-1}] : \exists t \in S,\ tg(y) = 0\right\} \overset{\because y/s = ty/ts}{=\!=} \left\{\frac{y}{s} : y \in \ker(g)\right\} \\ &= \operatorname{im}\left[\ker(g)[S^{-1}] \to M[S^{-1}]\right].\end{aligned}$$

Thus it remains to show that if $f : M' \hookrightarrow M$, then $f[S^{-1}] : M'[S^{-1}] \to M[S^{-1}]$ is injective as well. If $x/s \mapsto f(x)/s = 0$ under $f[S^{-1}]$, there exists $t \in S$ such that $tf(x) = f(tx) = 0$ in M, therefore $tx = 0$ in M', but the latter condition implies $x/s = 0$ in $M'[S^{-1}]$. □

Lemma 1.2.6. *Let M be an R-module. The localizations $M \to M_{\mathfrak{m}}$ for various maximal ideals $\mathfrak{m}$ assemble into an injection*

$$M \hookrightarrow \prod_{\mathfrak{m} \in \operatorname{MaxSpec}(R)} M_{\mathfrak{m}}.$$

Proof. Let $m \in M$ be such that $m \mapsto 0 \in M_{\mathfrak{m}}$ for all $\mathfrak{m}$. This means that for all $\mathfrak{m}$ there exists $s \in R \setminus \mathfrak{m}$ such that $sm = 0$. Hence the annihilator ideal $\operatorname{ann}_R(m) := \{r \in R : rm = 0\}$ is not contained in any maximal ideal, thus $\operatorname{ann}_R(m) = R$. □

There is an analogue for rings. Observe that when R is an integral domain, all the localizations $R[S^{-1}]$ can be regarded as subrings of the field of fractions $\operatorname{Frac}(R)$.

Lemma 1.2.7. *Let R be an integral domain, then $R = \bigcap_{\mathfrak{m} \in \operatorname{MaxSpec}(R)} R_{\mathfrak{m}}$ as subrings of* $\operatorname{Frac}(R)$.

Proof. Only the inclusion $\supset$ requires proof. Let $x \in \operatorname{Frac}(R)$ and define $D := \{r \in R : rx \in R\}$ (the ideal of denominators). Suppose $x \in R_{\mathfrak{m}}$ for all maximal $\mathfrak{m}$, then $D \not\subset \mathfrak{m}$ for all maximal $\mathfrak{m}$. The same reasoning as above leads to $D = R$. □

It will be important to gain finer control on the ideals $\mathfrak{m}$ in the assertion above, say by using some prime ideals "lower" than the maximal ones. We will return to this issue later.

1.3 Radicals and Nakayama's lemma

We begin with two important notions of radicals. The first version is defined as follows. Given an ideal I of R, the *nilpotent radical* $\sqrt{I}$ is defined to be

$$\sqrt{I} := \{r \in R : \exists n,\ r^n \in I\}.$$

It is readily seen to be an ideal from the binomial identity $(a+b)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} a^k b^{2n-k}$. It should also be clear that $\sqrt{I} \subset R$ equals the preimage of $\sqrt{0} \subset R/I$.

Exercise 1.3.1. Show that $\sqrt{\sqrt{I}} = I$ for all ideal I.

Proposition 1.3.2. *Let I be a proper ideal of R. We have*

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec}(R) \\ \mathfrak{p} \supset I}} \mathfrak{p}.$$

Proof. By replacing R by R/I, this is easily reduced to the case $I = \{0\}$. If r is nilpotent and $\mathfrak{p} \in \operatorname{Spec}(R)$, then $r^n = 0 \in \mathfrak{p}$ implies $r \in \mathfrak{p}$. Conversely, suppose that r is not nilpotent. There exists a prime ideal in $R[r^{-1}]$, which comes from some $\mathfrak{p} \in \operatorname{Spec}(R)$ with $r \in R \setminus \mathfrak{p}$ by (1–1). Hence $r \notin \mathfrak{p}$. □

Remark 1.3.3. A ring R is called *reduced* if $\sqrt{0} = \{0\}$. In any case, $R_{\mathrm{red}} := R/\sqrt{0}$ is a reduced ring. Furthermore, any reduced quotient of R factors through R_{red}.

The second radical is probably familiar to the readers. The *Jacobson radical* $\operatorname{rad}(R)$ of the ring R is the intersection of all maximal ideals. The previous proposition implies $\operatorname{rad}(R) \supset \sqrt{(0)}$. Note that

$$a \in \operatorname{rad}(R) \implies (1 + a) \in R^\times.$$

Indeed, $1+a$ cannot be contained in any maximal ideal $\mathfrak{m}$, for otherwise $1 = (1+a)-a \in \mathfrak{m}$, which is absurd.

To prove the celebrated Nakayama's Lemma, let us recall an easy variant of the Cayley–Hamilton theorem from linear algebra.

Lemma 1.3.4. *Suppose that $I \subset R$ is an ideal, M is an R-module with generators $x_1, \dots, x_n$ and $\varphi \in \mathrm{End}_R(M)$ satisfies $\varphi(M) \subset IM$, then there exists a polynomial $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in R[X]$ with $a_i \in I$, such that $P(\varphi) = \varphi^n + a_{n-1}\varphi^{n-1} + \cdots + a_0 = 0$.*

Proof. Write $\varphi(x_i) = \sum_{j=1}^n a_{ij}x_j$ where $a_{ij} \in I$. Set $A := (a_{ij})_{1\le i,j\le n} \in \mathrm{Mat}_n(R)$. Regard M as an $R[X]$-module by letting X act as φ. Then we have the matrix equation over $R[X]$

$$(X \cdot \mathrm{id}_{n\times n} - A) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Multiplying by the cofactor matrix $(X \cdot \mathrm{id}_M - A)^\vee$ on the left, we see that $P(X) := \det(X \cdot \mathrm{id}_{n\times n} - A) \in R[X]$ acts as 0 on each x_i, thus on the whole M. This is the required polynomial. □

Theorem 1.3.5 (Nakayama's Lemma)**.** *Suppose that M is a finitely generated R-module and I is an ideal of R such that $IM = M$. Then there exists $a \in I$ such that $(1+a)M = 0$. If $I \subset rad(R)$, then we have $M = \{0\}$ under these assumptions.*

Proof. Write $M = Rx_1 + \cdots + Rx_n$. Plug $\varphi = \mathrm{id}_M$ into Lemma 1.3.4 to deduce that $P(\mathrm{id}_M) = 1 + \underbrace{a_{n-1} + \cdots + a_0}_{=:a\in I}$ acts as 0 on M. This proves the first part. Assume furthermore that $I \subset \mathrm{rad}(R)$, then $1 + a \in R^\times$ so that $M = (1+a)M = 0$. □

Nakayama's Lemma is named after Tadashi Nakayama (1912—1964). Picture borrowed from [14].

Corollary 1.3.6. *Let M be a finitely generated R-module, and let $I \subset \mathrm{rad}(R)$ be an ideal of R. If the images of $x_1, \dots, x_n \in M$ in M/IM form a set of generators, then $x_1, \dots, x_n$ generate M.*

Proof. Apply Theorem 1.3.5 to $N := M/(Rx_1 + \cdots + Rx_n)$; our assumption $M = IM + Rx_1 + \cdots + Rx_n$ entails that $IN = N$, thus $N = 0$. □

We record another amusing consequence of Theorem 1.3.5.

Proposition 1.3.7. *Let M be a finitely generated R-module and $\psi \in \mathrm{End}_R(M)$. If ψ is surjective then ψ is an automorphism.*

Proof. Introduce a variable Y. Make M into an $R[Y]$-module by letting Y act as ψ. Put $I := (Y)$ so that $IM = M$. Theorem 1.3.5 yields some $Q(Y) \in R[Y]$ satisfying $(1 - Q(Y)Y)M = 0$, that is, $Q(\psi)\psi = \mathrm{id}_M$. □

1.4 Noetherian and Artinian rings

An R-module M is called *Noetherian* (resp. *Artinian*) if every ascending (resp. descending) chain of submodules eventually stabilizes. Recall that in a short exact sequence $0 \to M' \to M \to M'' \to 0$, we have M is Noetherian (resp. Artinian) if and only if M' and M'' are. Being both Noetherian and Artinian is equivalent to being a module of *finite length*, that is, a module admitting composition series.

If we take $M := R$ on which R acts by multiplication, then the submodules are precisely the ideals of R. We say that R is a Noetherian (resp. Artinian) ring if R as an R-module is Noetherian (resp. Artinian); this translates into the corresponding chain conditions on the ideals. Both chain conditions are preserved under passing to quotients and localizations. Finitely generated modules over a Noetherian ring are Noetherian. The following result ought to be known to the readers.

Theorem 1.4.1 (Hilbert's Basis Theorem)**.** *If R is Noetherian, then so is the polynomial algebra $R[X_1, \ldots, X_n]$ for any $n \in \mathbb{Z}_{\geq 1}$.*

Joint with the foregoing remarks, we infer that finitely generated algebras over Noetherian rings are still Noetherian.

On the other hand, being Artinian is a rather stringent condition on rings.

Theorem 1.4.2. *A ring R is Artinian if and only if R is of finite length as an R-module. Such rings are semi-local.*

Proof. As noticed before, having finite length implies that R is Noetherian as well as Artinian. Assume conversely that R is an Artinian ring. First we claim that $\mathrm{MaxSpec}(R)$ is finite, i.e. R is semi-local. If there were an infinite sequence of distinct maximal ideals $\mathfrak{m}_1, \mathfrak{m}_2, \ldots$, we would have an infinite chain

$$\mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3 \supset \cdots.$$

This chain is strictly descending, since $\mathfrak{m}_1 \cdots \mathfrak{m}_i = \mathfrak{m}_1 \cdots \mathfrak{m}_{i+1}$ would imply $\mathfrak{m}_{i+1} \supset \mathfrak{m}_1 \cdots \mathfrak{m}_i$, hence $\mathfrak{m}_{i+1} \supset \mathfrak{m}_j$ for some $1 \leq j \leq i$ because maximal ideals are prime. From the Artinian property we conclude that there are only finitely many maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ of R.

Set $\mathfrak{a} := \mathfrak{m}_1 \cdots \mathfrak{m}_n$. Since R is Artinian we must have $\mathfrak{a}^k = \mathfrak{a}^{k+1}$ for some $k > 0$. We claim that $\mathfrak{a}^k = 0$.

Put $\mathfrak{b} := \{r \in R : r\mathfrak{a}^k = 0\}$, we have to show $\mathfrak{b} = R$. If not, let $\mathfrak{b}'$ be a minimal ideal lying strictly over $\mathfrak{b}$. Thus $\mathfrak{b}' = Rx + \mathfrak{b}$ for any $x \in \mathfrak{b}' \setminus \mathfrak{b}$. We must have $\mathfrak{a}x + \mathfrak{b} \subsetneq \mathfrak{b}'$, for otherwise $M := \mathfrak{b}'/\mathfrak{b}$ is finitely generated (say by x) and satisfies $M = \mathfrak{a}M$, then Theorem 1.3.5 plus $\mathfrak{a} \subset \mathrm{rad}(R)$ would imply $M = \{0\}$, which is absurd. By minimality we have $\mathfrak{b} = \mathfrak{a}x + \mathfrak{b}$. It follows that $\mathfrak{a}x \subset \mathfrak{b}$, i.e. $\mathfrak{a}^{k+1}x = 0$; from $\mathfrak{a}^k = \mathfrak{a}^{k+1}$ we infer $x \in \mathfrak{b}$. Contradiction.

All in all, we obtain a descending chain of ideals

$$\begin{aligned} R &\supset \mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \cdots \supset \mathfrak{m}_1 \cdots \mathfrak{m}_n = \mathfrak{a} \\ &\supset \mathfrak{a}\mathfrak{m}_1 \supset \mathfrak{a}\mathfrak{m}_1\mathfrak{m}_2 \supset \cdots \supset \mathfrak{a}\mathfrak{m}_1 \cdots \mathfrak{m}_n = \mathfrak{a}^2 \\ &\supset \cdots \supset \mathfrak{a}^k = \{0\}. \end{aligned}$$

Each subquotient thereof, which is *a priori* an R-module, is actually an $R/\mathfrak{m}_i$-vector space for some $1 \leq i \leq n$. Such a vector space must also satisfy the descending chain condition on vector subspaces, otherwise pulling-back will contradict the Artinian assumption on R. Artinian vector spaces must be finite-dimensional. It follows that all these subquotients are of finite length, hence so is R itself. □

Corollary 1.4.3. *A ring R is Artinian if and only if it is Noetherian and every prime ideal of R is maximal.*

Proof. If R is Artinian, then R is of finite length, hence is Noetherian as well. For every prime ideal $\mathfrak{p}$, we have $\mathfrak{p} \supset \{0\} = (\mathfrak{m}_1 \cdots \mathfrak{m}_n)^k$ in the notations of the proof above, therefore $\mathfrak{p} \supset \mathfrak{m}_i$ for some i, so $\mathfrak{p} = \mathfrak{m}_i$ is maximal.

Conversely, if R is Noetherian but of infinite length, then the nonempty set of ideals

$$\mathcal{S} := \{\text{ideals } I \subsetneq R : R/I \text{ has infinite length}\}$$

contains a maximal element $\mathfrak{p}$. We contend that $\mathfrak{p}$ is prime. If $xy \in \mathfrak{p}$ with $x, y \notin \mathfrak{p}$, then $R/(\mathfrak{p} + Rx)$ has finite length by the choice of $\mathfrak{p}$; on the other hand, $\mathfrak{a} := \{r \in R : rx \in \mathfrak{p}\} \supsetneq \mathfrak{p}$ (as $y \in \mathfrak{a}$), hence $R/\mathfrak{a}$ has finite length as well. From the short exact sequence $0 \to R/\mathfrak{a} \xrightarrow{x} R/\mathfrak{p} \to R/(\mathfrak{p} + Rx) \to 0$ we see $R/\mathfrak{p}$ has finite length, contradiction.

If we assume moreover that every prime ideal is maximal, then for the $\mathfrak{p}$ chosen above, $R/\mathfrak{p}$ will be a field, thus of finite length. This is impossible. □

Rings whose prime ideals are all maximal are said to have *dimension zero*, in the sense of Krull dimensions; we shall return to this point in §5.4.

1.5 What is commutative algebra?

In broad terms, *commutative algebra* is the study of commutative rings. Despite its intrinsic beauty, we prefer to motivate from an external point of view. See also [8].

(A) **Algebraic geometry**. To simplify matters, we consider affine algebraic varieties over an algebraically closed field $\Bbbk$. Roughly speaking, such a variety is the zero locus $\mathcal{X} = \{f_1 = \cdots = f_r = 0\}$ in $\mathbb{A}^n = \Bbbk^n$ of $f_i \in \Bbbk[X_1, \ldots, X_n]$. The choice of equations is of course non-unique: what matters is the ideal $I(\mathcal{X}) := \{f \in \Bbbk[X_1, \ldots, X_n] : f|_{\mathcal{X}} = 0\}$.

Conversely, every ideal $\mathfrak{a}$ defines a subset $V(\mathfrak{a}) := \{x \in \mathbb{k}^n : \forall f \in \mathfrak{a},\ f(x) = 0\}$. As consequences of Hilbert's Nullstellensatz, which we will discuss later, we have

$$V \circ I(\mathcal{X}) = \mathcal{X}, \qquad I \circ V(\mathfrak{a}) = \sqrt{\mathfrak{a}}.$$

One can deduce from this that the (closed) subvarieties of $\mathbb{A}^n$ are in bijection with ideals $\mathfrak{a}$ satisfying $\sqrt{\mathfrak{a}} = \mathfrak{a}$.
Furthermore, $\mathbb{k}[\mathcal{X}] := \mathbb{k}[X_1, \dots, X_n]/I(\mathcal{X})$ may be regarded as the ring of "regular functions" (i.e. functions definable by means of polynomials) on $\mathcal{X}$, and $\mathrm{MaxSpec}(\mathbb{k}[\mathcal{X}])$ is in bijection with the points of $\mathcal{X}$: to $x = (x_1, \dots, x_n) \in \mathcal{X}$ we attach

$$\mathfrak{m}_x = (X_1 - x_1, \dots, X_n - x_n) \supset I(\mathcal{X}).$$

By passing to the ring $\mathbb{k}[\mathcal{X}]$, we somehow obtain a description of $\mathcal{X}$ that is independent of embeddings into affine spaces. Moreover, $\mathcal{X}$ inherits the Zariski topology from that on $\mathrm{Spec}(\mathbb{k}[\mathcal{X}])$.
Naively speaking, the geometric properties of $\mathcal{X}$ transcribe in ring-theoretic terms to the reduced Noetherian $\mathbb{k}$-algebra $\mathbb{k}[\mathcal{X}]$. For example, assume that $f \in \mathbb{k}[\mathcal{X}]$ is not nilpotent, then the formation of $\mathbb{k}[\mathcal{X}][f^{-1}]$ corresponds to taking the Zariski-open subset $\mathcal{X}_f = \{x \in \mathcal{X} : f(x) \neq 0\}$ of $\mathcal{X}$. This may be explained as follows:

$$\mathcal{X}_f \simeq \{(x_1, \dots, x_n, y) : f_1(x_1, \dots, x_n) = \cdots = f_r(x_1, \dots, x_n) = 0,\ f(x_1, \dots, x_n)y = 1\}$$

which is also an affine algebraic variety in $\mathbb{k}^{n+1}$, and one may verify that $\mathbb{k}[\mathcal{X}_f] = \mathbb{k}[\mathcal{X}][f^{-1}]$.

(B) **Invariant theory**. Let G be a group acting on a finite-dimensional $\mathbb{k}$-vector space V from the right, and let $\mathbb{k}[V]$ be the $\mathbb{k}$-algebra of polynomials on V. Thus $\mathbb{k}[V]$ carries a left G-action by $gf(v) = f(vg)$. For "reasonable" groups G, say finite or $\mathbb{k}$-algebraic ones, the classical invariant theory seeks to describe the subalgebra $\mathbb{k}[V]^G$ of invariants[1] in terms of *generators* and *relations*.
In particular, one has to know when is the algebra $\mathbb{k}[V]^G$ finitely generated. This is actually the source of many results in commutative algebra, such as the Basis Theorem and Nullstellensatz of Hilbert. For example, let the symmetric group $G = \mathfrak{S}_n$ act on $V = \mathbb{k}^n$ in the standard manner, then our question is completely answered by the following classical result: $\mathbb{k}[V]^G$ equals the polynomial algebra $\mathbb{k}[e_1, \dots, e_n]$, where e_i stands for the i-th elementary symmetric function in n variables.
The same questions may be posed for any affine algebraic variety V. From the geometric point of view, if $\mathbb{k}[V]^G$ is finitely generated, it will consist of regular functions of some kind of quotient variety $V//G$. The study of quotients in this sense naturally leads to *geometric invariant theory*, for which we refer to [16] for details.

[1] More generally, we are also interested in the algebra of invariant differential operators with polynomial coefficients.

Lecture 2

Primary decompositions

We shall follow [8, §3] and [11, §8] closely.

2.1 The support of a module

Fix a ring R. For any R-module M and $x \in M$, we define the *annihilator* $\operatorname{ann}_R(x) := \{r \in R : rx = 0\}$; it is an ideal of R. Also define $\operatorname{ann}_R(M) := \{r \in R : rM = 0\} = \bigcap_{x \in M} \operatorname{ann}_R(x)$.

Definition 2.1.1. The *support* of an R-module M is

$$\operatorname{Supp}(M) := \left\{\mathfrak{p} \in \operatorname{Spec}(R) : M_{\mathfrak{p}} \neq 0\right\}.$$

Let us unwind the definition: $\mathfrak{p} \notin \operatorname{Supp}(M)$ means that every $x \in M$ maps to $0 \in M_{\mathfrak{p}}$, equivalently $\operatorname{ann}_R(x) \not\subset \mathfrak{p}$. To test whether $\mathfrak{p} \notin \operatorname{Supp}(M)$, we only need to check the foregoing condition for x ranging over a generating set of M.

Proposition 2.1.2. *If M is finitely generated then $\operatorname{Supp}(M) = V(\operatorname{ann}_R(M))$; in particular it is Zariski-closed in $\operatorname{Spec}(R)$.*

Proof. Suppose $M = Rx_1 + \cdots + Rx_n$. Set $I_i := \operatorname{ann}_R(x_i)$ and observe that $\bigcap_{i=1}^n I_i = \operatorname{ann}_R(M)$. Then $\mathfrak{p} \in \operatorname{Supp}(M)$ if and only if $\mathfrak{p} \supset I_i$ for some i, that is, $\mathfrak{p} \in \bigcup_{i=1}^n V(I_i)$. To conclude, note that $V(I) \cup V(J) = V(IJ) = V(I \cap J)$ for any ideals $I, J \subset R$ (an easy exercise). □

Finite generation is needed in the result above. Consider the $\mathbb{Z}$-module $M := \bigoplus_{a \geq 1} \mathbb{Z}/p^a\mathbb{Z}$. Its support is $\{p\}$ but $\operatorname{ann}(M) = \{0\}$.

Proposition 2.1.3. *For an exact sequence $0 \to M' \to M \to M'' \to 0$ we have $\operatorname{Supp}(M) = \operatorname{Supp}(M') \cup \operatorname{Supp}(M'')$. For arbitrary direct sums we have $\operatorname{Supp}(\bigoplus_i M_i) = \bigcup_i \operatorname{Supp}(M_i)$.*

Proof. Again, we use the exactness of localization for the first assertion. For $\mathfrak{p} \in \operatorname{Spec}(R)$ we have an exact $0 \to M'_{\mathfrak{p}} \to M_{\mathfrak{p}} \to M''_{\mathfrak{p}} \to 0$, hence $M_{\mathfrak{p}} \neq 0$ if and only if $\mathfrak{p} \in \operatorname{Supp}(M') \cup \operatorname{Supp}(M'')$. The second assertion is obvious. □

From an R-module M, one can build a "field of modules" over $\mathrm{Spec}(R)$ by assigning to each $\mathfrak{p}$ the $R_\mathfrak{p}$-module $M_\mathfrak{p}$, and $\mathrm{Supp}(M)$ is precisely the subset of $M_\mathfrak{p}$ over which the field is non-vanishing. This is how the support arises in algebraic geometry. A more precise description will require the notion of quasi-coherent sheaves on schemes.

Exercise 2.1.4. Let M, N be finitely generated R-modules. Show that $\mathrm{Supp}(M \underset{R}{\otimes} N) = \mathrm{Supp}(M) \cap \mathrm{Supp}(N)$. Hint: since localization commutes with $\otimes$, it suffices to prove that $M \underset{R}{\otimes} N \neq \{0\}$ when M, N are both nonzero finitely generated modules over a local ring R. Nakayama's Lemma implies that $M \underset{R}{\otimes} \Bbbk$ and $\Bbbk \underset{R}{\otimes} N$ are both nonzero where $\Bbbk$ is the residue field of R. Now

$$(M \underset{R}{\otimes} \Bbbk) \underset{\Bbbk}{\otimes} (\Bbbk \underset{R}{\otimes} N) \simeq M \underset{R}{\otimes} (\Bbbk \underset{\Bbbk}{\otimes} \Bbbk) \underset{R}{\otimes} N \simeq (M \underset{R}{\otimes} N) \underset{R}{\otimes} \Bbbk$$

is nonzero.

2.2 Associated primes

Throughout this section, R will be a Noetherian ring.

Definition 2.2.1. A prime ideal $\mathfrak{p}$ is said to be an *associated prime* of an R-module M if $\mathrm{ann}_R(x) = \mathfrak{p}$ for some $x \in M$; equivalently, $R/\mathfrak{p}$ embeds into M. Denote the set of associated primes of M by $\mathrm{Ass}(M)$.

Example 2.2.2. For the $\mathbb{Z}$-module $M := \mathbb{Z}/n\mathbb{Z}$ with $n \in \mathbb{Z}_{>1}$, one easily checks that $\mathrm{Ass}(M)$ is the set of prime factors of n.

Lemma 2.2.3. *Consider the set $\mathcal{S} := \{\mathrm{ann}_R(x) : x \in M,\ x \neq 0\}$ of ideals, partially ordered by inclusion. Every maximal element in $\mathcal{S}$ is prime.*

Proof. Let $\mathfrak{p} = \mathrm{ann}_R(x)$ be a maximal element of $\mathcal{S}$ and suppose $ab \in \mathfrak{p}$. If $b \notin \mathfrak{p}$, then

$$bx \neq 0, \quad abx = 0, \quad R \neq \mathrm{ann}_R(bx) \supset \mathrm{ann}_R(x) = \mathfrak{p}.$$

Hence $a \in \mathrm{ann}_R(bx) = \mathfrak{p}$ by the maximality of $\mathfrak{p}$ in $\mathcal{S}$. □

Definition 2.2.4. Call $r \in R$ a *zero divisor* on M if $rx = 0$ for some $x \in M \setminus \{0\}$.

Theorem 2.2.5. *Let M be an R-module.*

(*i*) *We have $M = \{0\}$ if and only if $\mathrm{Ass}(M) = \emptyset$.*

(*ii*) *The union of all $\mathfrak{p} \in \mathrm{Ass}(M)$ equals the set of zero divisors on M.*

(*iii*) *For any multiplicative subset $S \subset R$, we have*

$$\mathrm{Ass}(M[S^{-1}]) = \left\{\mathfrak{p}[S^{-1}] : \mathfrak{p} \in \mathrm{Ass}(M),\ \mathfrak{p} \cap S = \emptyset\right\}.$$

(*iv*) *If $0 \to M' \to M \to M''$ is exact, then $\mathrm{Ass}(M') \subset \mathrm{Ass}(M) \subset \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$.*

Proof. (i) Clearly $\mathrm{Ass}(\{0\}) = \emptyset$. If $M \neq 0$, the set $\mathcal{S}$ in Lemma 2.2.3 is then nonempty, hence contains a maximal element $\mathfrak{p}$ because R is Noetherian; this yields $\mathfrak{p} \in \mathrm{Ass}(M)$.

(ii) Elements of any $\mathfrak{p} \in \mathrm{Ass}(M)$ are all zero divisors by the very definition of associated primes. Conversely, if $r \in \mathrm{ann}_R(x)$ for some $x \in M \setminus \{0\}$, there must exist some maximal element $\mathfrak{p}$ of $\mathcal{S}$ with $\mathfrak{p} \supset \mathrm{ann}_R(x)$ as R is Noetherian; so $\mathfrak{p}$ is the required associated prime containing r.

(iii) If $\mathfrak{p} \in \mathrm{Spec}(R)$, $\mathfrak{p} \cap S = \emptyset$ and there is some $R/\mathfrak{p} \hookrightarrow M$, then

$$\{0\} \neq R[S^{-1}]/\mathfrak{p}[S^{-1}] \simeq (R/\mathfrak{p})[S^{-1}] \hookrightarrow M[S^{-1}]$$

by the exactness of localizations, hence $\mathfrak{p}[S^{-1}] \in \mathrm{Ass}(M[S^{-1}])$. Conversely, every element of $\mathrm{Ass}(M[S^{-1}])$ has the form $\mathfrak{p}[S^{-1}]$ for some $\mathfrak{p} \in \mathrm{Spec}(R)$ disjoint from S. Also recall that $\mathfrak{p}$ equals the preimage of $\mathfrak{p}[S^{-1}]$ under $R \to R[S^{-1}]$. There exist $x \in M$ and $s \in S$ such that $\mathfrak{p}[S^{-1}] = \mathrm{ann}_{R[S^{-1}]}(x/s) = \mathrm{ann}_{R[S^{-1}]}(x)$. Ideals in a Noetherian ring being finitely generated, we infer that $\exists t \in S$ with $\mathfrak{p} \subset \mathrm{ann}_R(tx)$. It remains to show $\mathfrak{p} = \mathrm{ann}_R(tx)$. If $rtx = 0$ for some $r \in R$, then r maps into $r/1 \in \mathfrak{p}[S^{-1}] = \mathrm{ann}_{R[S^{-1}]}(x)$; thus $r \in \mathfrak{p}$.

(iv) It suffices to treat the second $\subset$. Suppose that $\mathfrak{p} \in \mathrm{Ass}(M)$ and $R/\mathfrak{p} \simeq N$ for some submodule $N \subset M$. Identify M' with $\ker(M \to M'')$. If $M' \cap N = \{0\}$ then $R/\mathfrak{p} \simeq N \hookrightarrow M''$, so $\mathfrak{p} \in \mathrm{Ass}(M'')$. If there exists $x \in M' \cap N \subset N$ with $x \neq 0$, then we have $\mathrm{ann}_R(x) = \mathfrak{p}$ since $N \simeq R/\mathfrak{p}$ and $\mathfrak{p}$ is prime; in this case $\mathfrak{p} \in \mathrm{Ass}(M')$. □

We remark that $0 \to M' \to M \to M'' \to 0$ being exact does not imply $\mathrm{Ass}(M) = \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$. To see this, consider $R = \mathbb{Z}$ and $0 \to \mathbb{Z} \xrightarrow{p} \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0$ for some prime number p.

Exercise 2.2.6. Show that $\mathrm{Ass}(M_1 \oplus M_2) = \mathrm{Ass}(M_1) \cup \mathrm{Ass}(M_2)$.

Theorem 2.2.7. *For every R-module M we have* $\mathrm{Supp}(M) = \bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)} V(\mathfrak{p})$, *in particular* $\mathrm{Ass}(M) \subset \mathrm{Supp}(M)$. *Furthermore, every minimal element of* $\mathrm{Supp}(M)$ *with respect to inclusion is actually a minimal element of* $\mathrm{Ass}(M)$.

Proof. For any prime $\mathfrak{q}$ we have $M_{\mathfrak{q}} \neq 0 \iff \mathrm{Ass}(M_{\mathfrak{q}}) \neq \emptyset$, and the latter condition holds precisely when there exists $\mathfrak{p} \in \mathrm{Ass}(M)$ with $\mathfrak{p} \cap (R \setminus \mathfrak{q}) = \emptyset$, i.e. $\mathfrak{q} \supset \mathfrak{p}$. This proves the first assertion. The second assertion is a direct consequence. □

Observe that if $\mathfrak{p} \in \mathrm{Supp}(M)$, then $\mathfrak{q} \supset \mathfrak{p} \implies \mathfrak{q} \in \mathrm{Supp}(M)$: the reason is that

$$M_{\mathfrak{p}} = (M_{\mathfrak{q}})_{\mathfrak{p}R_{\mathfrak{q}}} \tag{2–1}$$

thus the occurrence of non-minimal elements in $\mathrm{Supp}(M)$ is unsurprising. In contrast, the non-minimal elements in $\mathrm{Ass}(M)$ are somehow mysterious. These non-minimal associated primes are called *embedded primes*.

Exercise 2.2.8. Prove the formula (2–1) of "localization in stages".

Hereafter we impose finite generation on M. This implies M is Noetherian.

Theorem 2.2.9. *Let M be a finitely generated R-module. There exists a chain $M = M_n \supset M_{n-1} \supset \cdots \supset M_0 = \{0\}$ of submodules such that for every $0 < i \leq n$, the subquotient M_i/M_{i-1} is isomorphic to $R/\mathfrak{p}_i$ for some prime ideal $\mathfrak{p}_i$.*

Furthermore we have $\mathrm{Ass}(M) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$; in particular $\mathrm{Ass}(M)$ is a finite set.

Proof. Assume $M \supsetneq M_0 := \{0\}$. There exists $\mathfrak{p}_1 \in \mathrm{Ass}(M)$ together with a submodule $M_1 \subset M$ isomorphic to $R/\mathfrak{p}_1$. Furthermore $\mathrm{Ass}(M_1) = \mathrm{Ass}(R/\mathfrak{p}_1) = \{\mathfrak{p}_1\}$ as easily seen. Hence the Theorem 2.2.5 entails $\mathrm{Ass}(M) \subset \{\mathfrak{p}_1\} \cup \mathrm{Ass}(M/M_1)$.

If $M_1 = M$ we are done. Otherwise we start over with M/M_1, finding $M_1 \subset M_2 \subset M$ with $M_2/M_1 \simeq R/\mathfrak{p}_2$ where $\mathfrak{p}_2 \in \mathrm{Ass}_R(M/M_1)$, and so forth. This procedure terminates in finite steps since M is Noetherian. □

2.3 Primary and coprimary modules

The classical framework of primary decompositions concerns ideals, but it is advantageous to allow modules here. As before, the ring R is Noetherian.

Definition 2.3.1. An R-module M is called *coprimary* if $\mathrm{Ass}(M)$ is a singleton. A submodule $N \subsetneq M$ is called a $\mathfrak{p}$-*primary* submodule if M/N is coprimary with associated prime $\mathfrak{p} \in \mathrm{Spec}(R)$.

Proposition 2.3.2. *The following are equivalent for a nonzero R-module M.*

(*i*) *M is coprimary;*

(*ii*) *for every zero divisor $r \in R$ for M and every $x \in M$, there exists $n \geq 1$ such that $r^n x = 0$.*

The condition (ii) is usually called the local-nilpotency of r on M. When $M = R/I$ for some ideal I, it translates into: all zero divisors of the ring R/I are nilpotent.

Proof. (i) $\implies$ (ii): Suppose $\mathrm{Ass}(M) = \{\mathfrak{p}\}$ and $x \in M \setminus \{0\}$. From $\emptyset \neq \mathrm{Ass}(Rx) \subset \mathrm{Ass}(M)$ we infer that $\mathrm{Ass}(Rx) = \{\mathfrak{p}\}$, thus by Theorem 2.2.7 we see $V(\mathfrak{p}) = \mathrm{Supp}(Rx) = V(\mathrm{ann}(Rx))$. Hence $\mathfrak{p} = \sqrt{\mathrm{ann}(Rx)}$. This implies (ii) by the definition of $\sqrt{\ }$.

(ii) $\implies$ (i): It is routine to check that

$$\mathfrak{p} := \{r \in R : \forall x \in M \ \exists n \geq 1,\ r^n x = 0\}$$

is an ideal of R. For every $\mathfrak{q} \in \mathrm{Ass}(M)$ there exists $x \in M$ with $\mathrm{ann}_R(x) = \mathfrak{q}$. Every $r \in \mathfrak{p}$ has some power falling in $\mathfrak{q}$, thus $\mathfrak{p} \subset \mathfrak{q}$. Conversely, (ii) and Theorem 2.2.5 imply $\mathfrak{q} = \mathrm{ann}_R(x) \subset \mathfrak{p}$. From $\mathfrak{q} = \mathfrak{p}$ we conclude M is coprimary with the unique associated prime $\mathfrak{p}$. □

Exercise 2.3.3 (Classical definition of primary ideals)**.** Let I be a proper ideal of R. Show that R/I is coprimary if and only if the following holds:

$$\forall a, b \in R,\ (ab \in I) \wedge (a \notin I) \implies \exists n \geq 1,\ b^n \in I.$$

In this case we also say I is a *primary ideal* of R. Show that $\{\sqrt{I}\} = \mathrm{Ass}(R/I)$ if I is a primary ideal. Hint: apply Proposition 2.3.2.

Exercise 2.3.4. Let $\mathfrak{m}$ be a maximal ideal of R. Show that every ideal $I \subsetneq R$ containing some power of $\mathfrak{m}$ is primary, and $\mathrm{Ass}(R/I) = \{\mathfrak{m}\}$. Hint: show that $\mathfrak{m}$ is the only prime ideal containing $I = \mathrm{ann}_R(R/I)$.

Lemma 2.3.5. *Let $\mathfrak{p} \in \mathrm{Spec}(R)$ and $N_1, N_2 \subset M$ are $\mathfrak{p}$-primary submodules. Then $N_1 \cap N_2$ is a $\mathfrak{p}$-primary submodule of M.*

Proof. We have $M/N_1 \cap N_2 \hookrightarrow M/N_1 \oplus M/N_2$. Since $N_1 \cap N_2 \neq M$, we have

$$\emptyset \neq \mathrm{Ass}(M/N_1 \cap N_2) \subset \mathrm{Ass}(M/N_1) \cup \mathrm{Ass}(M/N_2) = \{\mathfrak{p}\}$$

by Theorem 2.2.5. □

2.4 Primary decomposition: the main theorem

We still assume R Noetherian and fix a finitely generated R-module M.

Theorem 2.4.1 (Lasker–Noether)**.** *Let $N \subsetneq M$ be an R-submodule. Then we can express N as*

$$N = M_1 \cap \cdots \cap M_n,$$

for some $n \geq 1$ and primary R-submodules M_i, say with $\mathrm{Ass}(M/M_i) = \{\mathfrak{p}_i\}$ for $i = 1, \ldots, n$. Such a decomposition is called a primary decomposition *of N. We say it is* irredundant *if none of the M_i can be dropped, and* minimal *if there is no such decomposition with fewer terms.*

(*i*) *We have $\mathrm{Ass}(M/N) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, equality holds when the decomposition is irredundant.*

(*ii*) *If the decomposition is minimal, then for every $\mathfrak{p} \in \mathrm{Ass}(M/N)$ there exists a unique $1 \leq i \leq n$ with $\mathfrak{p} = \mathfrak{p}_i$; consequently $n = |\mathrm{Ass}(M/N)|$.*

(*iii*) *Consider a primary decomposition of N. Let $S \subset R$ be any multiplicative subset, and assume without loss of generality that $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ are the primes among $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ which are disjoint from S, then $m \geq 1 \iff N[S^{-1}] \subsetneq M[S^{-1}]$ and*

$$N[S^{-1}] = M_1[S^{-1}] \cap \cdots \cap M_m[S^{-1}]$$

is a primary decomposition of the $R[S^{-1}]$-submodule $N[S^{-1}] \subsetneq M[S^{-1}]$; this decomposition of $N[S^{-1}]$ is minimal if the one for N is.

Note that the "irredundant" condition in [11, (8.D)] corresponds to minimality here. The rings whose ideals all have primary decompositions are called *Laskerian rings*, thus part (i) of the Theorem says Noetherian implies Laskerian, but there exist non-Noetherian examples.

Proof. Establish the existence of primary decompositions first. Replacing M by M/N, we may assume $N = \{0\}$ from the outset. We claim that

$$\forall \mathfrak{p} \in \mathrm{Ass}(M),\ \exists Q(\mathfrak{p}) \subset M,\ \begin{cases} Q(\mathfrak{p}) \text{ is } \mathfrak{p}\text{-primary}, \\ \mathrm{Ass}(Q(\mathfrak{p})) = \mathrm{Ass}(M) \setminus \{\mathfrak{p}\}. \end{cases} \tag{2–2}$$

Granting this, $Q := \bigcap_{\mathfrak{p}\in \mathrm{Ass}(M)} Q(\mathfrak{p})$ yields the required decomposition since $\mathrm{Ass}(M)$ is finite and $\mathrm{Ass}(Q) = \emptyset$.

Establish (2–2) as follows. Put $\Psi := \{\mathfrak{p}\}$. By Zorn's Lemma we get a maximal element $Q(\mathfrak{q})$ from the set

$$\emptyset \neq \{Q \subset M : \text{submodule},\ \mathrm{Ass}(Q) \subset \mathrm{Ass}(M) \setminus \Psi\}$$

which is partially ordered by inclusion (details omitted, and you may also use the Noetherian property of M). Since

$$\mathrm{Ass}(M) \subset \mathrm{Ass}(M/Q(\mathfrak{p})) \cup \mathrm{Ass}(Q(\mathfrak{p})),$$

it suffices to show $\mathrm{Ass}(M/Q(\mathfrak{p})) \subset \Psi$. Let $\mathfrak{q} \in \mathrm{Ass}(M/Q(\mathfrak{p}))$ so that there exists $M \supset Q' \supset Q(\mathfrak{p})$ with $Q'/Q(\mathfrak{p}) \simeq R/\mathfrak{q}$. Since $\mathrm{Ass}(Q') \subset \mathrm{Ass}(Q(\mathfrak{p})) \cup \{\mathfrak{q}\}$, maximality forces $\mathfrak{q} \in \Psi$ (otherwise $\mathrm{Ass}(Q') \subset \mathrm{Ass}(M) \setminus \Psi$), whence (2–2). Now we turn to the properties (i) — (iii).

(i) The obvious embedding

$$M/N \hookrightarrow \bigoplus_{i=1}^{n} M/M_i$$

together with Theorem 2.2.5 yield $\mathrm{Ass}(M/N) \subset \bigcup_{i=1}^{n} \mathrm{Ass}(M/M_i) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$.
Now assume the given primary decomposition is irredundant, we have

$$\begin{aligned}\{0\} \neq \frac{M_2 \cap \cdots \cap M_n}{N} &= \frac{M_2 \cap \cdots \cap M_n}{M_1 \cap (M_2 \cap \cdots \cap M_n)} \\ &\simeq \frac{M_1 + M_2 \cap \cdots \cap M_n}{M_1} \hookrightarrow M/M_1.\end{aligned}$$

Thus $\mathrm{Ass}(M/N)$ contains $\mathrm{Ass}((M_2 \cap \cdots \cap M_n)/N) = \{\mathfrak{p}_1\}$. Same for $\mathfrak{p}_2, \dots, \mathfrak{p}_n$.

(ii) Suppose $N = M_1 \cap \cdots \cap M_n$ is an irredundant primary decomposition, so that $\mathrm{Ass}(M/N) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$. If $\mathfrak{p}_i = \mathfrak{p}_j$ for some $1 \leq i \neq j \leq n$, Lemma 2.3.5 will imply that $M_i \cap M_j$ is primary, leading to a shorter primary decomposition. This is impossible when the primary decomposition is minimal.

(iii) Suppose $S \cap \mathfrak{p}_i = \emptyset$ (equivalently, $i \leq m$). By Theorem 2.2.5 and the exactness of localization, $M_i[S^{-1}] \subset M[S^{-1}]$ will be $\mathfrak{p}_i[S^{-1}]$-primary. On the other hand $S \cap \mathfrak{p}_i \neq \emptyset$ implies $\mathrm{Ass}((M/M_i)[S^{-1}]) = \emptyset$ by Theorem 2.2.5, thus $M[S^{-1}]/M_i[S^{-1}] = 0$. Since localization respects intersections, we obtain

$$N[S^{-1}] = \bigcap_{i=1}^{m} M_i[S^{-1}].$$

In particular $N[S^{-1}]$ is proper if and only if $m \geq 1$.
It remains to show $\mathrm{Ass}(M[S^{-1}]/N[S^{-1}])$ has m elements if the original primary decomposition is minimal. Indeed, that set is just $\{\mathfrak{p}[S^{-1}] : \mathfrak{p} \in \mathrm{Ass}(M/N),\ \mathfrak{p} \cap S = \emptyset\}$ by Theorem 2.2.5, which equals $\{\mathfrak{p}_1[S^{-1}], \dots, \mathfrak{p}_m[S^{-1}]\}$ (distinct) by (ii).

□

A natural question arises: to what extent are minimal primary decompositions unique? For those M_i whose associated primes are minimal in $\mathrm{Ass}(M/N)$, the answer turns out to be positive.

Corollary 2.4.2. *Let $N = M_1 \cap \cdots \cap M_n$ be a minimal primary decomposition of $N \subsetneq M$. Suppose that M_1 is $\mathfrak{p}$-primary where $\mathfrak{p} := \mathfrak{p}_1$ is a minimal element in $\mathrm{Ass}(M/N)$, then M_1 equals the preimage of $N_\mathfrak{p}$ under $M \to M_\mathfrak{p}$. Call it the* $\mathfrak{p}$-primary component *of N.*

Proof. Recall the proof of Theorem 2.4.1, especially the part (iii); here we localize with respect to $S := R \setminus \mathfrak{p}$. The minimality assumption entails

$$N_\mathfrak{p} = M_{1,\mathfrak{p}} \subset M_\mathfrak{p}.$$

It remains to show that the preimage of $M_{1,\mathfrak{p}}$ under $M \to M_\mathfrak{p}$ equals M_1, in other words the injectivity of the natural map $M/M_1 \to (M/M_1)_\mathfrak{p} = M_\mathfrak{p}/M_{1,\mathfrak{p}}$. Indeed, $\bar{x} \in M/M_1$ maps to 0 if and only if there exists $s \notin \mathfrak{p}$ with $s\bar{x} = 0$, but Theorem 2.2.5 implies that the zero divisors of M/M_1 must lie in $\mathfrak{p}$. □

It follows that the non-uniqueness of minimal primary decompositions can only arise from embedded primes in $\mathrm{Ass}(M/N)$.

2.5 Examples and remarks

Primary decompositions are most often applied in the case $M = R$ and $N = I$ is a proper ideal. The goal is to express I as an intersection of primary ideals. To begin with, let us take $R = \mathbb{Z}$. Observations:

- The primary ideals of R take the form $(p)^n$, where $n \geq 1$ and p is a prime number or zero. This may be deduced from Exercise 2.3.3 or directly from definitions.
- The irredundant primary decompositions of $\mathbb{Z}/n\mathbb{Z}$, for $n > 1$, corresponds to the factorization of n into prime-powers. There are no embedded primes in this case; the irredundant primary decomposition is unique and automatically minimal.

Exercise 2.5.1. Justify the foregoing assertions.

Therefore one can regard primary decompositions as a generalization of factorization of integers, now performed on the level of ideals. The most important case is $R = \Bbbk[X_1, \ldots, X_n]$ (fix some field $\Bbbk$), as it is naturally connected to classical problems in algebraic geometry. Let us consider a simple yet non-trivial example from [8, §3].

Example 2.5.2. Take $R = \Bbbk[X, Y]$ and $I = (X^2, XY)$. The reader is invited to check that

$$I = (X) \cap (X^2, XY, Y^2) = (X) \cap (X^2, Y).$$

Claim: this gives two minimal primary decompositions of I. The ideal (X) is prime, hence primary. In fact, $(X^2, XY, Y^2) = (X, Y)^2$ and (X^2, Y) are both primary ideals associated to the maximal ideal (X, Y). This follows either by direct arguments or by Exercise 2.3.4, noting that $(X, Y)^2 = (X^2, XY, Y^2)$ is contained in (X^2, Y). The embedded prime (X, Y) is seen to be responsible non-uniqueness of primary decompositions.

CHESS PLAYER EMANUEL LASKER.

Emanuel Lasker (1868–1941) first obtained the primary decomposition for finitely generated $\Bbbk$-algebras and the algebras of convergent power series in 1905. His method involves techniques from *elimination theory*. His result is then generalized and rewritten by Emmy Noether in 1921, in which the ascending chain condition plays a pivotal role. Lasker is best known for being the World Chess Champion from 1894 to 1921. (Picture taken from Wikimedia Commons)

To see the geometry behind, recall that $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{ab}) = V(\mathfrak{a} \cap \mathfrak{b})$ for any ideals $\mathfrak{a}, \mathfrak{b}$, thus expressing I as an intersection means breaking the corresponding geometric object into a union of simpler pieces. Also recall that for an ideal $I \subset \Bbbk[X, Y]$, the points in $\bigcap_{f \in I} \{f = 0\}$ are in bijection with the maximal ideals lying over I, at least for $\Bbbk$ algebraically closed (Nullstellensatz). Thus we may interpret these primary decompositions as equalities among "geometric objects" embedded in $\Bbbk^2$:

$$\left\{X^2 = 0, XY = 0\right\} = \begin{cases} \{X = 0\} \cup \left\{X^2 = XY = Y^2 = 0\right\} \\ \{X = 0\} \cup \left\{X^2 = Y = 0\right\}. \end{cases}$$

1. The geometric object defined by $X = 0$ inside $\Bbbk^2$ is certainly the Y-axis: the regular functions living on this space form the $\Bbbk$-algebra $\Bbbk[X, Y]/(X) = \Bbbk[Y]$.

2. The geometric object defined by $X^2 = XY = Y^2 = 0$ looks "physically" like the origin $(0, 0)$, but the $\Bbbk$-algebra of "regular functions" (in an extended sense) living on it equals $\Bbbk[X, Y]/(X^2, XY, Y^2)$: by restricting a polynomial function $f(X, Y)$ to this "thickened point", we see not only $f(0, 0)$ but also $\frac{\partial f}{\partial x}(0, 0)$ and $\frac{\partial f}{\partial y}(0, 0)$. In other words, we shall view $X^2 = XY = Y^2 = 0$ as the first-order infinitesimal neighborhood of $(0, 0) \in \Bbbk^2$.

3. In a similar vein, $X^2 = Y = 0$ physically defines $(0, 0)$, but by restricting f to that thickened point, we retrieve $f(0, 0)$ as well as $\frac{\partial f}{\partial x}(0, 0)$. Therefore we obtain the first-order infinitesimal neighborhood of 0 inside the X-axis.

Both decomposition says that we obtain the Y-axis together with first-order infinitesimal information at the origin $(0, 0)$. This is also a nice illustration of the use

of nilpotent elements in scheme theory.

Example 2.5.3 (Symbolic powers)**.** Let $\mathfrak{p}$ be a prime ideal in a Noetherian ring R and fix $n \geq 1$. Observe that $\mathfrak{p}$ is the unique minimal element in $\mathrm{Supp}(R/\mathfrak{p}^n) = V(\mathfrak{p}^n)$. By Theorem 2.2.7 $\mathfrak{p} \in \mathrm{Ass}(R/\mathfrak{p}^n)$, so it makes sense to denote by $\mathfrak{p}^{(n)}$ the $\mathfrak{p}$-primary component (Corollary 2.4.2) of $\mathfrak{p}^n$, called the n-th *symbolic power* of $\mathfrak{p}$. In general $\mathfrak{p}^{(n)} \supsetneq \mathfrak{p}^n$. For a nice geometric interpretation of symbolic powers due to Nagata and Zariski, we refer to [8, §3.9].

Getting primary decomposition of ideals in polynomial algebras is a non-trivial task. Thanks to the pioneers in computational commutative algebra, this can now achieved on your own computer, eg. by the open-source SageMath system.

Lecture 3

Integral dependence, Nullstellensatz and flatness

The materials below largely come from [8, §4], [1, V.4] and [11, §§5–6]. In what follows, any ring R and the R-algebras are assumed to be commutative. For elements $a, b, \ldots$ in an R-algebra, denote by $R[a, b, \ldots]$ the R-subalgebra generated by them.

3.1 Integral extensions

Consider an R-algebra A. Recall that to give an R-algebra A is the same as to give a ring homomorphism $\varphi : R \to A$. We shall switch freely between algebra and homomorphisms, omitting φ if necessary. In many concrete circumstances R is simply a subring of A.

Definition 3.1.1. An element $x \in A$ is said to be *integral* over R if there exists a monic polynomial $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in R[X]$ (with $n \geq 1$) such that $P(x) = 0$. If every $x \in A$ is integral over R, we say A is integral over R.

Note that elements from R are trivially integral: take $P(X)$ with $n = 1$. In the case $A = \mathbb{C}$ and $R = \mathbb{Z}$, we recover the notion of *algebraic integers*.

When R is a field, we usually say *algebraic* instead of *integral*. The monic assumption on P is crucial when R is not a field, as illustrated by the following proof.

Proposition 3.1.2. *An element $x \in A$ is integral over R if and only if there exists an R-submodule $M \subset A$ such that*

- *M is a finitely generated R-module;*
- *$xM \subset M$, thus M is an $R[x]$-module;*
- *M is a faithful $R[x]$-module i.e. $\operatorname{ann}_{R[x]}(M) = \{0\}$, and*

If x is integral, $M := R[x]$ satisfies the conditions listed above.

Proof. This is a familiar application of Cayley-Hamilton theorem, which we recall below. If x is integral, say $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, a straightforward induction shows that

$$R[x] = \sum_{i=0}^{n-1} Rx^i.$$

In particular we may take $M := R[x]$ to be the required submodule, which is faithful as $1 \in R[x]$. Conversely, given a submodule M as above, with generators $x_1, \dots, x_m$, we make M into an $R[X]$-module by letting the variable X act as multiplication by x. Writing $x \cdot x_i = \sum_{j=1}^{m} a_{ij} x_j$, there is the matrix equation

$$(X \cdot 1_{m\times m} - A) \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = 0, \quad A = (a_{ij})_{1\le i,j\le m} \in \mathrm{Mat}_{m\times m}(R)$$

over $R[X]$. Now multiply both sides by the cofactor matrix $(X \cdot 1_{m\times m} - A)^\vee$, we get $P(X)x_i = 0$ for all i, where $P \in R[X]$ is the characteristic polynomial of A, i.e. $P(x)M = \{0\}$. Since M is faithful as an $R[x]$-module, we get $P(x) = 0$. □

Corollary 3.1.3. *The integral elements in an R-subalgebra A form a subalgebra. In particular, A is integral over R if and only if it has a set of integral generators.*

Proof. Let $a, b \in A$ be integral elements. One readily checks that

- $R[a, b]$ is finitely generated as an R-module (say by certain monomials $a^i b^j$);
- $R[a, b]$ is faithful (as an $R[a, b]$-module) because it contains 1.

Thus $R[a, b]$ witnesses the integrality of $a+b$ and ab, since they both stabilize $R[a, b]$. □

Proposition 3.1.4. *Consider ring homomorphisms $R \to A \to B$ such that A is integral over R. If $y \in B$ is integral over A, then it is integral over R.*

Proof. Assume $y^n + a_{n-1}y^{n-1} + \cdots + a_0 = 0$ with $a_0, \dots, a_{n-1} \in A$ integral over R. The $R[a_0, \dots, a_{n-1}]$-module $R[a_0, \dots, a_{n-1}][y]$ is also finitely generated over R, faithful and preserved by y, hence it witnesses the integrality of y over R. □

This subalgebra of integral elements in A is called the *integral closure* of R in A. If the integral closure equals the image of R in A, we say R is *integrally closed* in A. The integral closure is automatically integrally closed by virtue of Proposition 3.1.4.

Definition 3.1.5. Let R be an integral domain and denote by K its field of fractions. The integral closure of R in K is called the *normalization* of R. The domain R is said to be *normal* if R is integrally closed in K.

The first examples of normal domains come from unique factorization domains (UFD) that you have seen in undergraduate algebra, including $\mathbb{Z}$, $\mathbb{Q}[X, Y]$, etc.

Proposition 3.1.6. *Unique factorization domains are normal.*

Proof. Given $x = r/s \in K$ with coprime $r, s \in R$. If there is an integral dependence relation $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, we will have $r^n + a_{n-1}r^{n-1}s + \cdots + a_0 s^n = 0$, hence $s \mid r^n$. As r is coprime to s, we see $s \in R^\times$ and $x \in R$. □

Let us show that taking integral closure commutes with localizations. Geometrically, this means that taking integral closure is a local operation on $\mathrm{Spec}(R)$.

Lemma 3.1.7. *Let A be an R-algebra, S be a multiplicative subset of R. Denote by $\tilde{R}$ the integral closure of R in A. Then the integral closure of $R[S^{-1}]$ in $A[S^{-1}]$ equals $\tilde{R}[S^{-1}]$.*

Proof. Suppose that $x \in A$ satisfies $x^n + \sum_{i=0}^{n-1} b_i x^i = 0$ with $b_0, \dots, b_{n-1} \in R$. For all $s \in S$ we deduce $\left(\frac{x}{s}\right)^n + \sum_{i=0}^{n-1} \frac{b_i}{s^{n-i}} \cdot \left(\frac{x}{s}\right)^i = 0$ in $A[S^{-1}]$. Therefore $\tilde{R}[S^{-1}]$ is in the integral closure of $R[S^{-1}]$ in $A[S^{-1}]$.

Conversely, suppose that $x/s \in A[S^{-1}]$ satisfies

$$\left(\frac{x}{s}\right)^n + \sum_{i=0}^{n-1} \frac{a_i}{s_i} \left(\frac{x}{s}\right)^i = 0, \quad a_i \in A,\ s_i \in S.$$

Cleaning denominators, we see that $xs_1 \cdots s_{n-1}$ is integral over R, hence $x = \frac{xs_1 \cdots s_{n-1}}{s_1 \cdots s_n} \in \tilde{R}[S^{-1}]$. □

In particular, localizations of a normal domain are still normal. We have the following converse.

Exercise 3.1.8. Let R be a domain. If for every maximal ideal $\mathfrak{m}$ of R we have $R_{\mathfrak{m}}$ is normal, then so is R itself. Hint: recall that $R = \bigcap_{\mathfrak{m}} R_{\mathfrak{m}}$ inside the fraction field K.

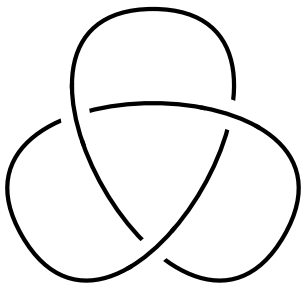
Exercise 3.1.9. Let $R := \mathbb{C}[X, Y]/(Y^2 - X^3)$. Show that

(i) R is a domain, or equivalently, $Y^2 - X^3$ is an irreducible polynomial;
(ii) the element $x := \bar{Y}/\bar{X} \in \mathrm{Frac}(R)$ does not lie in R, where $\bar{X}, \bar{Y}$ denote the images of $X, Y \in \mathbb{C}[X, Y]$;
(iii) show that $x^3 \in R$, therefore R is not a normal ring.

Remark 3.1.10. The rationale of the previous Exercise comes from singularity. Consider the *cuspidal curve* $C := \{(x, y) \in \mathbb{C}^2 : y^2 = x^3\}$. It has an isolated singularity at $(0, 0)$ since $\nabla(y^2 - x^3) = (0, 0)$ at the origin. On the other hand, it admits a (non-injective) parametrization from $\mathbb{C}$ by

$$t \mapsto (x = t^2, y = t^3).$$

Following Milnor [12], a nice way to understand the "cusp" at $(0, 0)$ is to cut C by a 3-sphere $S := \{(x, y) \in \mathbb{C}^2 : |x|^2 + |y|^2 = \epsilon\}$ enclosing the origin, with $0 < \epsilon \ll 1$. Writing the parametrization above as $t = re^{i\theta}$ in polar coordinates, we get the equation $r^4 + r^6 = \epsilon$ which has a unique positive root ρ. Hence $S \cap C$ is described by the closed curve $\theta \mapsto (\rho^2 e^{2i\theta}, \rho^3 e^{3i\theta})$ in $S \simeq \mathbb{S}^3$. We call $S \cap C$ the *link of singularity* at $(0, 0)$; in this case it is equivalent to the $(2, 3)$-torus knot, i.e. the *trefoil* shown below.



If we started from a non-singular curve in $\mathbb{C}^2$, the result would then be an unknotted $\mathbb{S}^1$ inside $\mathbb{S}^3$. In this sense the link provides a measure for the singularity.

Our study of normality has to be paused here. We refer to [13, §§8–9] for a beautiful discussion on the algebro-geometric content of normality, as well as important consequences such as Zariski's Main Theorem. Roughly speaking, normality means there is only one branch through each point of the corresponding variety.

3.2 Nullstellensatz

Our aim is to present a generalization of the celebrated *Nullstellensatz*, which is one of the cornerstones of algebraic geometry. We shall also write the nilpotent radical of a ring R as

$$\mathrm{nil}(R) := \sqrt{0_R}.$$

For an ideal $\mathfrak{a} \subset R$, we write $\mathfrak{a}[X]$ for the ideal of $R[X]$ formed by polynomials with all coefficients lying in $\mathfrak{a}$.

Definition 3.2.1. A ring R is called a *Jacobson ring* if every prime ideal $\mathfrak{p}$ satisfies

$$\mathfrak{p} = \bigcap_{\mathfrak{m}:\text{maximal ideal } \supset \mathfrak{p}} \mathfrak{m}. \tag{3–1}$$

Equivalently, we require that the Jacobson radical $\mathrm{rad}(R/\mathfrak{p}) = \mathrm{nil}(R/\mathfrak{p}) = \{0\}$ for all $\mathfrak{p}$. Note that $\supset$ always holds.

Observations:
- ◇ Quotients of Jacobson rings are still Jacobson.
- ◇ Fields are trivially Jacobson.

Exercise 3.2.2. Prove that every principal ideal domain (a domain in which every ideal is generated by one element) with infinitely many maximal ideals is Jacobson.

Theorem 3.2.3 (E. Snapper)**.** *For any R, the polynomial algebra $R[X]$ satisfies* $\mathrm{rad}(R[X]) = \mathrm{nil}(R[X])$.

Proof. To show that $\mathrm{nil}(R[X]) \supset \mathrm{rad}(R[X])$, let $f(X) = \sum_i a_i X^i \in \mathrm{rad}(R[X])$, then $1 + Xf(X) = 1 + \sum_i a_i X^{i+1} \in R[X]^\times$. By looking at the reduction modulo $\mathfrak{p}$ of $f(X)$ for every prime ideal $\mathfrak{p}$ of R, we see that $a_i \in \bigcap \mathfrak{p} = \mathrm{nil}(R)$ for all i. Hence $f(X) \in \mathrm{nil}(R)[X] \subset \mathrm{nil}(R[X])$. □

Lemma 3.2.4. *Let $R \subset A$ be integral domains such that A is a finitely generated R-algebra. If* $\mathrm{rad}(R) = \{0\}$, *then* $\mathrm{rad}(A) = \{0\}$.

Proof. We may assume that A is generated by a single element $a \in A$ over R. If a is transcendental over $K := \mathrm{Frac}(R)$, Theorem 3.2.3 above can be applied as $\mathrm{nil}(R[X]) = \{0\}$. Let us assume that a satisfies $f(a) = 0$ for some $f(X) = \sum_{i=0}^{n} r_i X^i \in R[X]$ with $r_n \neq 0$. Let $b \in \mathrm{rad}(A)$ and suppose $b \neq 0$. Hereafter we embed everything into the K-algebra $\mathrm{Frac}(A)$. Since a is algebraic over K, so is every element from $R[a]$ or even $K[a] \subset \mathrm{Frac}(A)$. Hence b is integral over K as well. By cleaning denominators, we

arrive at $g(b) = 0$ for some $g(X) = \sum_{i=0}^{m} s_i X^i \in R[X]$ with the smallest possible degree m. Since A is a domain, we have $s_0 \neq 0$.

Using $\mathrm{rad}(R) = \{0\}$, there exists a maximal ideal $\mathfrak{m}$ of R such that $r_n s_0 \notin \mathfrak{m}$. Taking localization at $\mathfrak{m}$, we get the subring $A' := A \otimes_R R_{\mathfrak{m}} \subset \mathrm{Frac}(A)$ containing $R_{\mathfrak{m}}$, and A' is also a finitely generated $R_{\mathfrak{m}}$-module since we inverted r_n. Nakayama's Lemma for $R_{\mathfrak{m}}$-modules implies $\mathfrak{m}A' \subsetneq A'$, thus $\mathfrak{m}A \subsetneq A$. Now choose a maximal ideal $\mathfrak{m}_A$ of A over $\mathfrak{m}$. We must have $\mathfrak{m}_A \cap R = \mathfrak{m}$, which entails $s_0 \notin \mathfrak{m}_A$. This is a contradiction since $s_0 = -\sum_{i=1}^{m} s_i b^i \in \mathrm{rad}(A)$. □

Theorem 3.2.5 (Nullstellensatz)**.** *Let A be a finitely generated R-algebra. Assume that R is a Jacobson ring, then the following statements hold.*

(*i*) *A is a Jacobson ring.*

(*ii*) *Let $\mathfrak{n} \in \mathrm{Spec}(A)$ be maximal, then its image $\mathfrak{m} \in \mathrm{Spec}(R)$ is maximal as well, and $A/\mathfrak{n}$ is a finite extension of the field $R/\mathfrak{m}$.*

Proof. We start with (i). One may assume $R \subset A$ from the outset. Condition (3–1) for A amounts to $\mathrm{rad}(A/\mathfrak{p}) = 0$ for every $\mathfrak{p} \in \mathrm{Spec}(A)$. Apply the previous Lemma to the integral domains $R/R \cap \mathfrak{p} \subset A/\mathfrak{p}$ to prove (i).

Now turn to (ii). Using (i) and induction, we may assume that $A = R[a]$ for some $a \in A$. By considering the homomorphism $R/\mathfrak{m} \hookrightarrow A/\mathfrak{n}$ between Jacobson rings, we may further reduce to the case $\mathfrak{n} = \{0\}$ and $\mathfrak{m} = \{0\}$, so that R is a domain embedded in the field A. In particular a cannot be transcendental (as $R[X]$ is not a field) and must satisfy $\sum_{i=0}^{n} c_i a^i = 0$ for some $c_0, \dots, c_n \in R$ with $c_n \neq 0$. Let $\mathfrak{k}$ be any maximal ideal of R not containing c_n, which exists since $\mathrm{rad}(R) = \{0\}$.

As in the proof of the previous Lemma, a becomes integral over $R_{\mathfrak{k}}$ and Nakayama's Lemma for $R_{\mathfrak{k}}$-modules entails $\mathfrak{k}A \neq A$, hence $\mathfrak{k} = 0$ because A is a field. This implies that R is a field and A is a finite extension of R. □

Corollary 3.2.6. *Let $\Bbbk$ be an algebraically closed field, and $A := \Bbbk[X_1, \dots, X_n]$. The maximal ideals of A are in bijection with $\Bbbk^n$ by attaching to each $x := (x_1, \dots, x_n) \in \Bbbk^n$ the ideal*

$$\mathfrak{m}_x = \{f \in A : f(x) = 0\} = (X_1 - x_1, \dots, X_n - x_n).$$

Proof. Since $A/\mathfrak{m}_x \xrightarrow{\sim} \Bbbk$ by evaluation at x, we see $\mathfrak{m}_x$ is indeed maximal. It is routine to show that $x = y \iff \mathfrak{m}_x = \mathfrak{m}_y$. It remains to show that every maximal ideal $\mathfrak{n}$ contains some $\mathfrak{m}_x$. Indeed, Theorem 3.2.5 implies the field $A/\mathfrak{n}$ is algebraic over $\Bbbk$, hence $A/\mathfrak{n} \simeq \Bbbk$ as $\Bbbk$-algebras. Let x_i be the image of X_i under $A \twoheadrightarrow A/\mathfrak{n} \xrightarrow{\sim} \Bbbk$ and set $x := (x_1, \dots, x_n)$, then $\mathfrak{n} \supset \mathfrak{m}_x$ as required. □

Corollary 3.2.7. *Keep the notations above and set*

$$Z(\mathfrak{a}) := \{x \in \Bbbk^n : \forall f \in \mathfrak{a},\ f(x) = 0\},$$
$$I(\mathcal{X}) := \{f \in A : \forall x \in X,\ f(x) = 0\}$$

for ideals $\mathfrak{a} \subset A$ and subsets $\mathcal{X} \subset \Bbbk^n$, then we have $IZ(\mathfrak{a}) = \sqrt{\mathfrak{a}}$ for all $\mathfrak{a}$.

If we identify $\Bbbk^n$ with $\mathrm{MaxSpec}(A)$ by the previous Corollary, then $Z(\mathfrak{a})$ is just the intersection of $V(\mathfrak{a}) \subset \mathrm{Spec}(A)$ and $\mathrm{MaxSpec}(A)$. Details are left to the readers.

Proof. If $f \in A$ and $f^n \in \mathfrak{a}$ for some n, the vanishing of f^n on $Z(\mathfrak{a})$ will entail that of f, hence the inclusion $\supset$ holds. Assume conversely that $f \in A$ vanishes on $Z(\mathfrak{a})$. This means: for every maximal ideal $\mathfrak{m}_x$ we have

$$\mathfrak{m}_x \supset \mathfrak{a} \iff x \in Z(\mathfrak{a}) \implies f(x) = 0 \iff f \in \mathfrak{m}_x.$$

Hence

$$f \in \bigcap_{\mathfrak{m}_x \supset \mathfrak{a}} \mathfrak{m}_x = \sqrt{\mathfrak{a}},$$

the last equality being based on Definition 3.2.1 since $A/\mathfrak{a}$ is a Jacobson ring. This concludes the $\subset$. □

Remark 3.2.8. How about $ZI(\mathcal{X})$? Unwinding definitions, it is seen to equal the set of points that "satisfy the algebraic equations that $\mathcal{X}$ satisfies." The Zariski topology on $\Bbbk^n$ is defined by stipulating the subsets $\{x \in \Bbbk^n : f(x) = 0\}$ to be closed, for all $f \in A$, so we obtain $ZI(\mathcal{X}) = \bar{\mathcal{X}}$, the Zariski-closure of $\mathcal{X}$. The reader is invited to verify that by identifying $\Bbbk^n$ with $\mathrm{MaxSpec}(A)$, the foregoing topology is induced from the Zariski topology on the prime spectrum $\mathrm{Spec}(A)$.

An (algebraic, closed) subvariety of $\Bbbk^n$ is the vanishing locus $f_1 = \cdots = f_m = 0$ for some $f_1, \ldots, f_m \in \Bbbk[X_1, \ldots, X_n]$; it is determined by the ideal $\mathfrak{a} = (f_1, \ldots, f_m)$, in fact it depends only on $\sqrt{\mathfrak{a}}$. An ideal $\mathfrak{a}$ is called *radical* if $\sqrt{\mathfrak{a}} = \mathfrak{a}$. To recap, we obtain a dictionary:

Subvariety $\mathcal{X}$ in $\Bbbk^n$	Radical ideal $\mathfrak{a}$ in $\Bbbk[X_1, \ldots, X_n]$
Points of $\mathcal{X}$	$\mathrm{MaxSpec}(A)$, $A = A_{\mathcal{X}} := \Bbbk[X_1, \ldots, X_n]/\mathfrak{a}$
Union of two varieties	product or intersection of two ideals
Intersection of varieties	sum of ideals
Polynomial map $\mathcal{X} \to \mathcal{Y}$	$\Bbbk$-homomorphism $A_{\mathcal{Y}} \to A_{\mathcal{X}}$
⋮	⋮

If one allows arbitrary rings A instead of just $\Bbbk[X_1, \ldots, X_n]/\mathfrak{a}$, and consider $\mathrm{Spec}(A)$ instead of $\mathrm{MaxSpec}(A)$ (the latter is well-behaved only for Jacobson rings), the result is the category of *affine schemes*. A proper treatment of these ideas should be left to the Algebraic Geometry course, if it exists.....

3.3 Flatness: the first glance

To begin with, we consider a ring A and a module N. It has been observed that the additive functor $N \underset{A}{\otimes} - : A\text{-}\mathsf{Mod} \to A\text{-}\mathsf{Mod}$ is *right exact*, namely it preserves the exactness of sequences like

$$\bullet \to \bullet \to \bullet \to 0.$$

If we consider exactness of sequences like $0 \to \bullet \to \bullet \to \bullet$, the corresponding notion is *left exactness*. The same applies to any additive functor F instead of $N \underset{A}{\otimes} -$. Being both

left and right exact is equivalent to that F preserves all exact sequences; in this case we say F is an *exact functor*.

Definition 3.3.1. We say N is a *flat* A-module if $N \underset{A}{\otimes} -$ is exact. We say N is *faithfully flat* if for every sequence $M_\bullet = [\cdots \to M_i \to M_{i-1} \to \cdots]$ of R-modules, we have $M_\bullet \underset{R}{\otimes} N$ is exact if and only if $M_\bullet$ is.

Remark 3.3.2. In view of the right-exactness of $\otimes$, to assure flatness of N it suffices that $N \underset{A}{\otimes} -$ preserves kernels.

Now we consider a ring homomorphism $A \to B$, which makes B into an A-algebra. Tensor product now gives an additive functor, often called the *base change*:

$$B \underset{A}{\otimes} - : A\text{-}\mathsf{Mod} \to B\text{-}\mathsf{Mod}.$$

Thus we can also talk about flatness and faithful flatness of B over A. Since B is naturally an A-module, this notion is compatible with the previous one.

Example 3.3.3. Let S be a multiplicative subset of A, then $A[S^{-1}]$ is flat over A. It is not faithfully flat in general, however; see Theorem 3.5.6.

Example 3.3.4. A routine fact is that for any family $\left(M_\bullet^{(i)}\right)_{i\in I}$ of complexes of A-modules, we have

$$\forall i \in I,\ M_\bullet^{(i)} \text{ is exact } \iff \bigoplus_{i\in I} M_\bullet^{(i)} \text{ is exact.}$$

Recall that $\otimes$ preserves direct sums. It follows that a direct sum of modules is flat if and only if each summand is flat. From this we deduce the flatness of free modules since $A \underset{A}{\otimes} M \simeq M$ functorially for each M. Furthermore, projective modules are flat as they are direct summands of free modules.

Exercise 3.3.5. Show that $\mathbb{Z}/n\mathbb{Z}$ is not flat over $\mathbb{Z}$ for $n > 1$.

We list some basic properties below.

▷ **Tensor products** Let M, N be flat (resp. faithfully flat) R-modules, then so is $M \underset{R}{\otimes} N$. This follows the associativity constraint of tensor products: $(- \otimes M) \otimes N \simeq - \otimes (M \otimes N)$.

▷ **Transitivity** Given ring homomorphisms $A \to B \to C$, if B is flat (resp. faithfully flat) over A and C is flat (resp. faithfully flat) over B, then C is also flat (resp. faithfully flat) over A. This follows from the transitivity of base change, namely there is a isomorphism of functors $A\text{-}\mathsf{Mod} \to C\text{-}\mathsf{Mod}$.

$$(- \underset{A}{\otimes} B) \underset{B}{\otimes} C \xrightarrow{\sim} - \underset{A}{\otimes} C.$$

▷ **Base change** Suppose N is a flat (resp. faithfully flat) A-module and B is any A-algebra, then $N \underset{A}{\otimes} B$ is a flat (resp. faithfully flat) B-module. Again, any B-module M can be viewed as an A-module, and there is a functorial isomorphism

$$(N \underset{A}{\otimes} B) \underset{B}{\otimes} M \xrightarrow{\sim} N \underset{A}{\otimes} M.$$

Remark 3.3.6. A sequence $[\cdots \to M_i \xrightarrow{d_i} M_{i-1} \to \cdots]$ of R-modules is a complex (resp. exact) if and only if so is its localization at $\mathfrak{m}$, for every maximal ideal $\mathfrak{m}$. Indeed:

- $(M_\bullet, d_\bullet)$ is a complex if and only if $\mathrm{im}(d_{i-1}d_i) = 0$ for all i. Since localization is an exact functor, it preserves images and we know a module N is zero if and only if $N_\mathfrak{m} = 0$ for all $\mathfrak{m}$.
- a complex $(M_\bullet, d_\bullet)$ is exact if and only if $\mathrm{H}_i(M_\bullet) = 0$ for all i. The same reasoning applies since localization preserves H_i.

Proposition 3.3.7. *The following are equivalent for an R-module N. (i) N is flat over R, (ii) $N_\mathfrak{p}$ is flat over $R_\mathfrak{p}$ for all prime ideal $\mathfrak{p}$, (iii) $N_\mathfrak{m}$ is flat over $R_\mathfrak{m}$ for all maximal ideal $\mathfrak{m}$.*

Proof. Direct consequence of the exactness of localization and Remark 3.3.6. □

Lemma 3.3.8. *Let $\varphi : R \to R'$ be a ring homomorphism, $\mathfrak{p}' \in \mathrm{Spec}(R')$ maps to $\mathfrak{p} \in \mathrm{Spec}(R)$ under $\varphi^\sharp$. If φ is flat, so is the induced homomorphism $R_\mathfrak{p} \to R'_{\mathfrak{p}'}$.*

Proof. Set $S = R \setminus \mathfrak{p}$ so that $\varphi(S) \subset R' \setminus \mathfrak{p}'$. Factorize $R_\mathfrak{p} \to R_{\mathfrak{p}'}$ as

$$R_\mathfrak{p} \to \underbrace{R'[\varphi(S)^{-1}]}_{\text{as a ring}} \to R'_{\mathfrak{p}'}.$$

The first arrow is also the base-change to $R_\mathfrak{p}$ of φ (as a homomorphism of R-modules), whereas the second one is a localization of R'. Their composite is therefore flat. □

Proposition 3.3.9. *Let $\varphi : R \to R'$ be a ring homomorphism. The following are equivalent:*

(i) *R' is flat over R,*

(ii) *$R'_{\mathfrak{p}'}$ is flat over $R_\mathfrak{p}$ for all $\mathfrak{p}' \in \mathrm{Spec}(R')$ with $\mathfrak{p} = \varphi^\sharp(\mathfrak{p}')$;*

(iii) Idem, *but for $\mathfrak{p}' \in \mathrm{MaxSpec}(R')$.*

Proof. (i) $\implies$ (ii): Set $S := R \setminus \mathfrak{p}$. Base change implies $R'[S^{-1}]$ is flat over $R[S^{-1}] = R_\mathfrak{p}$. Since $R'_{\mathfrak{p}'}$ is a localization of $R[S^{-1}]$ (exercise), we conclude by transitivity.

(ii) $\implies$ (iii): Trivial.

(iii) $\implies$ (i): By Remark 3.3.6 applied to complexes of R'-modules, it suffices to show the exactness of the functor $- \underset{R}{\otimes} R'_{\mathfrak{p}'}$ for all $\mathfrak{p}' \in \mathrm{MaxSpec}(R')$. In view of Lemma 3.3.8, the factorization of $R \to R'_{\mathfrak{p}'}$ into $R \to R_\mathfrak{p} \to R'_{\mathfrak{p}'}$ and the flatness of $R \to R_\mathfrak{p}$ show that $R'_{\mathfrak{p}'}$ is indeed flat over R. □

Lemma 3.3.10 (Equational criterion of flatness)**.** *An R-module N is flat if and only if for all $r \geq 1$, $a_1, \ldots, a_r \in R$, $x_1, \ldots, x_r \in N$ verifying $\sum_{i=1}^r a_i x_i = 0$, there exist $s \in \mathbb{Z}_{\geq 1}$, an R-valued matrix $B = (b_{ij})_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s}}$ and $y_1, \ldots, y_s \in N$ such that*

$$\begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = B \begin{pmatrix} y_1 \\ \vdots \\ y_s \end{pmatrix}, \quad \begin{pmatrix} a_1 & \cdots & a_r \end{pmatrix} B = 0.$$

Proof. Suppose M is flat and consider the exact sequence $0 \to \ker(f) \to R^{\oplus r} \xrightarrow{f} R$ where $f(t_1, \dots, t_r) = \sum_i a_i t_i$. We obtain an exact

$$0 \to \ker(f) \underset{A}{\otimes} M \to M^{\oplus r} \xrightarrow{(x_i)_i \mapsto \sum_i a_i x_i} M.$$

Thus if $(x_1, \dots, x_r) \mapsto 0$ by the arrow above, we can express it as $\sum_{j=1}^{s} (b_{1j}, \dots, b_{rj}) \otimes y_j \in \ker(f) \underset{A}{\otimes} M$ as required.

To show the converse, we invoke the fact that flatness is equivalent to the injectivity of $\mathfrak{a} \otimes N \to \mathfrak{a}N$ for all finitely generated ideal $\mathfrak{a}$. See Proposition 3.4.1. □

It will be useful to rephrase the condition in Lemma 3.3.10 as follows: for all
- ◇ homomorphism $x : R^{\oplus r} \to M$, where $r \in \mathbb{Z}_{\geq 1}$, and
- ◇ $K \subset \ker(x)$: submodule generated by one element,

there exist some $s \in \mathbb{Z}_{\geq 1}$ and a commutative diagram

$$\begin{array}{ccc} R^{\oplus r} & \xrightarrow{B} & R^{\oplus s} \\ & {\scriptstyle x}\searrow \quad \swarrow{\scriptstyle y} & \\ & M & \end{array} \qquad \text{s.t. } K \subset \ker(B).$$

Indeed, x (resp. y) corresponds to $(x_1, \dots, x_r)$ via $x : (t_1, \dots, t_r) \mapsto \sum_i t_i x_i$ (resp. $y : (u_1, \dots, u_s) \mapsto \sum_j u_j y_j$), and $K \subset \ker(x)$ corresponds to $R \cdot (a_1, \dots, a_r)$. The homomorphism B corresponds to the matrix $(b_{ij})_{i,j}$.

Remark 3.3.11. For flat N, the equational criterion so rephrased is applicable to any finitely generated $K \subset \ker(x)$. Indeed, one may iterate the construction for $R^{\oplus s} \xrightarrow{y} M$, etc. to make every generator of K mapped to 0.

3.4 Structure of flat modules

Recall from homological algebra that the right exact functor $N \underset{A}{\otimes} - : R\text{-Mod} \to R\text{-Mod}$ has $(\mathrm{Tor}_i^R(N, -))_{i \geq 0}$ as its left derived functors.

Proposition 3.4.1. *The following are equivalent for an R-module N:*

(*i*) *N is flat,*

(*ii*) $\mathrm{Tor}_i^R(N, -) = 0$ *for all* $i > 0$,

(*iii*) $\mathrm{Tor}_1^R(N, -) = 0$,

(*iv*) $\mathrm{Tor}_1^R(N, R/\mathfrak{a}) = 0$ *for all finitely generated ideal* $\mathfrak{a}$, *or equivalently* $\mathfrak{a} \underset{R}{\otimes} N \to N$ *is injective.*

Proof. First, the equivalence mentioned in (iv) is a consequence of the exact sequence

$$\underbrace{\mathrm{Tor}_1^R(N,R)}_{=0} \to \mathrm{Tor}_1^R(N,R/\mathfrak{a}) \to N \underset{R}{\otimes} \mathfrak{a} \to N \to N \underset{R}{\otimes} (R/\mathfrak{a}) \to 0$$

deduced from $0 \to \mathfrak{a} \to R \to R/\mathfrak{a} \to 0$.

Clearly (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii) $\Longrightarrow$ (iv). To show (iii) $\Longrightarrow$ (i), note that if $0 \to M' \to M \to M'' \to 0$ is exact, then $\mathrm{Tor}_1^R(N,M'') \to N \otimes M' \to N \otimes M \to N \otimes M'' \to 0$ is exact.

We show (iv) $\Longrightarrow$ (i), (ii) or (iii) as follows: $\mathrm{Tor}_1^R(N,M) = 0$ can be tested for finitely generated M only, since $\mathrm{Tor}_i^R(N,-)$ preserves filtered inductive limits such as

$$M = \varinjlim \{\text{f.g. submodules}\}.$$

We do induction on the minimal number n of generators of M. If $M = Rx_1 + \cdots + Rx_n$, put $M' := \sum_{i<n} Rx_i$ so that we have a short exact sequence $0 \to M' \to M \to M'' \to 0$ where M'' is generated by the image of x_n, hence isomorphic to some $R/\mathfrak{a}$. Since $\mathrm{Tor}_1^R(N,M') \to \mathrm{Tor}_1^R(N,M) \to \mathrm{Tor}_1^R(N,M'')$ is exact, we are reduced to the $n = 1$ case, i.e. $M = R/\mathfrak{a}$. It boils down to assure $\mathfrak{a} \otimes N \hookrightarrow N$. Again, using the exactness of filtered $\varinjlim$ and the fact that $\otimes$ respects $\varinjlim$, it suffices to test this on finitely generated $\mathfrak{a}$.

For a down-to-earth approach, see [8, §6.3]. □

Corollary 3.4.2. *If $r \in R$ is not a zero divisor, then r is not a zero divisor for any flat R-module N.*

Proof. Take $\mathfrak{a} := Rr$, which is $\simeq R$, and contemplate on $N \simeq \mathfrak{a} \underset{R}{\otimes} N \hookrightarrow N$. □

Exercise 3.4.3. Suppose R is a principal ideal domain. Show that N is flat if and only if N has no zero divisors except 0. Hint: the ideals take the form $\mathfrak{a} = (t)$, so the condition (iv) amounts to $tx = 0 \iff x = 0$.

Exercise 3.4.4. For all field $\Bbbk$, show that

(i) $\Bbbk[X,Y]/(XY - X)$ is not flat over $\Bbbk[X]$,

(ii) $\Bbbk[\![t]\!][Y,Z]/(YZ - t)$ is flat over $\Bbbk[\![t]\!]$.

Lemma 3.4.5. *Suppose $A \to B$ is flat. Write $M_B := B \underset{A}{\otimes} M$ for any A-module B. Then there are natural isomorphisms $\mathrm{Tor}_i^B(M_B,N_B) \simeq B \underset{A}{\otimes} \mathrm{Tor}_i^A(M,N)$ for all i.*

Proof. Take a projective resolution $0 \leftarrow M \leftarrow P_\bullet$ of A-modules. Since B is flat over A, its base-change $0 \leftarrow M_B \leftarrow P_{\bullet,B}$ to B is still a projective resolution; we are using the fact that base-change preserves projectivity. Hence $\mathrm{H}_i(P_{\bullet,B} \underset{B}{\otimes} N_B)$ computes $\mathrm{Tor}_i^B(M_B,N_B)$. On the other hand, by flatness the homology groups are equal to $\mathrm{H}_i(P_\bullet \underset{A}{\otimes} N) \underset{A}{\otimes} B$, that is, $\mathrm{Tor}_i^A(M,N) \underset{A}{\otimes} B$. We leave it to the reader to convince him- or herself that the isomorphism so constructed is natural.

Another way is to use to associativity and commutativity of tensor products on the derived level, namely the flatness of $A \to B$ implies

$$M_B \overset{\mathrm{L}}{\otimes}_B N_B \simeq (M \overset{\mathrm{L}}{\otimes}_A B) \overset{\mathrm{L}}{\otimes}_B (N \otimes_A B) \simeq (M \overset{\mathrm{L}}{\otimes}_A N) \overset{\mathrm{L}}{\otimes}_A B$$

in the derived categories, and it remains to take H_i. □

In particular, let $S \subset R$ be a multiplicative subset. By Example 3.3.3 we infer

$$\mathrm{Tor}_i^{R[S^{-1}]}\left(M[S^{-1}], N[S^{-1}]\right) \simeq \mathrm{Tor}_i^R(M,N)[S^{-1}].$$

Theorem 3.4.6. *Let R be a local ring with maximal ideal $\mathfrak{m}$. Let M be a finitely generated R-module. The following are equivalent:*

- *M is free,*
- *M is projective.*

If we assume moreover that M is finitely presented, both conditions are equivalent to the flatness of M.

Proof. Free modules are known to be projective. Now let M be finitely generated projective, and take a basis $\bar{x}_1, \dots \bar{x}_n$ of the $R/\mathfrak{m}$-vector space $M/\mathfrak{m}M$, together with liftings $M \ni x_i \mapsto \bar{x}_i$. Nakayama's Lemma then implies the surjectivity of

$$\begin{aligned} \Phi : R^{\oplus n} &\longrightarrow M \\ (a_1, \dots, a_n) &\longmapsto a_1 x_1 + \cdots + a_n x_n. \end{aligned}$$

As M is projective, Φ admits a section so that we may identify M with a direct summand of $R^{\oplus n}$, namely $M \oplus N = R^{\oplus n}$ for some N. Taking $- \otimes_R R/\mathfrak{m}$ leads to

$$(R/\mathfrak{m})^{\oplus n} = M/\mathfrak{m}M \oplus N/\mathfrak{m}N \quad \text{as vector spaces over } R/\mathfrak{m},$$

and by comparing dimensions we see $N/\mathfrak{m}N = \{0\}$, which in turn gives $N = \{0\}$ by Nakayama's Lemma (N is finitely generated since $R^{\oplus n} \twoheadrightarrow N$). Hence $M \simeq R^{\oplus n}$ is free.

Now turn to the second assertion. Projective modules are flat since they are direct summands of free modules, and it remains to show that every flat M with finite presentation $R^{\oplus q} \to R^{\oplus r} \xrightarrow{x} M \to 0$ is a direct summand of a free module. Let's plug $x : R^{\oplus r} \twoheadrightarrow M$ and $K := \ker(x)$ into the equational criterion of flatness (Lemma 3.3.10), rephrased as in Remark 3.3.11. Let N be the image of $B : R^{\oplus r} \to R^{\oplus s}$. One readily sees that y induces $N \xrightarrow{\sim} M$. This furnishes a section $s : M \to R^{\oplus s}$ for y. □

We deduce the following result characterizing finitely presented projective modules: in geometric language, they correspond to *vector bundles* over the *affine scheme* $\mathrm{Spec}(R)$.

Corollary 3.4.7. *Let M be a finitely presented R-module. Then M is projective if and only $M_\mathfrak{m}$ is free for every maximal ideal $\mathfrak{m}$.*

Proof. In view of Theorem 3.4.6, it suffices to show M is projective if and only if $M_\mathfrak{m}$ is for all maximal ideal $\mathfrak{m}$. One direction is easy: if M is a direct summand of a free module, then so is $M_\mathfrak{m}$.

Conversely, the assumption on finite presentation entails an isomorphism between additive functors R-Mod $\to R_\mathfrak{m}$-Mod

$$\mathrm{Hom}_R(M, -) \underset{R}{\otimes} R_\mathfrak{m} \simeq \mathrm{Hom}_{R_\mathfrak{m}}(M_\mathfrak{m}, (-)_\mathfrak{m}).$$

Hence $M_\mathfrak{m}$ is projective for all $\mathfrak{m}$ implies M is projective, by Remark 3.3.6 and the exactness of localizations. □

Note that for finitely presented M, the equivalence between projectivity and flatness holds for any ring R. The arguments are verbatim, and this can also be deduced from the local case.

We close this section by a stronger result, whose proof is referred to [8, Theorem A6.6].

Theorem 3.4.8 (Govorov–Lazard)**.** *An R-module is flat if and only if it is a filtered $\varinjlim$ of free R-modules.*

3.5 Faithful flatness and surjectivity

We begin by a contemplation on the definition of faithful flatness. Recall that R-Mod is the template of *abelian categories*, in which one can talk about the zero object 0, direct sums, kernels, cokernels, images and exactness.

We say a functor between categories is *faithful* if it induces injections on Hom-sets. A functor between additive categories is called *additive* if it induces group homomorphisms between Hom-sets. An additive functor between abelian categories is *exact* if it preserves all exact sequences. Exact functors preserve kernels, cokernels and images.

Lemma 3.5.1. *Let $F : \mathcal{C} \to \mathcal{C}'$ be an additive functor between abelian categories. The following are equivalent.*

(*i*) *F is exact and faithful;*

(*ii*) *F is exact and $(FM = 0 \iff M = 0)$ for every object M of $\mathcal{C}$;*

(*iii*) *a sequence $M' \to M \to M''$ is exact in $\mathcal{C}$ if and only if $FM' \to FM \to FM''$ is exact in $\mathcal{C}'$.*

Proof. (i) $\implies$ (ii): If $FM = 0$ then $F(\mathrm{id}_M) = \mathrm{id}_{FM} = 0$, and the faithfulness implies $\mathrm{id}_M = 0$ in $\mathrm{End}_{\mathcal{C}}(M)$; this is possible only when $M = 0$.

(ii) $\implies$ (i): Suppose $u : N \to M$ is mapped to 0 under F. Then we have $F(\mathrm{im}(u)) = 0$, thereby $\mathrm{im}(u) = 0$ and $u = 0$.

(i) $\implies$ (iii): Suppose $M' \xrightarrow{u} M \xrightarrow{v} M''$ induces an exact sequence $FM' \xrightarrow{Fu} FM \xrightarrow{Fv} FM''$. From $F(vu) = F(v)F(u) = 0$ we get $vu = 0$. Thus it makes sense to define $C := \ker(v)/\mathrm{im}(u)$. One has an exact sequence

$$\mathrm{im}(u) \to \ker(v) \to C \to 0.$$

Since F is exact, we deduce $FC = 0$, which implies $C = 0$ by (i) $\implies$ (ii).

(iii) $\implies$ (i): Suppose $u : N \to M$ is mapped to 0 under F. Consider $v : M \to \mathrm{coker}(u)$. Since F preserves exact sequences and Fv is an isomorphism, we see v is also an isomorphism, therefore $u = 0$. □

Proposition 3.5.2. *The following are equivalent for an R-module N.*

(*i*) *N is faithfully flat.*

(*ii*) *The functor $- \underset{R}{\otimes} N$ is exact and faithful.*

(*iii*) *N is flat and for every maximal ideal $\mathfrak{m}$ of R, we have $N/\mathfrak{m}N \simeq N \underset{R}{\otimes} R/\mathfrak{m} \neq 0$.*

Proof. The equivalence (i) $\iff$ (ii) has just been established. An R-module M is nonzero if and only if there exist exact sequences

$$0 \to R/\mathfrak{a} \to M, \quad R/\mathfrak{a} \to R/\mathfrak{m} \to 0$$

where $\mathfrak{a}$ is a proper ideal and $\mathfrak{m}$ is a maximal over-ideal of $\mathfrak{a}$. Next, let's show (iii) $\implies$ (i) or (ii): there are exact sequences

$$0 \to T \to M \underset{R}{\otimes} N, \quad T \to M \underset{R}{\otimes} (R/\mathfrak{m}) \to 0$$

where $T := (R/\mathfrak{a}) \underset{R}{\otimes} N$, therefore $M \underset{R}{\otimes} N \neq 0$ and we apply Lemma 3.5.1. Finally, (i) or (ii) $\implies$ (iii) is clear. □

Corollary 3.5.3. *Let $R \to R'$ be a local homomorphism[1] between local rings and let M be a finitely generated R'-module, $M \neq 0$. Then as an R-module, M is faithfully flat if and only if it is flat.*

Proof. Let $\mathfrak{m}, \mathfrak{m}'$ be the maximal ideals of R, R', respectively. Since $\mathfrak{m}$ is mapped into $\mathfrak{m}' = \mathrm{rad}(R')$, the assertion follows from Proposition 3.5.2 together with Nakayama's Lemma. □

This is often applied to the cases $R = R'$ or $M = R'$.

Exercise 3.5.4 (Faithfully flat descent for flatness)**.** Given a faithfully flat homomorphism $\varphi : R \to R'$. If M is an R-module such that $M \underset{R}{\otimes} R'$ is a flat (resp. faithfully flat) R'-module, then so is M over R.

Proposition 3.5.5. *Suppose $\varphi : A \to B$ is a faithfully flat ring homomorphism and regard B as an A-algebra.*

- *For any A-module M, the natural map $M \to M \underset{A}{\otimes} B$ is injective; in particular, φ is seen to be injective by taking $M = A$.*
- *For any ideal $\mathfrak{a} \subsetneq A$ we have $\varphi^{-1}(\mathfrak{a}B) = \mathfrak{a}$.*
- *The map $\varphi^\sharp : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective.*

Proof. Let N be the kernel of $M \to M \underset{A}{\otimes} B$. The B-module homomorphism $N \underset{A}{\otimes} B \to M \underset{A}{\otimes} B$ is injective by flatness; it is zero on $N \otimes 1$, hence identically zero and we obtain $N = \{0\}$ by faithful flatness (Lemma 3.5.1).

Let $\mathfrak{a} \subset A$ be a proper ideal. The previous step with $M := A/\mathfrak{a}$ implies that $A/\mathfrak{a} \to (A/\mathfrak{a}) \underset{A}{\otimes} B \simeq B/\mathfrak{a}B$ is injective, hence $\varphi^{-1}(\mathfrak{a}B) = \mathfrak{a}$.

To show the surjectivity of $\varphi^\sharp$, consider a given $\mathfrak{p} \in \mathrm{Spec}(A)$ and form the faithfully flat ring homomorphism

$$\varphi_\mathfrak{p} : A_\mathfrak{p} \to B \underset{A}{\otimes} A_\mathfrak{p} = B_\mathfrak{p}$$

[1] That is, the preimage of the maximal ideal $\mathfrak{m}_{R'}$ equals $\mathfrak{m}_R$.

by base change. The previous step implies $\varphi_{\mathfrak{p}}^{-1}(\mathfrak{p}B_{\mathfrak{p}}) = \mathfrak{p}A_{\mathfrak{p}}$, hence $\mathfrak{p}B_{\mathfrak{p}}$ is a proper ideal of $B_{\mathfrak{p}}$. Any maximal over-ideal $\mathfrak{m}_0$ of $\mathfrak{p}B_{\mathfrak{p}}$ satisfies $\varphi_{\mathfrak{p}}^{-1}(\mathfrak{m}_0) = \mathfrak{p}A_{\mathfrak{p}}$. Take $\mathfrak{m} \in \mathrm{Spec}(B)$ mapping to $\mathfrak{m}_0$. From the commutative diagrams

$$\begin{array}{ccc} B & \longrightarrow & B_{\mathfrak{p}} \\ {\scriptstyle\varphi}\uparrow & & \uparrow{\scriptstyle\varphi_{\mathfrak{p}}} \\ A & \longrightarrow & A_{\mathfrak{p}} \end{array} \qquad \begin{array}{ccc} \mathrm{Spec}(B) & \longleftarrow & \mathrm{Spec}(B_{\mathfrak{p}}) \\ {\scriptstyle\varphi^\sharp}\downarrow & & \downarrow{\scriptstyle\varphi_{\mathfrak{p}}^\sharp} \\ \mathrm{Spec}(A) & \longleftarrow & \mathrm{Spec}(A_{\mathfrak{p}}) \end{array}$$

one infers $\varphi^\sharp(\mathfrak{m}) = \mathfrak{p}$. □

Theorem 3.5.6. *The following are equivalent for a ring homomorphism $\varphi : A \to B$.*

(*i*) *φ is faithfully flat;*

(*ii*) *φ is flat and $\varphi^\sharp : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective;*

(*iii*) *φ is flat and for any maximal ideal $\mathfrak{p} \subset A$ there exists a maximal ideal $\mathfrak{m} \subset B$ such that $\varphi^{-1}(\mathfrak{m}) = \mathfrak{p}$.*

Proof. (i) $\Longrightarrow$ (ii) is contained in Proposition 3.5.5. As for (ii) $\Longrightarrow$ (iii), take any $\mathfrak{q} \in \mathrm{Spec}(B)$ that pulls back to $\mathfrak{p} \in \mathrm{Spec}(A)$, then any maximal over-ideal $\mathfrak{m}$ of $\mathfrak{q}$ also pulls back to $\mathfrak{p}$. To show (iii) $\Longrightarrow$ (i), apply the criterion of Proposition 3.5.2: for any $\mathfrak{p} \in \mathrm{MaxSpec}(A)$, the existence of $\mathfrak{m} \mapsto \mathfrak{p}$ implies $\mathfrak{m} \supset \varphi(\mathfrak{p}) \cdot B = \mathfrak{p}B$, hence $\mathfrak{p}B \neq B$. □

The notion of flatness was first introduced by J.-P. Serre in [15]. The surjections $\varphi^\sharp : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ (or rather their global avatars) for faithfully flat $\varphi : A \to B$ are often employed as candidates of "coverings" in algebraic geometry, leading up to the well-known *fpqc* (faithfully flat + quasi-compact) and *fppf* (faithfully flat + finitely presented) topologies in the sense of Grothendieck. They have been indispensable tools for contemporary geometers; [17] serves as a readable introduction to this circle of ideas.

Lecture 4

Going-up, going-down, gradings and filtrations

This lecture will be less self-contained than the other ones.

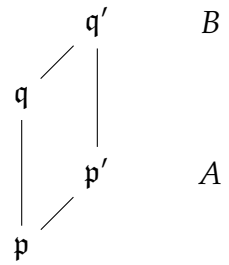
4.1 Going-up and going-down

In geometry, it is often crucial to know properties of a morphism between algebraically defined geometric objects. Rephrased in terms of commutative algebra, our goal is to understand the image of $\varphi^\sharp : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ where $\varphi : A \to B$ is a given ring homomorphism.

- We say the *going-up* property holds for φ if for every $\mathfrak{p} \subset \mathfrak{p}'$ in $\mathrm{Spec}(A)$ and $\mathfrak{q} \in \mathrm{Spec}(B)$ with $\varphi^\sharp(\mathfrak{q}) = \mathfrak{p}$ (and we say $\mathfrak{q}$ *lies over* $\mathfrak{p}$...) there exists $\mathfrak{q}' \supset \mathfrak{q}$ lying over $\mathfrak{p}'$.

- We say the *going-down* property holds for φ if for every $\mathfrak{p} \subset \mathfrak{p}'$ in $\mathrm{Spec}(A)$ and $\mathfrak{q}' \in \mathrm{Spec}(B)$ lying over $\mathfrak{p}'$, there exists $\mathfrak{q} \subset \mathfrak{q}'$ lying over $\mathfrak{p}$.

Pictorially:



Lemma 4.1.1 (Existence of minimal over-primes)**.** *Let $\mathfrak{a}$ be a proper ideal in a ring R. There exists a prime ideal $\mathfrak{p}$ which is minimal among all primes containing $\mathfrak{a}$. If $\mathfrak{P}$ is an ideal containing $\mathfrak{a}$, one can choose $\mathfrak{p} \subset \mathfrak{P}$.*

Proof. One easily reduces to the case $\mathfrak{a} = \{0\}$. We want to use Zorn's Lemma to find a minimal prime. It boils down to show that any chain $(\mathfrak{p}_i)_{i\in I}$ of prime ideals (I: totally ordered set with $j > i \implies \mathfrak{p}_i \supset \mathfrak{p}_j$) has a lower bound; we assume $\mathfrak{p}_i \subset \mathfrak{P}$ when $\mathfrak{P}$ is prescribed. It suffices to show $\mathfrak{p} := \bigcap_{i\in I} \mathfrak{p}_i$ is prime: if $xy \in \mathfrak{p}$ but there exists i with $x \notin \mathfrak{p}_i$, then $x \notin \mathfrak{p}_j$ whenever $j \geq i$; in this case $j \geq i \implies y \in \mathfrak{p}_j$. This entails $y \in \mathfrak{p}$. □

Lemma 4.1.2. *The going-down property for φ is equivalent to the following: for every $\mathfrak{p} \in \operatorname{Spec}(A)$ with $\varphi(\mathfrak{p})B \neq B$ and any minimal over-prime $\mathfrak{q}$ of $\varphi(\mathfrak{p})B$, we have $\varphi^\sharp(\mathfrak{q}) = \mathfrak{p}$.*

Proof. Assuming going-down for φ, let $\mathfrak{p}, \mathfrak{q}$ be as above. Evidently $\varphi^\sharp(\mathfrak{q}) \supset \varphi^{-1}(\varphi(\mathfrak{p})B) \supset \mathfrak{p}$. If we have $\supsetneq$, then going-down guarantees the existence of $\mathfrak{q}^\flat \subsetneq \mathfrak{q}$ lying over $\mathfrak{p}$. Thus $\varphi^{-1}(\mathfrak{q}^\flat) = \mathfrak{p}$ implies $\mathfrak{q}^\flat \supset \varphi(\mathfrak{p})B$, contradicting the minimality of $\mathfrak{q}$.

To show the converse, consider $\mathfrak{p} \subset \mathfrak{p}'$ with $\mathfrak{q}'$ lying over $\mathfrak{p}'$. We have $\varphi(\mathfrak{p})B \subset \varphi(\mathfrak{p}')B \subset \mathfrak{q}' \neq B$. Take $\mathfrak{q}$ to be a minimal over-prime of $\varphi(\mathfrak{p})B$ (which exists by Lemma 4.1.1) to verify the going-down property. □

Theorem 4.1.3. *Going-down holds for flat $\varphi : A \to B$.*

Proof. Consider $\mathfrak{p} \subset \mathfrak{p}'$ and $\mathfrak{q}'$ lying over $\mathfrak{p}'$ in the setting of going-down. First, $B_{\mathfrak{q}'}$ is flat over $A_{\mathfrak{p}'}$ by Proposition 3.3.9. Secondly, $A_{\mathfrak{p}'} \to B_{\mathfrak{q}'}$ is faithfully flat since it is local by Theorem 3.5.6 (iii), therefore induces a surjection on spectra. Take any prime of $B_{\mathfrak{q}'}$ mapping to $\mathfrak{p}A_{\mathfrak{p}} \in \operatorname{Spec}(A_{\mathfrak{p}'})$ and to $\mathfrak{q} \in \operatorname{Spec}(B)$. In view of the commutative diagrams

$$\begin{array}{ccc} B & \longrightarrow & B_{\mathfrak{q}'} \\ {\scriptstyle\varphi}\uparrow & & \uparrow{\scriptstyle\varphi_{\mathfrak{p}'}} \\ A & \longrightarrow & A_{\mathfrak{p}'} \end{array} \qquad \begin{array}{ccc} \operatorname{Spec}(B) & \longleftarrow & \operatorname{Spec}(B_{\mathfrak{q}'}) \\ {\scriptstyle\varphi^\sharp}\downarrow & & \downarrow{\scriptstyle\varphi^\sharp_{\mathfrak{p}'}} \\ \operatorname{Spec}(A) & \longleftarrow & \operatorname{Spec}(A_{\mathfrak{p}'}) \end{array}$$

we see $\mathfrak{q}$ is the required prime in going-down. □

Theorem 4.1.4 (Krull–Cohen–Seidenberg)**.** *Suppose the ring B is integral over its subring A. The following holds.*

(*i*) *The map $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ given by $\mathfrak{q} \mapsto \mathfrak{q} \cap A$ is surjective.*

(*ii*) *There are no inclusion relations in any fiber of $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$.*

(*iii*) *Going-up holds for $A \hookrightarrow B$.*

(*iv*) *If A is a local ring and $\mathfrak{p} \in \operatorname{MaxSpec}(A)$, then the fiber $\{\mathfrak{q} : \mathfrak{q} \cap A = \mathfrak{p}\}$ equals $\operatorname{MaxSpec}(B)$.*

(*v*) *Assume A, B are domains and A is normal. Then going-down holds for $A \hookrightarrow B$.*

(*vi*) *Assume furthermore that B is the integral closure of A in a normal field extension $L \supset K := \operatorname{Frac}(A)$, then $\Gamma := \operatorname{Aut}(L/K)$ acts transitively on each fiber of $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$.*

The last assertion should be familiar to readers with a background in algebraic number theory.

Proof. (iv): Let $\mathfrak{q} \in \mathrm{MaxSpec}(B)$ and $\mathfrak{p}_0 := \mathfrak{q} \cap A$. We know $B/\mathfrak{q}$ is a field, integral over its subring $A/\mathfrak{p}_0$. We claim that $A/\mathfrak{p}_0$ is also a field, therefore $\mathfrak{p}_0 = \mathfrak{p}$. Let $x \in A/\mathfrak{p}_0 \setminus \{0\}$. Its inverse in $B/\mathfrak{q}$ satisfies an integral relation $(\frac{1}{x})^n + a_{n-1}(\frac{1}{x})^{n-1} + \cdots + a_0 = 0$ over $A/\mathfrak{p}_0$. Multiplying both sides by x^{n-1} yields $\frac{1}{x} \in (A/\mathfrak{p}_0)[x]$.

Conversely, we have to show any $\mathfrak{q} \in \mathrm{Spec}(B)$ with $\mathfrak{q} \cap A = \mathfrak{p}$ is maximal. Again, there is an integral extension of domains $A/\mathfrak{p} \hookrightarrow B/\mathfrak{q}$. Consider $y \in B/\mathfrak{q}$ satisfying $y^n + a_{n-1}y^{n-1} + \cdots + a_0 = 0$, with the smallest possible n. If $y \neq 0$ then $a_0 \neq 0$. Since $A/\mathfrak{p}$ is a field, the recipe to produce $y^{-1} \in (A/\mathfrak{p})[y]$ is well-known.

(i), (ii): Fix $\mathfrak{p}$ and consider the inclusion $A_{\mathfrak{p}} \hookrightarrow B_{\mathfrak{p}} = B \underset{A}{\otimes} A_{\mathfrak{p}}$ which is still integral (note that $A \setminus \mathfrak{p}$ is a multiplicative subset of B, and $B_{\mathfrak{p}}$ is nonzero). We are reduced to the case A is local with maximal ideal $\mathfrak{p}$. By (iv) the fiber of $\mathfrak{p}$ in $\mathrm{Spec}(B)$ is nothing but $\mathrm{MaxSpec}(B)$. This establishes (i) and (ii) since there are no inclusions among maximal ideals.

(iii): Consider $\mathfrak{p} \subset \mathfrak{p}'$ and $\mathfrak{q}$ over $\mathfrak{p}$ in the setting of going-up. Then (i) is applicable to $A/\mathfrak{p} \hookrightarrow B/\mathfrak{q}$ and yields the required $\mathfrak{q}' \in \mathrm{Spec}(B/\mathfrak{q}) \hookrightarrow \mathrm{Spec}(B)$.

(vi): Observe that every $\sigma \in \Gamma$ induces an A-automorphism of B. Let $K' := L^{\Gamma}$. By (infinite) Galois theory we know L/K' is Galois and K'/K is purely inseparable. Let A' be the integral closure of A in K'. First observe that

$$\mathrm{Spec}(A') \longrightarrow \mathrm{Spec}(A), \quad \mathfrak{p}' \mapsto \mathfrak{p} = \mathfrak{p}' \cap A$$

is a bijection. Indeed, $K' \neq K$ only when $p := \mathrm{char}(K) > 0$, in which case the inverse is given by $\mathfrak{p}' = \left\{t \in A' : t^{p^m} \in \mathfrak{p},\ m \gg 0\right\}$. Thus we assume henceforth that L/K is Galois.

Deal with the case $[L : K] < \infty$ first. Consider $\mathfrak{q}, \mathfrak{q}' \in \mathrm{Spec}(B)$ in the fiber over $\mathfrak{p}$. Suppose on the contrary that $\Gamma\mathfrak{q}$ does not meet $\mathfrak{q}'$, then by (ii) we have $\mathfrak{q}' \not\subset \sigma(\mathfrak{q})$ for each $\sigma \in \Gamma$. By the prime avoidance (Proposition 1.1.5), there exists $x \in \mathfrak{q}' \setminus \bigcup_{\sigma} \sigma(\mathfrak{q})$, since Γ is finite. Now define the norm $y := N_{L/K}(x) \in K$, which is some positive power (namely $[L : K]_i$) of $\prod_{\sigma\in\Gamma} \sigma(x)$, hence belongs to B. Notice that

- A normal implies $y \in A$;
- $x \notin \sigma^{-1}(\mathfrak{q})$ for all $\sigma \in \Gamma$ implies $y \notin \mathfrak{p}$;
- however $y \in \mathfrak{q}' \cap A = \mathfrak{p}$ since $x \in \mathfrak{q}'$. Contradiction.

Now suppose $[L : K]$ is infinite and $\mathfrak{q}, \mathfrak{q}'$ in the fiber over $\mathfrak{p}$. We need to use the Krull topology on Γ. For every finite, Galois subextension E/K of L/K, define the set

$$\mathcal{T}(E) := \{\sigma \in \Gamma : \sigma(\mathfrak{q} \cap E) = \mathfrak{q}' \cap E\}.$$

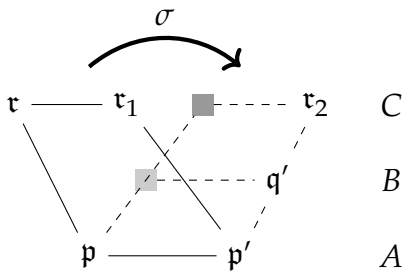
By the finite case we know $\mathcal{T}(E) \neq \emptyset$. Furthermore,

- $\mathcal{T}(E)$ is closed in Γ (it is the preimage of some subset of $\mathrm{Gal}(E/K)$);
- $E' \subset E \implies \mathcal{T}(E') \supset \mathcal{T}(E)$;
- the intersection of all $\mathcal{T}(E)$ is nonempty (by the compactness of Γ and the previous step).

Taking $\sigma \in \bigcap_E \mathcal{T}(E)$ gives $\sigma(\mathfrak{q}) = \mathfrak{q}'$.

(v): Define $L_0 := \mathrm{Frac}(B)$ and $K := \mathrm{Frac}(A)$. Then L_0/K is algebraic and we may take a normal closure L of L_0 over K. Let C be the integral closure of A (thus of B) in L. Consider the setting $\mathfrak{p} \subset \mathfrak{p}'$ and $\mathfrak{q} \cap A = \mathfrak{p}$ of going-down. Take any $\mathfrak{r} \in \mathrm{Spec}(C)$ mapping to $\mathfrak{p}$. By (iii) for $A \to C$ we obtain $\mathfrak{r}_1 \in \mathrm{Spec}(C)$ such that $\mathfrak{r}_1 \mapsto \mathfrak{p}'$ and

$\mathfrak{r}_1 \supset \mathfrak{r}$. Next, take $\mathfrak{r}_2 \in \operatorname{Spec}(C)$ mapping to $\mathfrak{q}'$; by (vi) there exists $\sigma \in \operatorname{Aut}(L/K)$ with $\sigma(\mathfrak{r}_1) = \mathfrak{r}_2$. One can check that $\mathfrak{q} := \sigma(\mathfrak{r}) \cap B$ is the required prime ideal. Explained pictorially:



we first construct $\mathfrak{r}$ and then $\mathfrak{r}_1$ by going-up, then "tilt" it via some σ to match $\mathfrak{r}_1$ with some chosen $\mathfrak{r}_2$ above $\mathfrak{q}'$, so that $\sigma(\mathfrak{r}) \cap B$ produces the required going-down: □

Exercise 4.1.5. Let $A \subset B$ be an integral extension of rings. Show that $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is a closed map (Cf. Proposition 4.2.1.) Hint: Let $\mathfrak{b} \subset B$ be a proper ideal, then $A/\mathfrak{b}\cap A \hookrightarrow B/\mathfrak{b}$ is still integral. Reduce the problem to showing that $V(\{0_B\}) = \operatorname{Spec}(B)$ has closed image in $\operatorname{Spec}(A)$.

4.2 Subsets in the spectrum

Proposition 4.2.1. *Let $\varphi : A \to B$ be a ring homomorphism with going-up property and suppose B is Noetherian. Then $\varphi^\sharp : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is a closed map: it maps closed subsets to closed subsets.*

Proof. Consider a closed subset $V(\mathfrak{b})$ of $\operatorname{Spec}(B)$. First, every $\mathfrak{q} \in \operatorname{Spec}(B)$ with $\mathfrak{q} \supset \mathfrak{b}$ lies over a minimal over-prime of $\mathfrak{b}$, by Lemma 4.1.1. Secondly, B is Noetherian implies $\operatorname{Ass}(B/\mathfrak{b})$ is finite; in particular there are only finitely many minimal over-primes $\mathfrak{q}_1, \dots, \mathfrak{q}_n$ of $\mathfrak{b}$.

Set $\mathfrak{p}_i := \varphi^\sharp(\mathfrak{q}_i)$ for all i. By going-up, $V(\mathfrak{p}_i)$ is contained in $\varphi^\sharp(V(\mathfrak{b}))$. On the other hand, every $\mathfrak{p} = \varphi^\sharp(\mathfrak{q})$ with $\mathfrak{q} \in V(\mathfrak{b})$ lies over some $\mathfrak{p}_i = \varphi^\sharp(\mathfrak{q}_i)$ by the foregoing discussion. This shows $\varphi^\sharp(V(\mathfrak{b})) = \bigcup_{i=1}^n V(\mathfrak{p}_i)$ is closed. □

Corollary 4.2.2. *Suppose B is Noetherian and integral over a subring A. Then $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is a closed surjection with finite fibers.*

Proof. Apply Theorem 4.1.4 with Proposition 4.2.1 to show that $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is closed and surjective.

To show the finiteness of the fiber over $\mathfrak{p} \in \operatorname{Spec}(A)$, note that the preimage of $V(\mathfrak{p})$ in $\operatorname{Spec}(B)$ equals $V(\mathfrak{p}B)$. Since there are no inclusions in the fiber over $\mathfrak{p}$, every element in that fiber must be a minimal over-prime of $\mathfrak{p}B$. We have seen in the proof of Proposition 4.2.1 that there are only finitely many such minimal-over primes. □

Note that the "closed surjection" part applies to any integral extension of rings. See Exercise 4.1.5.

In order to obtain further results of this type, we have to introduce more notions. Let R be a ring.

Definition 4.2.3. For $\mathfrak{p}, \mathfrak{p}' \in \operatorname{Spec}(R)$ satisfying $\mathfrak{p} \subset \mathfrak{p}'$, we say $\mathfrak{p}$ is a *generalization* of $\mathfrak{p}'$, and $\mathfrak{p}'$ is a *specialization* of $\mathfrak{p}$.

To make geometric meaning from it, being "specialized" signifies that there are "more equations" in $\mathfrak{p}'$, therefore it corresponds a smaller embedded geometric object. For example, in $R = \mathbb{C}[X, Y]$ the prime ideal (X, Y) is a specialization of (X), as the origin $X = Y = 0$ belongs to the line $X = 0$.

Lemma 4.2.4. *With respect to the Zariski topology, $\mathfrak{p}$ is a generalization of $\mathfrak{p}'$ if and only if $\mathfrak{p}' \in \overline{\{\mathfrak{p}\}}$.*

Proof. The condition $\mathfrak{p}' \in \overline{\{\mathfrak{p}\}}$ means that for every ideal $\mathfrak{a}$, if $\mathfrak{p} \supset \mathfrak{a}$ then $\mathfrak{p}' \supset \mathfrak{a}$. Taking $\mathfrak{a} = \mathfrak{p}$ yields $\mathfrak{p}' \supset \mathfrak{p}$, and the converse is even easier. □

A subset is called stable under specialization (resp. generalization) if the specialization (resp. generalization) of any member still belongs to that set. The following is straightforward.

Lemma 4.2.5. *Any closed subset is stable under specialization; any open subset is stable under generalization.*

Definition 4.2.6. Suppose R is Noetherian. A subset is called *locally closed* if it is the intersection of an open with a closed subset, called *constructible* if it is a finite union of locally closed subsets.

Closed subsets of the form $V(\mathfrak{p})$, where $\mathfrak{p} \in \operatorname{Spec}(R)$, are called *irreducible*; in this case we call $\mathfrak{p}$ the *generic point* of Z, which is uniquely characterized as the point which generalizes every member of Z.

- The foregoing definition is standard only for R Noetherian. The general definition in EGA differs.
- These notions can be applied to any topological space X. In practice one usually suppose X to be
  - *Noetherian*: the closed subsets satisfy descending chain condition,
  - *sober*: every irreducible has a generic point,

  in order to get interesting results. This explains our Noetherian assumption.
- If $\Bbbk$ is algebraically closed, $R = \Bbbk[X_1, \dots, X_n]/\mathfrak{a}$ corresponds to an affine algebraic variety $\mathcal{X} \subset \Bbbk^n$ and we work with $\operatorname{MaxSpec}(R)$ instead of $\operatorname{Spec}(R)$, then a subset $E \subset \mathcal{X}$ being locally closed means that it can be defined by a formula using the usual language of algebraic operations over $\mathbb{C}$, with coordinate variables $X_1, \dots, X_n$ and the symbols $=, \neq$, but *without using the quantifiers* $\exists, \forall$. For example, the formula

  $$(\neg X = 0) \vee (X = 0 \wedge Y = 0)$$

  defines the constructible subset $E := \{(x, y) \in \Bbbk^2 : x \neq 0\} \cup \{(0, 0)\}$, which is neither closed nor open. Note that E is the image of the polynomial map $\Bbbk^2 \to \Bbbk^2$ given by $(x, y) \mapsto (x, xy)$.

Exercise 4.2.7. Show that the set of constructible subsets is stable under finite $\cup$, finite $\cap$ and taking complements.

Exercise 4.2.8. Show that irreducible closed subsets Z admit the following topological characterization: if $X = A \cup B$ with A, B closed, then either $X = A$ or $X = B$.

Suppose R is Noetherian. Given any closed subset $Z \subset \operatorname{Spec}(R)$, we may write $Z = Z_1 \cup \cdots \cup Z_n$ with each Z_i irreducible. One way to do this is to use the primary decomposition for $\mathfrak{a}$, where we assume $Z = V(\mathfrak{a})$; then $Z_1, \ldots, Z_n$ will correspond to the minimal elements in $\operatorname{Ass}(R/\mathfrak{a})$. One can show by purely topological means that such an irreducible decomposition is unique if we require $i \neq j \implies Z_i \not\subset Z_j$. See [10, I.1.5].

Lemma 4.2.9. *Let E be a subset of $\operatorname{Spec}(R)$ where R is a Noetherian ring. The following are equivalent:*

(*i*) *E is constructible;*

(*ii*) *for every irreducible subset Z of $\operatorname{Spec}(R)$, either $Z \cap E$ is not dense in Z or $Z \cap E$ contains a nonempty open subset of Z.*

Proof. Omitted. See [11, (6.C)]. □

Theorem 4.2.10 (C. Chevalley)**.** *Let $\varphi : A \to B$ be a ring homomorphism such that A is Noetherian and B is a finitely generated A-algebra. Then $\varphi^\sharp$ maps constructible subsets to constructible subsets.*

Proof. Omitted. See [11, (6.E)]. □

Now we can give a partial converse to Lemma 4.2.5, albeit not in the strongest form.

Proposition 4.2.11. *Suppose R is Noetherian and E is a constructible subset of $\operatorname{Spec}(R)$. If E is stable under specialization (resp. generalization), then E is closed (resp. open) in $\operatorname{Spec}(R)$.*

Proof. It suffices to treat the specialization-stable case by taking complements. Write the Zariski-closure $\bar{E}$ as a finite union of irreducibles components Z, without inclusion relations. For each irreducible component Z, notice that $Z \cap E$ is dense in Z for all Z, since otherwise $\bar{E} = \overline{\bigcup_Z (Z \cap E)} = \bigcup_Z \overline{Z \cap E}$ would lead to another irreducible decomposition. Thus $Z \cap E$ contains a nonempty open of Z by Lemma 4.2.9. This open subset of E must contain the generic point of Z. As E is stable under specialization, we obtain $Z \subset E$. This being true for all Z, we deduce that $E = \bar{E}$. □

Proposition 4.2.12. *Consider a ring homomorphism $\varphi : A \to B$ satisfying going-down. Suppose A is Noetherian and B is a finitely generated A-algebra, then $\varphi^\sharp : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is an open map.*

Proof. Let $U = \operatorname{Spec}(B) \setminus V(\mathfrak{a})$ be an open subset. Going-down implies that $\varphi^\sharp(U)$ is stable under generalization. It suffices to show $\varphi^\sharp(U)$ is constructible, and this is the content of Chevalley's Theorem 4.2.10. □

4.3 Graded rings and modules

Let $(\Gamma, +)$ be a commutative monoid. In most cases we consider $\Gamma = \mathbb{Z}_{\geq 0}$.

Definition 4.3.1. A Γ-graded ring is a ring R whose underlying additive group is endowed with a decomposition $R = \bigoplus_{\gamma\in\Gamma} R_\gamma$, such that $R_\gamma R_\eta \subset R_{\gamma+\eta}$ for all $\gamma, \eta \in \Gamma$.

For R as above, a Γ-graded R-module is an R-module M whose underlying additive group decomposes as $M = \bigoplus_{\gamma\in\Gamma} M_\gamma$, such that $R_\gamma M_\eta \subset M_{\gamma+\eta}$ for all $\gamma, \eta \in \Gamma$; in particular, R itself is a Γ-graded R-module. If $x \in M_\gamma \setminus \{0\}$, we say x is homogeneous of degree γ.

We will often omit Γ when there is no worry of confusion. Note that if 0 is allowed to be homogeneous, as people sometimes do, it will be homogeneous of any degree.

Exercise 4.3.2. Show that in a graded ring R we always have $1 \in R_0$, provides that $(\Gamma, +)$ satisfies the cancellation law: $\gamma + \eta = \eta \iff \gamma = 0$. Hint: let e_0 be the component of 1_R in degree 0, argue that $xe_0 = x = e_0 x$ for all homogeneous $x \in R$. The condition $1 \in R_0$ is sometimes built into the definition of graded rings.

Definition 4.3.3. A graded submodule of a graded R-module M is a submodule N with $N = \bigoplus_\gamma (N \cap M_\gamma)$, which gives rise to a natural grading $N_\gamma := N \cap M_\gamma$ on N.

For graded $N \subset M$, the quotient R-module $M/N = \bigoplus_\gamma M_\gamma/N_\gamma$ is again graded. As a special case, we have the notion of graded ideals of R (also known as *homogeneous ideals*), and the quotient ring $R/\mathfrak{a}$ with respect to graded $\mathfrak{a}$ inherits the evident grading.

Let N be an R-submodule of M and suppose M is graded. The following are easily seen to be equivalent:

(i) $N \subset M$ is graded;

(ii) N is generated by homogeneous elements;

(iii) if $x = \sum_\gamma x_\gamma \in N$ with each x_γ homogeneous of degree γ, then $\forall\ x_\gamma \in N$.

Example 4.3.4. Let A be a ring and $R := A[X_1, \dots, X_n]$. Then R is naturally $\mathbb{Z}_{\geq 0}$-graded by degrees: for each $d \in \mathbb{Z}_{\geq 0}$, let R_d be the set of homogeneous polynomials of total degree d. Ideals generated by homogeneous polynomials are precisely the graded ideals. The importance of this grading comes from projective algebraic geometry.

On the other hand, R can also be graded by monomials by taking $\Gamma = \mathbb{Z}_{\geq 0} \times \cdots \times \mathbb{Z}_{\geq 0}$ (n copies), and we set $R_{(d_1,\dots,d_n)} = A \cdot X_1^{d_1} \cdots X_n^{d_n}$

Many constructions in commutative algebra can be generalized to the graded case. Let us illustrate what one can do in an important case, the primary decomposition (cf. [8, §3.5 and Exercise 3.5]). In the $\mathbb{Z}$-graded context, it says that for a finitely generated graded module M over a Noetherian graded ring, the associated primes of M are all graded ideals, and one can write $\{0\} = N_1 \cap \cdots \cap N_m$ where $N_i \subset M$ are graded submodules with $\mathrm{Ass}(M/N_i) = \{\mathfrak{p}_i\}$, $\mathfrak{p}_i \in \mathrm{Ass}(M)$, etc. Most of the arguments in the ungraded case carry over verbatim, and the only new technique is the following

Lemma 4.3.5. *Let M be a $\mathbb{Z}$-graded module over a $\mathbb{Z}$-graded ring R. If $x \in M$ and $\mathfrak{p} := \operatorname{ann}(x)$ is a prime ideal, then*

(*i*) *$\mathfrak{p}$ is a homogeneous ideal, and*

(*ii*) *$\mathfrak{p} = \operatorname{ann}(y)$ for some homogeneous element $y \in M$.*

Proof. We begin with (i). Let $t \in \mathfrak{p}$ and $x \in M$ be such that $\mathfrak{p} = \operatorname{ann}(M)$. Write

$$t = \sum_{\gamma \in \mathcal{A}} t_\gamma, \quad x = \sum_{\eta \in \mathcal{B}} x_\eta,$$

where $t_\gamma \in R_\gamma \setminus \{0\}$ and $x_\eta \in M_\eta \setminus \{0\}$ for all γ, η. Denote by γ_0 and η_0 the minimal elements in $\mathcal{A}$ and $\mathcal{B}$, respectively. Homogenity amounts to $t_\gamma \in \mathfrak{p}$ for each $\gamma \in \mathcal{A}$, and this will be done by induction on $|\mathcal{B}|$. By a further induction on $|\mathcal{A}|$, for fixed x and $\mathfrak{p}$, this can be reduced to showing $t_{\gamma_0} \in \mathfrak{p}$.

First of all, considerations of degrees and $tx = 0$ lead to $t_{\gamma_0} x_{\eta_0} = 0$. If $x = x_{\eta_0}$ (i.e. $|\mathcal{B}| = 1$), we obtain $t_{\gamma_0} \in \operatorname{ann}(x) = \mathfrak{p}$ as required. In general:

- ⋄ Suppose that $\mathfrak{p} = \operatorname{ann}(t_{\gamma_0} x)$; since the decomposition

$$t_{\gamma_0} x = \sum_{\substack{\eta \in \mathcal{B} \\ \eta \neq \eta_0}} t_{\gamma_0} x_\eta$$

  involves fewer homogeneous terms, $\mathfrak{p}$ is then homogeneous by our induction hypothesis on $|\mathcal{B}|$.

- ⋄ Suppose there exists $s \in R \setminus \mathfrak{p}$ such that $s(t_{\gamma_0} x) = 0$, then $s t_{\gamma_0} \in \mathfrak{p}$, hence $t_{\gamma_0} \in \mathfrak{p}$. This concludes the homogeneity (i).

From the homogeneity $\mathfrak{p}$ we infer that $\mathfrak{p} \subset \operatorname{ann}(x_\eta)$ for each $\eta \in \mathcal{B}$. Now that

$$\mathfrak{p} = \operatorname{ann}(x) \supset \prod_{\eta \in \mathcal{B}} \operatorname{ann}(x_\eta),$$

we have $\mathfrak{p} \supset \operatorname{ann}(x_\eta)$ for some η, hence $\mathfrak{p} = \operatorname{ann}(x_\eta)$. Take $y = x_\eta$ to obtain (ii). □

4.4 Filtrations

Now turn to filtrations. We only deal with decreasing filtrations indexed by $\mathbb{Z}_{\geq 0}$.

Definition 4.4.1. A *filtration* on a ring R is a descending sequence

$$R = F^0 R \supset F^1 R \supset F^2 R \supset \cdots$$

of ideals such that $F^i R \cdot F^j R \subset F^{i+j} R$. Define the associated $\mathbb{Z}_{\geq 0}$-graded ring

$$\operatorname{gr}_F(R) := \bigoplus_{n \geq 0} \underbrace{F^n R / F^{n+1} R}_{=: \operatorname{gr}_F^n R}$$

whose multiplication is defined as follows: if $x \in F^nR/F^{n+1}R$ and $y \in F^mR/F^{m+1}R$, choose liftings $\tilde{x} \in F^nR$ and $\tilde{y} \in F^mR$ and define

$$xy := \text{the image of } \tilde{x}\tilde{y} \text{ in } F^{n+m}R/F^{n+m+1}R;$$

this is readily seen to be well-defined. The multiplication of arbitrarily many homogeneous elements can be obtained in the same recipe. The datum $(R, F^\bullet R)$ is called a *filtered ring*,

Given a filtered ring R, a *filtered R-module* M is an R-module M equipped with a descending sequence[1] of submodules

$$\cdots \supset F^iM \supset F^{i+1}M \supset \cdots, \quad i \in \mathbb{Z}$$

such that $F^iR \cdot F^jM \subset F^{i+j}M$. Define the associated graded module as the $\mathbb{Z}$-graded $\mathrm{gr}_F R$-module

$$\mathrm{gr}_F(M) := \bigoplus_{n\in\mathbb{Z}} \underbrace{F^nM/F^{n+1}M}_{=:\mathrm{gr}_F^i M}$$

whose scalar multiplication is defined using liftings as above.

The subscript F in gr will often be omitted. To guarantee that $\mathrm{gr}_F(R) \neq \{0\}$, we usually impose the harmless condition

$$R = F^0R \supsetneq F^1R.$$

Example 4.4.2. Let $\mathfrak{a}$ be a proper ideal of R, then $F^iR := \mathfrak{a}^i$ defines a filtration on R, called the $\mathfrak{a}$-*adic filtration*.

Definition 4.4.3. Equip R with the $\mathfrak{a}$-adic filtration. A filtered R-module M is called $\mathfrak{a}$-*stable* if $\mathfrak{a} \cdot F^iM = F^{i+1}M$ for $i \gg 0$.

Recall that $\mathfrak{a} \cdot F^iM \subset F^{i+1}M$ holds for all M, which is a part of our assumption.

As an easy example, set $F^iM := \mathfrak{a}^iM$ for $i \geq 1$, and $F^{\leq 0}M := M$; this is the $\mathfrak{a}$-adic filtration on M, which is obviously $\mathfrak{a}$-stable.

Proposition 4.4.4. *Suppose $\mathfrak{a}$ is a proper ideal of R. If R is Noetherian, so is $\mathrm{gr}(R)$ with respect to the $\mathfrak{a}$-adic filtration. In fact $\mathrm{gr}(R)$ is finitely generated over $\mathrm{gr}^0(R)$.*

Proof. Let $x_1, \ldots, x_n$ be generators of $\mathfrak{a}$, with images $\bar{x}_i \in \mathfrak{a}/\mathfrak{a}^2$. Then $\mathrm{gr}(R)$ is generated by $\bar{x}_1, \ldots \bar{x}_n$ over $R/\mathfrak{a} = \mathrm{gr}^0 R$, which is also Noetherian. Now apply Hilbert's Basissatz. □

Proposition 4.4.5. *Let $\mathfrak{a}$ be a proper ideal of R and M a finitely generated R-module. Suppose M is endowed with an $\mathfrak{a}$-stable filtration such that F^iM is finitely generated for each i, and $F^{\leq 0}M = M$. Then $\mathrm{gr}(M)$ is a finitely generated $\mathrm{gr}(R)$-module.*

Proof. Take n such that $\mathfrak{a} \cdot F^iM = F^{i+1}M$ for all $i \geq n$. Then in $\mathrm{gr}(M) = \bigoplus_i \mathrm{gr}^i M$ we have

$$(\mathfrak{a}/\mathfrak{a}^2) \cdot \mathrm{gr}^i M = \mathrm{gr}^{i+1} M, \quad i \geq n.$$

Therefore it suffices to take generators from $\mathrm{gr}^0 M, \ldots, \mathrm{gr}^n M$, each of whom is finitely generated over $R/\mathfrak{a} = \mathrm{gr}^0 R$. □

[1] In view of later applications, the filtration on a module is indexed by $\mathbb{Z}$ instead of $\mathbb{Z}_{\geq 0}$.

4.5 Theorems of Artin–Rees and Krull

Conserve the conventions in the previous section on filtrations, etc.

Definition 4.5.1 (Morphisms between filtered objects)**.** Let $(A, F^\bullet A)$ and $(B, F^\bullet B)$ be filtered rings. A *morphism* between them means a ring homomorphism $\varphi : A \to B$ satisfying $\varphi(F^i A) \subset F^i B$ for all i. Similarly, suppose A is filtered and let M, N be filtered A-modules. A morphism $M \to N$ means a homomorphism $\psi : M \to N$ of R-modules satisfying $\psi(F^i M) \subset F^i N$ for all i.

This makes the filtered rings and the filtered modules over a filtered ring into categories. Obviously, morphisms φ between filtered objects induce graded morphisms $\operatorname{gr}\varphi$ between the associated graded objects. Therefore we obtain a functor from the category of filtered rings or modules into their graded avatars.

Remark 4.5.2. Suppose $\varphi : M \to N$ is a morphism between filtered A-modules. The quotient $M/\ker(\varphi)$ inherits a filtration from M, whereas the submodule $\operatorname{im}(\varphi)$ inherits one from N. When the natural isomorphism $M/\ker(\varphi) \to \operatorname{im}(\varphi)$ is an isomorphism between filtered modules, or equivalently

$$\forall i \in \mathbb{Z},\ \varphi(F^i M) = \varphi(M) \cap F^i N,$$

we say φ is a *strict morphism*.

It is often useful to relate properties of a filtered module or morphism to its graded counterpart. Propositions 4.4.4 and 4.4.5 are such examples. Here is an example for the other direction. We say that a filtration on M is *exhaustive* if $\bigcup_i F^i M = M$, *separating* (or *Hausdorff*) if $\bigcap_i F^i M = \{0\}$

Proposition 4.5.3. *Suppose that $\varphi : M \to N$ is a morphism between filtered R-modules. If M is exhaustive and separating, and $\operatorname{gr}\varphi$ is injective, then φ is also injective.*

Proof. Let $x \in \ker(\varphi)$. There exists n such that $x \in F^n M$. Regard $x + F^{n+1}M$ as an element of $\operatorname{gr}^n M$. Then $\operatorname{gr}(\varphi)(x + F^{n+1}M) = \varphi(x) + F^{n+1}N = 0$, so $x \in F^{n+1}M$. Iterating this argument, we have $x \in \bigcap_{k \geq n} F^k M = \{0\}$. □

See Lemma 5.2.3 for the case of surjections.

In what follows, $\mathfrak{a}$ always denotes a proper ideal of a ring R.

Definition 4.5.4 (Blow-up algebras and modules)**.** Introduce an indeterminate X and define the $\mathbb{Z}_{\geq 0}$-graded R-algebra

$$\operatorname{Bl}_\mathfrak{a} R := \bigoplus_{n \geq 0} \mathfrak{a}^n X^n \ \subset R[X].$$

If an R-module M is endowed with a filtration $(F^i M)_{i \geq 0}$ compatible with $\mathfrak{a}$, we define

$$\operatorname{Bl}(M) := \bigoplus_{n \geq 0} (F^n M) \otimes X^n \subset M \underset{R}{\otimes} R[X].$$

Clearly, $\operatorname{Bl}(M)$ is a graded $\operatorname{Bl}_\mathfrak{a} R$-module.

Remark 4.5.5. The indeterminate X is somehow a placeholder. Enlarge $\mathrm{Bl}_{\mathfrak{a}}R$ to $\tilde{B}$ by setting the negative graded pieces to be $R \cdot X^{<0}$, and set $T = X^{-1}$. We see that $\tilde{B}$ is actually an $R[T]$-algebra, sometimes called the *Rees algebra* of $\mathfrak{a}$. Under the specialization $T = 0$ we get

$$\frac{\tilde{B}}{T\tilde{B}} \simeq \bigoplus_{n \geq 0} \frac{\mathfrak{a}^n}{\mathfrak{a}^{n+1}} \cdot T^{-n} \simeq \mathrm{gr}(R).$$

On the other hand, inverting T yields

$$\tilde{B}[T^{-1}] = \bigoplus_{n \in \mathbb{Z}} R \cdot T^{-n} = R[T^{\pm 1}].$$

This reflects a well-known deformation construction in geometry; $\mathrm{gr}(R)$ is actually the graded R-algebra corresponding to the *normal cone* defined by $\mathfrak{a} \subset R$. We refer to [9, §5.1] for details.

Lemma 4.5.6. *Consider a ring R with proper ideal $\mathfrak{a}$, together with a filtered R-module M, assume furthermore that each F^iM is finitely generated over R. The following are equivalent:*

(*i*) $\mathrm{Bl}(M)$ *is finitely generated over* $\mathrm{Bl}_{\mathfrak{a}}R$*;*

(*ii*) *the filtration on M is $\mathfrak{a}$-stable.* (*Definition 4.4.3*)

Proof. (i) $\implies$ (ii): Choose homogeneous generators $x_1, \dots, x_n \in \mathrm{Bl}(M)$ with degrees $d_1, \dots, d_n$ respectively. It is then routine to see that

$$i \geq \max\{d_1, \dots, d_n\} \implies (F^{i+1}M)X^{i+1} = \mathfrak{a}X \cdot (F^iM)X^i,$$

that is, $\mathfrak{a} \cdot F^iM = F^{i+1}M$ for these i.

(ii) $\implies$ (i): Suppose $\mathfrak{a} \cdot F^iM = F^{i+1}M$ for $i \geq d$, then $\mathrm{Bl}(M)$ is generated by $\bigoplus_{j \leq d}(F^jM)X^j$, and each F^jM is finitely generated over $R = (\mathrm{Bl}_{\mathfrak{a}}R)_0$. □

Theorem 4.5.7 (Artin–Rees)**.** *Let R be a Noetherian ring endowed with $\mathfrak{a}$-adic filtration. Let M be a finitely generated R-module and $N \subset M$ an R-submodule. Then the filtration on N induced by the $\mathfrak{a}$-adic filtration of M, namely $F^iN := \mathfrak{a}^iM \cap N$, is $\mathfrak{a}$-stable.*

Proof. Define $\mathrm{Bl}(N)$ using the induced filtration $F^iN := \mathfrak{a}^iM \cap N$, which is a submodule of the finitely generated $\mathrm{Bl}_{\mathfrak{a}}R$-module $\mathrm{Bl}(M)$ (Lemma 4.5.6). If $\mathfrak{a} = (a_1, \dots, a_m)$ than $\mathrm{Bl}_{\mathfrak{a}}R = R[a_1X, \dots, a_mX] \subset R[X]$, hence Noetherian by Hilbert's Basissatz. We deduce that $\mathrm{Bl}(N)$ is finitely generated over $\mathrm{Bl}_{\mathfrak{a}}R$. In turn, this implies $F^\bullet N$ is an $\mathfrak{a}$-stable filtration on N by Lemma 4.5.6. □

Theorem 4.5.8. *For $R, \mathfrak{a}, M$ as in the previous theorem, we set $N := \bigcap_{n \geq 0} \mathfrak{a}^nM$. Then $\mathfrak{a}N = N$.*

Proof. Since the induced filtration on N is $\mathfrak{a}$-stable by Theorem 4.5.7, for $n \gg 0$ we have

$$N = \mathfrak{a}^nM \cap N = \mathfrak{a} \cdot (\mathfrak{a}^{n-1}M \cap N) = \mathfrak{a}N.$$

The assertion follows. □

Corollary 4.5.9 (Krull)**.** *If* $\mathfrak{a} \subset \operatorname{rad}(R)$*, then* $\bigcap_{n\geq 0} \mathfrak{a}^n M = \{0\}$ *for any finitely generated* R*-module* M*. In particular* $\bigcap_{n\geq 0} \mathfrak{a}^n = \{0\}$ *whenever* $\mathfrak{a} \subset \operatorname{rad}(R)$*.*

Proof. Theorem 4.5.8 together with Nakayama's lemma imply $N = \{0\}$. □

Corollary 4.5.10 (Krull's Intersection Theorem)**.** *Let* R *be a Noetherian domain and* $\mathfrak{a}$ *a proper ideal. Then* $\bigcap_{n\geq 0} \mathfrak{a}^n = \{0\}$*.*

Proof. Define $N := \bigcap_{n\geq 0} \mathfrak{a}^n \subset R$. By Theorem 4.5.8 we have $\mathfrak{a}N = N$, thus there exists $r \in \mathfrak{a}$ with $1 + r \in \operatorname{ann}(N)$ by Nakayama's Lemma (Theorem 1.3.5). As $\mathfrak{a}$ is proper, $1 + r$ cannot be zero. Since R is a domain containing N, the only possibility is $N = \{0\}$ as asserted. □

Lecture 5

From completions to dimensions

The main references are [11, 8].

5.1 Completions

Consider a ring R together with a family of ideals $\mathcal{J} \neq \emptyset$, such that for any $I, J \in \mathcal{J}$ there exists $K \in \mathcal{J}$ with $K \subset I \cap J$. This turns R into a topological ring, characterized by the property that $\mathcal{J}$ forms a local base of open neighborhoods of 0. Recall that being a topological ring means that addition, multiplication and $x \mapsto -x$ are all continuous. By standard arguments, R is Hausdorff if and only if $\{0\}$ is closed, if and only if $\bigcap_{I \in \mathcal{J}} I = \{0\}$.

To simplify matters, we assume that

- the family $\mathcal{J}$ is countable, so that the topological properties (accumulation points, etc.) are detected by convergence of *sequences* as in the case of metric spaces;
- furthermore, we may arrange that $\mathcal{J} = \{I \supset J \supset K \supset \cdots\}$, in other words our topology comes from *filtrations*.

Without the countability assumption, the sequences will have to be replaced by *filters*.

It makes sense to talk about topological R-modules for a topological ring R. By replacing filtration by ideals by filtration by R-submodules subject to the usual compatibility relation $F^i R \cdot F^j M \subset F^{i+j} M$, the recipe above applies to R-modules as well. Given $N \subset M$, the topology so obtained on M passes to M/N by taking the quotient topology, or equivalently the quotient filtration $(F^\bullet M + N)/N$. If the filtration in question is I-adic, where $I \subsetneq R$ is an ideal, we obtain the *I-adic topology* on rings and modules.

An R-module M equipped with a topology as above is *complete* if every Cauchy sequence $(x_n)_{n \geq 1}$ has a limit; a Cauchy sequence $(x_n)_{n \geq 1}$ is a sequence satisfying

$$\forall I \in \mathcal{J},\ \exists N \quad i, j \geq N \implies x_i - x_j \in I.$$

As in the familiar case of metric spaces, one has the *completion* of M. It is actually a morphism $M \to \hat{M}$ with $\hat{M}$ complete Hausdorff, characterized by the following universal

property:

The uniqueness results immediately, and the formation of $M \mapsto \hat{M}$ is seen to be functorial in M. If M is already complete Hausdorff, one may take $\hat{M} = M$. Certainly, the same applies to the ring R.

Exercise 5.1.1. Suppose that R is complete Hausdorff with respect to the I-adic topology, where I is a proper ideal. Show that every element of the form $u + x$, $u \in R^\times$ and $x \in I$, is invertible.

From the algebraic perspective, the completion of a filtered R-module $M = F^0M \supset F^1M \supset \cdots$ can be constructed as the projective limit

$$\begin{aligned}\hat{M} &:= \varprojlim_{i\geq 1} M/F^iM \\ &= \left\{(x_i)_{i\geq 1} : i \leq j \implies x_i \equiv x_j \pmod{F^iM}\right\} \subset \prod_{i\geq 1} M/F^iM.\end{aligned}$$

The morphism $M \to \hat{M}$ is the diagonal map. The topology on $\hat{M}$ arises from the filtration

$$F^i\hat{M} := \ker\left[p_i : \hat{M} \to M/F^iM\right] = \left\{(x_n)_n \in \hat{M} : i \leq k \implies x_i = 0\right\},$$

so that the preimage of $F^i\hat{M}$ in M is precisely F^iM. In the case where $M = R$ and F^iR are ideals, we obtain the complete Hausdorff ring $\hat{R}$, which is a subring of $\prod_{i\geq 1} R/F^iR$. Since the filtrations on R and M are assumed compatible, $\hat{M}$ is an $\hat{R}$-module.

Example 5.1.2. Fix a prime number p. The completion of $\mathbb{Z}$ with respect to the ideal $p\mathbb{Z}$ is nothing but the ring $\mathbb{Z}_p$ of p-adic integers. Similarly, the completion of $\Bbbk[X]$ with respect to (X) is isomorphic to the $\Bbbk$-algebra $\Bbbk[\![X]\!]$.

Exercise 5.1.3. Describe the kernel of $M \to \hat{M}$ and show $M \hookrightarrow \hat{M}$ if and only if M is Hausdorff.

Exercise 5.1.4. Show that the topology of $\hat{M}$ is the restriction of the product topology of $\prod_i M/F^iM$, provided that each M/F^iM is endowed with the discrete topology. Show that $\hat{M}$ is a closed subspace of $\prod_i M/F^iM$

Lemma 5.1.5. *Let M be a complete R-module with respect to some filtration $F^\bullet M$. For any submodule N, the quotient M/N is also complete with respect to the quotient topology, or equivalently with respect to the quotient filtration $(F^\bullet M + N)/N$.*

Proof. Let $\bar{x}_n$ be a Cauchy sequence in M/N. Choose preimages $M \ni x_n \mapsto \bar{x}_n$ for all n. We have $\bar{x}_{n+1} - \bar{x}_n \in F^{i(n)}M + N$ where $\lim_{n\to\infty} i(n) = \infty$, therefore we can write $x_{n+1} - x_n = y_n + \delta_n$ where $y_n \in F^{i(n)}M$ and $\delta_n \in N$. We contend that $x'_n := x_1 + \sum_{i<n} y_i$ is a Cauchy sequence in M. Indeed, for any $i > j$ we have $x'_i - x'_j = \sum_{j\leq k<i} y_k$, which lies in $F^{\inf_k i(k)}M$. This implies $(x'_n)_n$ is a Cauchy sequence, hence has a limit $x \in M$. It is also clear that $x'_n \mapsto \bar{x}_n$. Hence $\bar{x}'_n$ has a limit $\bar{x} = x \bmod N$ in M/N. □

Let us turn to the exactness of completion. This should be understood in the broader framework of $\varprojlim$ of arbitrary projective systems. For simplicity, we only consider I-adic topologies on finitely generated modules over a Noetherian ring.

Observe that any homomorphism $\varphi : M \to N$ between R-modules is automatically $\mathfrak{a}$-adically continuous, for that $\varphi(\mathfrak{a}^n M) \subset \mathfrak{a}^n N$.

Proposition 5.1.6. *Let R be a Noetherian ring and $I \subsetneq R$ an ideal. Suppose $0 \to M' \to M \to M'' \to 0$ is an exact sequence of finitely generated R-modules, each term equipped with the I-adic topology. The completed sequence $0 \to \hat{M}' \to \hat{M} \to \hat{M}'' \to 0$ is also exact.*

Consequently, completion preserves the exactness of sequences formed by finitely generated R-modules. This is what makes completion so useful.

Proof. We shall show

(i) the topology on M' induced from M is the same as the I-adic topology;
(ii) the quotient topology on $M'' = M/M'$ is I-adic;
(iii) the completion $\hat{M}'$ is naturally identified with the closure of the image of M' in $\hat{M}$;
(iv) $\hat{M}''$ is naturally identified with the quotient of $\hat{M}$ by $\hat{M}'$.

(i) is a direct consequence of Artin–Rees Theorem 4.5.7: for $n \gg 0$ we have

$$I^n M' \subset M' \cap I^n M = I(M' \cap I^{n-1} M) \subset I^{n-1} M', \tag{5–1}$$

and this suffices to identify the resulting topologies.

(ii) is immediate. As for (iii), we may embed M' into M and work with the induced topology. Realize $\hat{M}$ as $\varprojlim_n M/I^n M$. As a topological module $\hat{M}'$ equals

$$\begin{aligned}\varprojlim_n \frac{M'}{M' \cap I^n M} &= \left\{\hat{x} = (x_n)_n \in \hat{M} : \forall k,\ x_k \text{ comes from } M'\right\} \\ &= \left\{\hat{x} \in \hat{M} : \forall k\ \exists y \in M' \text{ s.t. } \hat{x} \in y + F^k \hat{M}\right\}\end{aligned}$$

which is readily seen to be the closure of the image of M'.

For (iv), the quotient $\hat{M}/\hat{M}'$ is Hausdorff since $\hat{M}'$ is a closed submodule. It is also complete by Lemma 5.1.5. There is a natural homomorphism $M/M' \to \hat{M}/\hat{M}'$. Given any continuous homomorphism $\varphi : M/M' \to N$ to a complete Hausdorff R-module N, we may pull it back to $M \to N$, which corresponds to a unique continuous $\hat{M} \to N$ that is trivial on the image of M'; but such a homomorphism must also vanish on the closure $\hat{M}'$. This yields the required $\hat{\varphi} : \hat{M}/\hat{M}' \to N$ in the universal property. □

For any R-module M endowed with I-adic topology, there is a canonical homomorphism $M \otimes_R \hat{R} \to \hat{M}$. Indeed, $\hat{M} = \varprojlim_n M/I^n M$ is a $\hat{R} = \varprojlim_n R/I^n$-module by

$$(r_n)_{n\geq 1} \cdot (x_n)_{n \geq 1} = (r_n x_n)_{n \geq 1}, \quad (r_n)_n \in \hat{R},\ (x_n)_n \in \hat{M},$$

hence the R-homomorphism $M \to \hat{M}$ gives rise to $M \otimes_R \hat{R} \to \hat{M}$ by the universal property of base change. This homomorphism is continuous if $M \otimes_R \hat{R}$ is filtered by the images of $M \otimes_R (F^\bullet \hat{R})$, which makes it into a topological $\hat{R}$-module.

Theorem 5.1.7. *Suppose R is Noetherian. Let M be a finitely generated R-module endowed with the I-adic topology. The homomorphism $M \underset{R}{\otimes} \hat{R} \to \hat{M}$ is then an isomorphism.*

Proof. Write down a finite presentation $R^{\oplus a} \to R^{\oplus b} \to M \to 0$. By the naturality of the homomorphism above, the right-exactness of $\otimes$ and Proposition 5.1.6, we have a commutative diagram

$$\begin{array}{ccccccc} R^{\oplus a} \underset{R}{\otimes} \hat{R} & \longrightarrow & R^{\oplus a} \underset{R}{\otimes} \hat{R} & \longrightarrow & M \underset{R}{\otimes} \hat{R} & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ \widehat{R^{\oplus a}} & \longrightarrow & \widehat{R^{\oplus b}} & \longrightarrow & \hat{M} & \longrightarrow & 0 \end{array}$$

with exact rows. Completion commutes with direct sums: $(N_1 \oplus N_2)^\wedge = \hat{N}_1 \oplus \hat{N}_2$ canonically (easy, and the categorical reason is that completion is left adjoint to oblivion R-CompHausMod $\to$ R-TopMod). Therefore the first two vertical arrows may be identified with the canonical arrow $R^{\oplus \star} \underset{R}{\otimes} \hat{R} \to \hat{R}^{\oplus \star}$, $\star \in \{a, b\}$, which is an isomorphism of topological $\hat{R}$-modules. We infer that $M \underset{R}{\otimes} \hat{R} \xrightarrow{\sim} \hat{M}$ topologically. □

Remark 5.1.8. In fact $M \underset{R}{\otimes} \hat{R} \xrightarrow{\sim} \hat{M}$ is also a homeomorphism. It suffices to observe that in the rows of the commutative diagram above, $M \underset{R}{\otimes} \hat{R}$ and $\hat{M}$ are both realized as quotient topological $\hat{R}$-modules, and that $R^{\oplus \star} \underset{R}{\otimes} \hat{R} \xrightarrow{\sim} \hat{R}^{\oplus \star}$ is a homeomorphism. The second point has been observed in the proof of Proposition 5.1.6, and the first follows from the fact completed modules carry the $\hat{I}$-adic topology. See Proposition 5.2.2. We do not need this result.

In the following statements, R is Noetherian and an ideal $I \subsetneq R$ is chosen.

Corollary 5.1.9. *The canonical homomorphism $R \to \hat{R}$ is flat.*

Proof. Flatness can be tested on short exact sequences of the form $0 \to \mathfrak{a} \to R \to R/\mathfrak{a} \to 0$ where $\mathfrak{a}$ is a finitely generated ideal of R. Its base-change to $\hat{R}$ is the same as completion, and completion is an exact functor by Proposition 5.1.6. □

Corollary 5.1.10. *Assume R is I-adically complete Hausdorff. Then every finitely generated R-module M is I-adically complete Hausdorff, and any submodule $N \subset M$ is closed.*

Proof. For the first assertion: the completion of M can be identified with the composite $M = M \underset{R}{\otimes} R \to M \underset{R}{\otimes} \hat{R} \to \hat{M}$, which is bijective. Therefore every Cauchy sequence in M has a limit in M.

As to the second assertion, recall that the I-adic topology on N is the same as the one restricted from M by (5–1). It remains to notice that complete subspaces must be closed. □

5.2 Further properties of completion

Let R be a Noetherian ring and M a finitely generated R-module. Fix an ideal $I \subsetneq R$. Unless otherwise specified, the topologies and completions are always I-adic.

Proposition 5.2.1. *Let $\mathfrak{a}$ be an ideal, then $\mathfrak{a}\hat{M} = \widehat{\mathfrak{a}M} = \hat{\mathfrak{a}}\hat{M}$ as submodules of $\hat{M}$. Consequently $\hat{M}/\mathfrak{a}\hat{M} \simeq (M/\mathfrak{a}M)^\wedge$ canonically.*

Proof. By the exactness of completion (Proposition 5.1.6), we may realize $\hat{\mathfrak{a}}$ as an ideal of $\hat{R}$; in fact it is the image $\mathfrak{a}\hat{R}$ of $\mathfrak{a} \underset{R}{\otimes} \hat{R} \to R \underset{R}{\otimes} \hat{R} = \hat{R}$. Hence $\mathfrak{a}\hat{R} = \hat{\mathfrak{a}}$. Now consider the commutative diagram

$$\begin{array}{ccc} \mathfrak{a} \underset{R}{\otimes} M \underset{R}{\otimes} \hat{R} & \longrightarrow & \mathfrak{a} \underset{R}{\otimes} \hat{M} \\ \downarrow & \searrow & \downarrow \\ \mathfrak{a}M \underset{R}{\otimes} \hat{R} & \longrightarrow & \hat{M} \end{array}$$

The upper horizontal arrow is an isomorphism by Theorem 5.1.7, therefore the diagonal arrow has image equal to $\mathfrak{a}\hat{M}$. The lower horizontal arrow is just the completion of $\mathfrak{a}M \hookrightarrow M$, thus injective with image $(\mathfrak{a}M)^\wedge$ by Proposition 5.1.6. A comparison yields $(\mathfrak{a}M)^\wedge = \mathfrak{a}\hat{M}$. Also note that $\hat{\mathfrak{a}}\hat{M} = \mathfrak{a}\hat{R}\hat{M} = \mathfrak{a}\hat{M}$. The final assertion results from the exactness of completion. □

Since the I-adic topology on M/I^nM is discrete, as a special case ($\mathfrak{a} = I^n$) we deduce the natural identifications

$$\begin{gathered} M/I^nM = \hat{M}/I^n\hat{M} = \hat{M}/\hat{I}^n\hat{M}, \quad \forall n \geq 0, \\ \mathrm{gr}_I(R) = \mathrm{gr}_I(\hat{R}) = \mathrm{gr}_{\hat{I}}(\hat{R}), \\ \mathrm{gr}_I(M) = \mathrm{gr}_I(\hat{M}) = \mathrm{gr}_{\hat{I}}(\hat{M}). \end{gathered}$$

Proposition 5.2.2. *For any finitely generated R-module M, the topology on $\hat{M}$ coincides with the $\hat{I}$-adic one.*

Proof. Consider the closure of the image of I^nM in $\hat{M}$. It is readily seen to be $\{(x_k)_k : i \leq n \implies x_i = 0\} = F^n\hat{M}$. On the other hand, we have seen that this closure is $\widehat{I^nM} \subset \hat{M}$. By virtue of Proposition 5.2.1, we have $\widehat{I^nM} = \widehat{I^n}\hat{M}$ and $\widehat{I^n} = I^n\hat{R} = (I\hat{R})^n = \hat{I}^n$. □

Lemma 5.2.3. *Consider a homomorphism $\varphi : L \to N$ between filtered modules over some ring, such that L is complete, N is Hausdorff and exhaustive (see §4.5) with respect to their filtrations, and $\mathrm{gr}(\varphi) : \mathrm{gr}(L) \to \mathrm{gr}(N)$ is surjective. Then φ is also surjective.*

Proof. Let $y \in F^dN$, we may take $x \in F^dL$ such that $y' := y - \varphi(x) \in F^{d+1}N$. Next, take $x' \in F^{d+1}L$ with $y'' := y' - \varphi(x') \in F^{d+2}N$, and so forth. Use the completeness of L to define $x_\infty := x + x' + x'' + \cdots$, which maps to y since N is Hausdorff. □

Proposition 5.2.4. *The ring $\hat{R}$ is also Noetherian, and $\hat{I} \subset \mathrm{rad}(\hat{R})$.*

Proof. Let $\mathfrak{A}$ be any ideal of $\hat{R}$, equipped with the filtration $F^n\mathfrak{A} := \hat{I}^n \cap \mathfrak{A}$. We have to show $\mathfrak{A}$ is finitely generated. Since $\mathrm{gr}_I(R) = \mathrm{gr}_{\hat{I}}(\hat{R})$ is Noetherian, so is $\mathrm{gr}_F(\mathfrak{A})$. Take $t_1, \dots, t_n \in \mathfrak{A}$, $t_i \in F^{d_i}\mathfrak{A}$, whose images $\bar{t}_i$ in $\mathrm{gr}_F^{d_i}(\mathfrak{A})$ generates $\mathrm{gr}_F(\mathfrak{A})$. Using an appropriately shifted filtration on $L := \hat{R}^{\oplus n}$, we obtain a filtered homomorphism $\varphi : L \to \mathfrak{A}$ with image $(t_1, \dots, t_n)$, such that $\mathrm{gr}(\varphi)$ is surjective. Now apply the previous Lemma to obtain the first assertion.

One of the characterizations of Jacobson radical says that $\hat{I} \subset \mathrm{rad}(\hat{R})$ if and only if $1 - \hat{I} \subset \hat{R}^\times$. This is verified by noting that $(1-t)^{-1} = 1 + t + t^2 + \cdots$ converges I-adically. This proves the second assertion. □

Proposition 5.2.5. *The map $\mathfrak{p} \mapsto \hat{\mathfrak{p}}$ furnishes an injection from $V(I)$ to $\mathrm{Spec}(\hat{R})$ satisfying $R/\mathfrak{p} \simeq \hat{R}/\hat{\mathfrak{p}}$ (as rings). It restricts to a bijection $\mathrm{MaxSpec}(R) \cap V(I) \xrightarrow{1:1} \mathrm{MaxSpec}(\hat{R})$.*

Consequently, if R is local (resp. semi-local), so is $\hat{R}$.

Proof. Since $\mathfrak{p} \supset I$, the I-adic topology on $R/\mathfrak{p}$ is discrete. By Proposition 5.2.1, $\hat{R}/\hat{p} \simeq (R/\mathfrak{p})^\wedge = R/\mathfrak{p}$, and here the isomorphism even respects ring structures. Therefore $\hat{\mathfrak{p}}$ is a prime ideal. Moreover, it is maximal if and only if $\mathfrak{p}$ is. Claim: $\mathfrak{p}$ is the preimage of $\hat{\mathfrak{p}} = \varprojlim_n \mathfrak{p}/(I^n \cap \mathfrak{p})$ under $R \to \hat{R} = \varprojlim_n R/I^n$. Indeed, lying in that preimage amounts to $x \in I^n + \mathfrak{p} = \mathfrak{p}$, for all $n \geq 1$. Injectivity follows.

Lemma 5.2.4 implies that every $\mathfrak{A} \in \mathrm{MaxSpec}(\hat{R})$ contains $\hat{I}$, therefore is open by Proposition 5.2.2. Since $\hat{R}$ is Noetherian, $\mathfrak{A}$ is also closed by Corollary 5.1.10. As $R \to \hat{R}$ has dense image, we conclude that $\mathfrak{A}$ equals the completion of its preimage $\mathfrak{m} \in V(I) \subset \mathrm{Spec}(R)$. By the previous paragraph, $\mathfrak{m}$ is a maximal ideal. □

5.3 Hilbert–Samuel polynomials

For a graded ring $R = \bigoplus_\gamma R_\gamma$ (we always assume $1 \in R_0$) and a given η, we may define its twist $R(\eta)$ as the graded R-module

$$R(\eta)_\gamma := R_{\gamma+\eta}.$$

To generate a graded R-module M by finitely many homogeneous elements $x_1, \dots, x_n$, of degrees $\eta_1, \dots, \eta_n$ respectively, is equivalent to giving a surjection of graded R-modules

$$\begin{aligned} \textstyle\bigoplus_{i=1}^n R(-\eta_i) &\twoheadrightarrow M \\ (\dots, 0, \underbrace{1}_{i-\text{th slot}}, 0, \dots) &\longmapsto x_i. \end{aligned} \tag{5–2}$$

Hereafter, we assume that

- ◇ everything is graded by $\Gamma = (\mathbb{Z}_{\geq 0}^N, +)$ for some fixed N,
- ◇ $R_0/R_0 \cap \mathrm{ann}(M)$ is an Artinian ring,
- ◇ R is finitely generated over R_0.

The appearance of $\operatorname{ann}(M)$ is harmless since R can be safely replaced by $R/\mathfrak{ann}(M)$, which is legitimate since $\operatorname{ann}(M)$ is a graded ideal of R. To see this, write $\operatorname{ann}(M)$ as the intersection of $\operatorname{ann}(x)$ where x ranges over the homogeneous elements of M, and observe that $\operatorname{ann}(x)$ must be graded.

Lemma 5.3.1. *For R as above and M a finitely generated graded R-module, each graded piece M_γ is an R_0-module of finite length.*

Proof. Using (5–2) this is readily reduced to the case $M = R(-\eta)$, and then to $M = R$. Write $R = R_0[x_1, \dots, x_n]$ where each x_i is homogeneous of degree d_i. Given γ, the R_0-module M_γ is generated by monomials $x_1^{a_1} \cdots x_n^{a_n}$ with $\sum_i a_i d_i = \gamma$ and $a_1, \dots, a_n \in \mathbb{Z}_{\geq 0}$; this admits only finitely many solutions $(a_1, \dots, a_n)$. We conclude that M_γ has finite length since $R_0/R_0 \cap \operatorname{ann}(M)$ is an Artinian ring. □

Recall that saying a module N over a ring A has finite length means that there exists a composition series

$$N = N_0 \supset \cdots \supset N_n = \{0\}, \quad \forall N_i/N_{i+1} \text{ is simple.}$$

The unique number (Jordan–Hölder Theorem) is called the *length* of N, denoted by $\ell_A(N)$. The length function is additive in short exact sequences. When A is a field we have $\ell_A = \dim_A$.

Definition 5.3.2. For R and M as in Lemma 5.3.1, we define the functions

$$\chi(M, \gamma) := \ell_{R_0}(M_\gamma), \quad \gamma \in \Gamma := \mathbb{Z}_{\geq 0}^N$$

with values in $\mathbb{Z}_{\geq 0}$.

One sees immediately that for a short exact sequence $0 \to M' \to M \to M'' \to 0$ of finitely generated graded R-modules, we have $\chi(M, \gamma) = \chi(M', \gamma) + \chi(M'', \gamma)$ for all $\gamma \in \Gamma$. This extends to alternating sums of χ in finite exact sequences.

One can control the behavior of $\chi(M, \cdot)$ by forming the Poincaré series $P_M(\mathbf{X}) = \sum_{\gamma \in \Gamma} \chi(M, \gamma)\mathbf{X}^\gamma$; see [7, 6.D]. Here we shall restrict to the case $N = 1$, i.e. $\Gamma = \mathbb{Z}_{\geq 0}$, in order to gain more control of $\chi(M, \gamma)$. As a preparation, we say a function $H : \mathbb{Z} \to \mathbb{C}$ is a *quasi-polynomial* of period ϖ if its restriction to each congruence class modulo ϖ coincides with a polynomial function (necessarily unique); the degree of χ is defined by taken the maximum among congruence classes. In particular, a quasi-polynomial of period 1 is just a polynomial.

Theorem 5.3.3. *Assume $\Gamma = \mathbb{Z}_{\geq 0}$. Suppose R is generated by homogeneous elements $x_1, \dots, x_n$ over R_0. There exists a unique quasi-polynomial H_M of degree $\leq n - 1$, with coefficients in $\mathbb{Q}$ and period $e := \operatorname{lcm}(\deg x_1, \dots, \deg x_n)$, such that*

$$\chi(M, \gamma) = H_M(\gamma), \quad |\gamma| \gg 0.$$

Proof. Uniqueness is clear. We construct H_M by induction on the minimal number of generators n. If $n = 0$ then $R = R_0$ and $M_\gamma = 0$ for $|\gamma| \gg 0$, in which case $H_M = 0$.

For $n \geq 1$, write $R = R_0[x_1, \dots, x_n]$ as usual. We may assume that $x_i \neq 0$ has degree η_i, for $i = 1, \dots, n$. Fix i and define the graded modules

$$Z := \ker\left(M \xrightarrow{\cdot x_i} M(\eta_i)\right), \quad Y := \operatorname{coker}\left(M(-\eta_i) \xrightarrow{\cdot x_i} M\right)$$

which are again finitely generated, so that we have the exact sequence

$$0 \to Z_\gamma \to M_\gamma \to M_{\gamma+\eta_i} \to Y_{\gamma+\eta_i} \to 0, \quad \gamma \in \Gamma.$$

Since x_i annihilates Z and Y, induction hypothesis entails

$$\chi(M, \gamma + \eta_i) - \chi(M, \gamma) = \chi(Y, \gamma + \eta_i) - \chi(Z, \gamma),$$

the right-hand side being quasi-polynomials of period $\operatorname{lcm}(\dots, \widehat{\eta_i}, \dots)$ for large $|\gamma|$ and of degrees $\leq n-2$, since x_i acts trivially on Z and Y. Doing this for all i yields difference equations that witness the polynomiality of $\chi(M, \gamma)$ for $|\gamma| \gg 0$ in every congruence class modulo e. □

In particular, if R is generated by R_1 over R_0, the period $e = 1$ and we have the notion of *Hilbert–Samuel polynomials*.

Example 5.3.4. For $R = M = \Bbbk[X_1, \dots, X_n]$ graded by total degree, where $\Bbbk$ is a field, our assumptions are readily verified. We see $\chi(M, \gamma) = \dim_\Bbbk \Bbbk[X_1, \dots, X_n]_{\deg=\gamma}$ for all $\gamma \in \mathbb{Z}_{\geq 0}$, which equals $\binom{\gamma+n-1}{n-1}$ by high school combinatorics. Hence the Hilbert–Samuel polynomial is $H_M(X) = \binom{X+n-1}{n-1} \in \mathbb{Q}[X]$.

5.4 Definition of Krull dimension

Let R be a ring.

Definition 5.4.1 (Height and dimension)**.** For any prime ideal $\mathfrak{p}$ of R, define its *height* $\operatorname{ht}(\mathfrak{p})$ as the supremum of the lengths of prime chains

$$\mathfrak{p} = \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n, \quad \text{length} := n.$$

For any ideal $\mathfrak{a}$ of R, we define $\operatorname{ht}(\mathfrak{a}) := \inf\{\operatorname{ht}(\mathfrak{p}) : \mathfrak{p} \supset \mathfrak{a}\}$.

Define the *Krull dimension* of R to be $\dim R := \sup_{\mathfrak{p} \in \operatorname{Spec}(R)} \operatorname{ht}(\mathfrak{p})$.

The following results are immediate.

- ◇ The zero prime in a domain has height 0.
- ◇ Fields have dimension zero. In fact, a ring has dimension zero if and only if every prime ideal is maximal.
- ◇ We have $\operatorname{ht}(\mathfrak{p}) = \dim R_\mathfrak{p}$ for every prime ideal $\mathfrak{p} \subset R$.
- ◇ For any ideal $\mathfrak{a}$ we have $\dim R \geq \dim(R/\mathfrak{a}) + \operatorname{ht}(\mathfrak{a})$.

Exercise 5.4.2. Verify the last property above.

Exercise 5.4.3. Show that every principal ideal domain which is not a field has dimension one.

More generally, we define the dimension of an R-module M as

$$\dim M := \dim(R/\mathrm{ann}(M)), \quad \dim\{0\} := -\infty.$$

For a short exact sequence $0 \to M' \to M \to M'' \to 0$ we have $\dim M', \dim M'' \leq \dim M$.

Lemma 5.4.4. *Suppose R is Noetherian. The following are equivalent for a finitely generated R-module $M \neq \{0\}$.*

(*i*) $\dim M = 0$.

(*ii*) $R/\mathrm{ann}(M)$ *is Artinian.*

(*iii*) M *has finite length.*

Proof. (i) $\iff$ (ii) is already known: recall that a Noetherian ring is Artinian if and only if its prime ideals are all maximal (Corollary 1.4.3). Let us show (i) or (ii) $\implies$ (iii). By writing $M = M_1 + \cdots + M_n$ where each M_i is generated by one element, we may assume $M \simeq R/\mathfrak{a}$ for some ideal $\mathfrak{a} = \mathrm{ann}(M)$. It has been shown that $R/\mathfrak{a}$ has finite length as a module since it is an Artinian ring.

(iii) $\implies$ (i). Upon modulo $\mathrm{ann}(M)$ we may assume $\mathrm{ann}(M) = \{0\}$. Take any minimal prime $\mathfrak{p}$ in R. As $\mathrm{ann}(M) = \{0\}$ we have $M_{\mathfrak{p}} \neq \{0\}$. Therefore $\mathfrak{p}$ is a minimal element of $\mathrm{Supp}(M)$, hence belongs to $\mathrm{Ass}(M)$. We may embed $R/\mathfrak{p}$ into M. The R-module $R/\mathfrak{p}$ has finite length since M does, therefore $R/\mathfrak{p}$ is an Artinian ring. This implies $\mathfrak{p}$ is a maximal ideal, therefore $\dim R = 0$ since every prime in R lies over a minimal prime. □

Our strategy is to study the Krull dimension via completions and Hilbert polynomials. As a preparation, we begin with the local, or more generally the semi-local rings.

Definition 5.4.5. Let R be a Noetherian semi-local ring (i.e. there are finitely many maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$). Let $M \neq \{0\}$ be a finitely generated R-module. We say an ideal I is a *parameter ideal* for M if $I \subset \mathrm{rad}(R)$ and M/IM has finite length.

Parameter ideals are often called *ideals of definition*. Here we follow the terminologies of [8].

Exercise 5.4.6. Show that I is a parameter ideal for R if and only if there exists k with

$$\mathrm{rad}(R)^k \subset I \subset \mathrm{rad}(R).$$

Show that such an ideal is a parameter ideal for every M. Hint: If $I \supset \mathrm{rad}(R)^k$, every prime ideal $\mathfrak{p} \supset I$ must contain $(\mathfrak{m}_1 \cdots \mathfrak{m}_n)^k$, hence $\mathfrak{p} = \mathfrak{m}_i$ for some i. Conversely, show that in an Artinian ring we have $\mathrm{rad}(R)^k = 0$ for $k \gg 0$, using Corollary 1.4.3. Hint: for Artinian rings, $\mathrm{rad}(R)$ equals the nilpotent radical, and is finitely generated.

Dimension theory for modules can be built solely on the parameter ideals for R, but we opt to introduce the general notion here.

Hereafter we fix a Noetherian semi-local ring R and a finitely generated R-module $M \neq \{0\}$.

Lemma 5.4.7. *An ideal $I \subset \operatorname{rad}(R)$ is a parameter ideal for M if and only if there exists k with $\operatorname{rad}(R)^k \subset I + \operatorname{ann}(M)$. In this case $R/(I + \operatorname{ann}(M))$ is an Artinian ring.*

In particular, $\operatorname{rad}(R)$ is a parameter ideal for any M.

Proof. First we claim that $V(\operatorname{ann}(M/IM)) = \operatorname{Supp}(M/IM)$ equals $V(I + \operatorname{ann}(M))$. By the exactness of localizations together with Nakayama's Lemma, we have

$$\operatorname{Supp}(M/IM) = \operatorname{Supp}(M) \cap \left\{\mathfrak{p} : IR_{\mathfrak{p}} \subsetneq R_{\mathfrak{p}}\right\};$$

the last term equals $\operatorname{Supp}(M) \cap V(I) = V(\operatorname{ann}(M) + I)$, thereby proving our claim. By applying to M/IM the Lemma 5.4.4, $I \subset \operatorname{rad}(R)$ being a parameter ideal for M is equivalent to any one of the following

$$\begin{aligned} \frac{R}{\operatorname{ann}(M/IM)} \text{ is Artinian} &\iff V(\operatorname{ann}(M/IM)) \subset \operatorname{MaxSpec}(R) \\ &\iff V(I + \operatorname{ann}(M)) \subset \operatorname{MaxSpec}(R) \\ &\iff \bar{R} := \frac{R}{I + \operatorname{ann}(M)} \text{ is Artinian.} \end{aligned}$$

If $\bar{R}$ is Artinian, then the image of $\operatorname{rad}(R)$ in $\bar{R}$ is contained in $\operatorname{rad}(\bar{R})$, and we know $\operatorname{rad}(\bar{R})^k = 0$ for large k.

Conversely, suppose $\operatorname{rad}(R)^k \subset I + \operatorname{ann}(M)$. We claim that $R/\operatorname{rad}(R)^k$ is Artinian: $\operatorname{rad}(R)$ contains the product $\mathfrak{m}_1 \cdots \mathfrak{m}_k$ of all maximal ideals, so every over-prime of $\operatorname{rad}(R)^k$ is some $\mathfrak{m}_i$, thus maximal. This shows that M/IM has finite length by the previous equivalences and Lemma 5.4.4. □

Given an parameter ideal I for M. The I-adic grading gives rise to the graded objects

$$\operatorname{gr}_I(R) = \bigoplus_{n\geq 0} \frac{I^n}{I^{n+1}}, \quad \operatorname{gr}_I(M) = \bigoplus_{n\geq 0} \frac{I^n M}{I^{n+1}M}.$$

Recall that

- $\operatorname{gr}_I(R)$ is finitely generated over $\operatorname{gr}_I^0(R) = R/I$ as an algebra and is Noetherian (Proposition 4.4.4);
- more precisely, $\operatorname{gr}_I(R)$ is generated by $\operatorname{gr}_I^1(R)$ over R/I.
- $\operatorname{gr}_I(M)$ is a finitely generated $\operatorname{gr}_I(R)$-module (Proposition 4.4.5);
- the ring $\operatorname{gr}_I^0(R) = R/I$ becomes Artinian after modulo $\operatorname{gr}_I^0(R) \cap \operatorname{ann}(\operatorname{gr}_I(M))$, which contains $(\operatorname{ann}(M) + I)/I$ (use Lemma 5.4.7).

Upon recalling Lemma 5.3.1, it are justified to define

$$\chi(M, I; n) := \ell_{R/I^n}(M/I^n M) = \sum_{j=0}^{n-1} \ell_{R/I}(I^j M/I^{j+1}M), \quad n \in \mathbb{Z}_{\geq 0}.$$

By the theory of Hilbert–Samuel polynomials, $n \mapsto \chi(M, I; n)$ is a polynomial $H_I(M, \cdot)$ whenever $n \gg 0$, with $\deg H_I(M, \cdot)$ bounded by the minimal number of generators of $\operatorname{gr}_I(R)$ over $\operatorname{gr}_I^0(R) = R/I$.

Lemma 5.4.8. *Let $M \neq \{0\}$ be a finitely generated R-module with parameter ideal I.*

(*i*) *The degree $d(M)$ of $H_I(M,\cdot)$ is independent of the choice of the parameter ideal I.*

(*ii*) *In a short exact sequence $0 \to M' \to M \to M'' \to 0$ of finitely generated M-modules, we have*

$$\deg H_I(M',\cdot), \deg H_I(M'',\cdot) \leq \deg H_I(M,\cdot),$$

and $H_I(M,\cdot) - H_I(M',\cdot) - H_I(M'',\cdot)$ has degree $< d(M)$.

Proof. (i): To compare the graded objects associated to two parameter ideals I, J, we apply the characterization in Lemma 5.4.7: it suffices to take $J = \mathrm{rad}(R)$, so that

$$J^m + \mathrm{ann}(M) \subset I + \mathrm{ann}(M) \subset J + \mathrm{ann}(M)$$

for some $m \geq 1$. This implies $\chi(M,J;n) \leq \chi(M,I;n)$ and $\chi(M,I;n) \leq \chi(M,J;mn)$ for all $n \geq 0$. Whence (i).

(ii): For the first part, note that $M/I^nM \to M''/I^nM''$ is surjective, so $\chi(M'',I;n) \leq \chi(M,I;n)$. On the other hand, $M'/I^nM' \to M/I^nM$ has kernel $\frac{M' \cap I^nM}{I^nM'}$. For $n \geq n_0 \gg 0$, Artin–Rees (Theorem 4.5.7) gives

$$\begin{aligned}\ell\left(\frac{M' \cap I^nM}{I^nM'}\right) = \ell\left(\frac{I^{n-n_0}(M' \cap I^{n_0}M)}{I^nM'}\right) &\leq \ell\left(\frac{I^{n-n_0}M'}{I^nM'}\right) \\ &= \ell\left(\frac{M'}{I^nM'}\right) - \ell\left(\frac{M'}{I^{n-n_0}M'}\right) = \chi(M',I;n) - \chi(M',I;n-n_0)\end{aligned}$$

which has degree inferior to $H_I(M',\cdot)$. Hence $\deg H_I(M',\cdot) \leq \deg H_I(M,\cdot)$.

To establish the second part of (ii), we consider $\chi(M,I;n) - \chi(M'',I;n)$ which equals

$$\ell\left(\frac{M}{I^nM}\right) - \ell\left(\frac{M}{M' + I^nM}\right) = \ell\left(\frac{M' + I^nM}{I^nM}\right) = \ell\left(\frac{M'}{M' \cap I^nM}\right).$$

By Artin–Rees, the rightmost term is squeezed between $\ell(M'/I^nM') = \chi(M',I;n)$ and $\ell(M'/I^{n-k}M') = \chi(M',I;n-k)$ for some k independent of $n \gg 0$. Hence $\chi(M,I;n) - \chi(M'',I;n)$ is a polynomial with the same leading term as $\chi(M',I;n)$, for $n \gg 0$. □

Define $s(M)$ to be the smallest integer s such that there exist $t_1, \ldots, t_s \in \mathrm{rad}(R)$ with $M/\sum_{i=1}^s t_iM$ of finite length. In other words, $s(M)$ is the minimal number of generators for parameter ideals for M. Observe that $M/\sum_{i=1}^s t_iM \neq \{0\}$, otherwise Nakayama's Lemma will lead to $M = \{0\}$.

Theorem 5.4.9. *For any finitely generated nonzero R-module M, we have* $\dim M = s(M) = d(M)$. *In particular* $\dim M$ *is finite.*

Proof. We argue inductively on $d(M)$ to show $\dim M \leq d(M)$. If $d(M) = 0$ then $I^nM = I^{n+1}M = \cdots$ for $n \gg 0$. Corollary 4.5.9 implies $I^nM = \{0\}$, hence $M = M/I^nM$ has finite length and $\dim M = 0$ by Lemma 5.4.4.

Now assume $d(M) \geq 1$. Take a minimal $\mathfrak{p} \in \mathrm{Ass}(M)$ verifying $\dim(R/\mathfrak{p}) = \dim M$, so that $R/\mathfrak{p} \hookrightarrow M$. As $d(R/\mathfrak{p}) \leq d(M)$, we are reduced to the case $M = R/\mathfrak{p}$. Consider a chain of prime ideals

$$\mathfrak{p} = \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_m$$

in R. We claim that $m \leq d(R/\mathfrak{p})$. We may surely suppose $m \geq 1$. Take $t \in \mathfrak{p}_1 \setminus \mathfrak{p}_0$. Reduction modulo $Rt + \mathfrak{p}$ yields a prime chain of length $m-1$, namely

$$\frac{\mathfrak{p}_1}{Rt+\mathfrak{p}} \subsetneq \cdots \frac{\mathfrak{p}_m}{Rt+\mathfrak{p}}$$

in $R/(Rt+\mathfrak{p})$. Hence $\dim(R/Rt+\mathfrak{p}) \geq m-1$. In view of the exactness of

$$0 \to R/\mathfrak{p} \xrightarrow{t} R/\mathfrak{p} \to \frac{R}{Rt+\mathfrak{p}} \to 0,$$

Lemma 5.4.8 (ii) implies that $d(R/Rt+\mathfrak{p}) < d(R/\mathfrak{p})$. By induction we deduce $d(R/\mathfrak{p}) > d(R/Rt+\mathfrak{p}) \geq \dim(R/Rt+\mathfrak{p}) \geq m-1$, hence $d(R/\mathfrak{p}) \geq m$ as required.

Next, let us show $s(M) \leq \dim M$. Set $r := \dim M$. We contend that there exist $t_1, \ldots, t_r \in \operatorname{rad}(R)$ such that $M/(t_1, \ldots, t_r)M$ has finite length; therefore $s \leq r$. When $r = 0$ this follows from Lemma 5.4.4. For $r > 0$, we have $\operatorname{rad}(R) \not\subset \mathfrak{p}$ for any minimal $\mathfrak{p} \in \operatorname{Ass}(M)$ verifying $\dim R/\mathfrak{p} = \dim M$, for otherwise $\mathfrak{p}$ will contain, thus equal to a maximal ideal as R is semi-local, and we would get $\dim M = 0$. Using prime avoidance (Proposition 1.1.5 applied to $I := \operatorname{rad}(R)$ and the primes $\mathfrak{p}$ above), we may pick $t_1 \in \operatorname{rad}(R)$ that does not belong to any $\mathfrak{p}$ above. From $\operatorname{ann}(M/t_1M) \supset Rt_1 + \operatorname{ann}(M)$ and our choice of t_1,, we see $\dim M/t_1M < \dim M$. Our claim results from induction on r.

We finish the proof by showing $d(M) \leq s(M)$. Suppose $M/\sum_{i=1}^{s} t_iM \neq \{0\}$ has finite length. We contend that for any $t \in \operatorname{rad}(R)$ we have

$$d(M) \geq d(M/tM) \geq d(M) - 1. \tag{5–3}$$

If this holds, we can look at the sequence $M, M/t_1M, M/(t_1M + t_2M), \ldots$: at each step $d(\cdots)$ drops at most by one; at the end $L := M/\sum_{j=1}^{s} t_jM$ we have $d(L) = 0$: indeed, as L has finite length, $\ell(L/I^nL)$ is uniformly bounded by $\ell(L)$ so that $d(L) = 0$. Thus $d(M) \leq s$ as expected.

To prove (5–3), first note that $d(M) \geq d(M/tM)$ is known. Take any parameter ideal $I \ni t$. We bound $\chi(M/tM, I; n)$ as follows

$$\ell\left(\frac{M}{tM+I^nM}\right) = \ell\left(\frac{M}{I^nM}\right) - \ell\left(\frac{tM+I^nM}{I^nM}\right).$$

Note that

$$\frac{M}{I^{n-1}M} \twoheadrightarrow \frac{M}{\{x \in M : tx \in I^nM\}} \xrightarrow{\sim} \frac{tM}{tM \cap I^nM} \simeq \frac{tM+I^nM}{I^nM}$$
$$y \mapsto ty.$$

Hence $\chi(M/tM, I; n) \geq \chi(M, I; n) - \chi(M, I; n-1)$ for $n \gg 0$, proving the second inequality in (5–3). □

Corollary 5.4.10. *Under the same assumptions, we have* $\dim_R M = \dim_{\hat{R}} \hat{M}$, *where we take I-adic completions.*

Proof. Proposition 5.2.1 gives identifications $\operatorname{gr}_I(R) = \operatorname{gr}_{\hat{I}}(\hat{R})$ and $\operatorname{gr}_I(M) = \operatorname{gr}_{\hat{I}}(\hat{M})$; moreover $\hat{R}$ is still semi-local and $\hat{I}$ is still a parameter ideal for $\hat{M}$ (see Proposition 5.2.4, 5.2.5). Since $d(M)$ and $d(\hat{M})$ are read from these graded modules, they are equal. □

These results will be applied to the case $M = R$ in the next section.

5.5 Krull's theorems and regularity

We still assume R is a Noetherian ring.

Theorem 5.5.1 (Krull). *Suppose $\mathfrak{a} = (t_1, \dots, t_r)$ is a proper ideal of R, then for every minimal over-prime ideal $\mathfrak{p}$ of $\mathfrak{a}$, we have $\operatorname{ht}(\mathfrak{p}) \leq r$.*

From Definition 5.4.1 we infer that $\operatorname{ht}(\mathfrak{a}) \leq r$. The special case $r = 1$ says that every principal ideal $(t) \neq R$ has height at most one (exactly one if t is not a zero divisor — use Theorem 2.2.5 (ii)); this is called the Hauptidealsatz.

Proof. We work in $R_\mathfrak{p}$ and $I := \mathfrak{a}R_\mathfrak{p} = (t_1, \dots, t_r)$. Since $I \subset \operatorname{rad}(R_\mathfrak{p})$ and $R_\mathfrak{p}/I$ has dimension zero, thus Artinian, I is a parameter ideal. We conclude by Theorem 5.4.9 and $\operatorname{ht}(\mathfrak{p}) = \dim R_\mathfrak{p}$. □

Now assume R is Noetherian and local with maximal ideal $\mathfrak{m}$. The parameter ideals of R are precisely those squeezed between $\mathfrak{m}$ and $\mathfrak{m}^k$ for some $k \geq 1$, by Lemma 5.4.7. Set $d := \dim R$, which is finite by Theorem 5.4.9. The same theorem tells us that we can generate some parameter ideal $I \subset \mathfrak{m}$ (namely R/I Artinian) by elements $t_1, \dots, t_d \in \mathfrak{m}$. These elements form a *system of parameters* of R.

Proposition 5.5.2. *Suppose R is a Noetherian local ring with a system of parameters $t_1, \dots, t_d$, which generate a parameter ideal I. For any $0 \leq i \leq d$ we have $\dim(R/(t_1, \dots, t_i)) = d - i$, and $t_{i+1}, \dots, t_d$ form a system of parameters for $R/(t_1, \dots, t_i)$.*

Proof. Consider the sequence $R, R/(t_1), R/(t_1, t_2), \dots, R/(t_1, \dots, t_d)$. Recall the formalism in Theorem 5.4.9: at each stage $d(R/\cdots)$ drops at most by one, by (5–3). After d steps we arrive at R/I with $\dim(\cdot) = d(\cdot) = s(\cdot) = 0$, since it has finite length. Hence d drops exactly by one at each stage. The remaining assertions are immediate. □

A natural question arises: when can we assure $I = \mathfrak{m}$?

Definition 5.5.3. We say a Noetherian local ring R is a *regular local ring* if $\mathfrak{m}$ can be generated by $d = \dim R$ elements $t_1, \dots, t_d$. In this case we say $t_1, \dots, t_r$ form a *regular system of parameters*.

In particular, $\mathfrak{m} = \{0\}$ if R is regular local with $\dim R = 0$.

Exercise 5.5.4. Let $\Bbbk$ be a field. The $\Bbbk$-algebra of formal power series $\Bbbk[\![X_1, \dots, X_d]\!]$ is a regular local ring. Indeed, it is Noetherian with maximal ideal $\mathfrak{m} = (X_1, \dots, X_d)$, and $X_1, \dots, X_d$ form a regular system of parameters. On the other hand, $\mathfrak{m}/\mathfrak{m}^2$ has a $\Bbbk$-basis formed by the images of $X_1, \dots, X_d$. One way to determine its dimension and prove its regularity is to calculate the functions $n \mapsto \dim_\Bbbk(\mathfrak{m}^n/\mathfrak{m}^{n+1})$ explicitly, i.e. count the monomials in d variables with total degree n. You should get a polynomial in n with degree $d - 1$, cf. Exercise 5.3.4.

Theorem 5.5.5. *For any Noetherian local ring R with maximal ideal $\mathfrak{m}$ and residue field $\Bbbk$, we have $\dim R \leq \dim_\Bbbk \mathfrak{m}/\mathfrak{m}^2$. Equality holds if and only if R is a regular local ring.*

The $\Bbbk$-vector space $\mathfrak{m}/\mathfrak{m}^2$ is called the *Zariski cotangent space* of $\operatorname{Spec}(R)$, in honor of Oscar Zariski (1899–1986). Picture taken from Wikimedia Commons.

Proof. By Nakayama's Lemma (more precisely, Corollary 1.3.6), $\mathfrak{m}/\mathfrak{m}^2$ can be generated over $\Bbbk$ by s elements if and only if $\mathfrak{m}$ can be generated over R by s elements, for any $s \in \mathbb{Z}_{\geq 0}$. Hence Theorem 5.4.9 imposes the bound $s \geq \dim R$, and equality holds if and only if R admits a regular system of parameters. □

Due to time constraints, we cannot say too much about regular local rings. Below is one of their wonderful properties.

Theorem 5.5.6. *Regular local rings are integral domains.*

Proof. Induction on $d := \dim R$. If $\dim R = 0$ then $\mathfrak{m} = \{0\}$, hence R is a field. Assume hereafter that $d > 0$. We know there are only finitely many minimal prime ideals and $\dim_{\Bbbk} \mathfrak{m}/\mathfrak{m}^2 \geq 1$. By prime avoidance (Proposition 1.1.5) applied to $I := \mathfrak{m}$, the minimal prime ideals and $\mathfrak{m}^2$, there exists $t \in \mathfrak{m} \setminus \mathfrak{m}^2$ that does not lie in any minimal prime ideal. Put $R' := R/(t)$ with maximal ideal $\mathfrak{m}' = \mathfrak{m}/(t)$; our choice of t together with Proposition 5.5.2 imply

$$\begin{aligned} \dim R' &= \dim R - 1, \\ \dim_{\Bbbk} \mathfrak{m}'/(\mathfrak{m}')^2 &= \dim_{\Bbbk} \mathfrak{m}/\mathfrak{m}^2 - 1 = \dim R - 1. \end{aligned}$$

Hence R' is still regular local, and by induction it is a domain. This implies (t) is prime.

Take any minimal prime $\mathfrak{p}$ below (t); note that $t \notin \mathfrak{p}$ by construction. To show R is a domain it suffices to prove $\mathfrak{p} = \{0\}$. Indeed, every $s \in \mathfrak{p}$ can be written as $s = at$, $a \in R$. Since $t \notin \mathfrak{p}$, we must have $a \in \mathfrak{p}$. Hence $\mathfrak{p} = t\mathfrak{p} \subset \mathfrak{m}\mathfrak{p}$. Nakayama's Lemma (Theorem 1.3.5) implies $\mathfrak{p} = \{0\}$. □

Lecture 6

Dimension of finitely generated algebras

The main reference is [11, §13].

6.1 Dimensions in fibers

Consider a homomorphism $\varphi : A \to B$, which induces $\varphi^\sharp : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ on prime spectra. Given $\mathfrak{p} \in \operatorname{Spec}(A)$, we are interested in the fiber $(\varphi^\sharp)^{-1}(\mathfrak{p})$; the prime ideals $\mathfrak{q}$ therein are described by $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$, or equivalently:

$$\varphi^{-1}(\mathfrak{q}) \cap (A \setminus \mathfrak{p}) = \emptyset, \quad \mathfrak{q} \supset \varphi(\mathfrak{p}).$$

Adopt the convention that a zero ring has $\operatorname{Spec} = \emptyset$. The first condition says that $\mathfrak{q}$ comes from $\operatorname{Spec}(B_\mathfrak{p})$, where $B_\mathfrak{p}$ is the localization with respect to $\varphi(A \setminus \mathfrak{p})$ (possibly zero). The second condition then says that $\mathfrak{q}B_\mathfrak{p}$ lies over the image of $\mathfrak{p}A_\mathfrak{p}$. Set

$$\kappa(\mathfrak{p}) := A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}.$$

The fiber $(\varphi^\sharp)^{-1}(\mathfrak{p})$ is then identified with the spectrum of

$$B \underset{A}{\otimes} \kappa(\mathfrak{p}) = \left(B \underset{A}{\otimes} A_\mathfrak{p}\right) \underset{A_\mathfrak{p}}{\otimes} \kappa(\mathfrak{p}) = B_\mathfrak{p} \underset{A_\mathfrak{p}}{\otimes} (A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}),$$

which is empty if and only if $B \underset{A}{\otimes} \kappa(\mathfrak{p})$ is zero. This also equips $(\varphi^\sharp)^{-1}(\mathfrak{p})$ with an extra structure: it is the spectrum of an explicit quotient ring of $B_\mathfrak{p}$.

Observe that for all $\mathfrak{q} \in (\varphi^\sharp)^{-1}(\mathfrak{p})$, the localization of $B_\mathfrak{p} \underset{A_\mathfrak{p}}{\otimes} \kappa(\mathfrak{p})$ at the image of $\mathfrak{q}$ is canonically isomorphic to $B_\mathfrak{q} \underset{A_\mathfrak{p}}{\otimes} \kappa(\mathfrak{p})$.

Proposition 6.1.1. *Assume A, B to be Noetherian. Let $\mathfrak{q} \in \operatorname{Spec}(B)$ and $\mathfrak{p} := \varphi^\sharp(\mathfrak{q})$. We have*

(*i*) $\dim(B_\mathfrak{q}) \leq \dim(A_\mathfrak{p}) + \dim B_\mathfrak{q} \underset{A_\mathfrak{p}}{\otimes} \kappa(\mathfrak{p})$ (*note that the existence of $\mathfrak{q}$ ensures that $B_\mathfrak{p} \underset{A_\mathfrak{p}}{\otimes} \kappa(\mathfrak{p}) \neq \{0\}$, hence $B_\mathfrak{q} \underset{A_\mathfrak{p}}{\otimes} \kappa(\mathfrak{p}) \neq \{0\}$*);

(*ii*) *equality holds if going-down holds for* φ*;*

(*iii*) *if going-down holds and* $\varphi^\sharp$ *is surjective, then* $\dim(B) \geq \dim(A)$*, and for all ideal* $\mathfrak{a} \subsetneq A$ *we have* $\varphi(\mathfrak{a})B \neq B$ *and* $\operatorname{ht}(\mathfrak{a}) = \operatorname{ht}(\varphi(\mathfrak{a})B)$.

It is crucial to notice that $\dim B_\mathfrak{q} \underset{A_\mathfrak{p}}{\otimes} \kappa(\mathfrak{p}) = \operatorname{ht}(\mathfrak{q}B_\mathfrak{q}/\varphi(\mathfrak{p})B_\mathfrak{q}) = \operatorname{ht}(\mathfrak{q}/\varphi(\mathfrak{p})B)$.

This bounds the source dimension of a morphism by the target dimension plus the fiber dimension, localized both at $\mathfrak{p}$ and $\mathfrak{q} \in (\varphi^\sharp)^{-1}(\mathfrak{p})$. In order to have an equality, a certain submersion-like condition on $\varphi^\sharp$ is evidently required; this explains the going-down condition. Cf. [11, (6.H)].

Proof. We have an induced local homomorphism $A_\mathfrak{p} \to B_\mathfrak{q}$ since $\mathfrak{q} \mapsto \mathfrak{p}$. Since (i) and (ii) depend only on this induced homomorphism, we may assume from the outset that A, B are local with maximal ideals $\mathfrak{p}, \mathfrak{q}$, and φ is a local homomorphism. Let $d := \dim A$ and take a parameter ideal $I = (t_1, \dots, t_d)$ of A, so that $\mathfrak{p}^k \subset I \subset \mathfrak{p}$ for some k. It follows that $\sqrt{\varphi(\mathfrak{p})B} = \sqrt{\varphi(I)B}$, therefore $\dim(B \underset{A}{\otimes} \kappa(\mathfrak{p})) = \dim(B/\varphi(\mathfrak{p})B) = \dim(B/\varphi(I)B)$; denote this number as e. Take a $s_1, \dots, s_e \in \mathfrak{q}$ whose images generate a parameter ideal for $B/\varphi(I)B$, and put $J := (\varphi(t_1), \dots, \varphi(t_d), s_1, \dots, s_e)$. Then B/J is Artinian, therefore $\dim B \leq d + e$ establishes (i).

As for (ii), we conserve the same hypotheses and take a prime chain $\mathfrak{q} = \mathfrak{q}_0 \supsetneq \cdots \supsetneq \mathfrak{q}_e$ with $\mathfrak{q}_e \supset \varphi(\mathfrak{p})B$ in B, as well as a prime chain $\mathfrak{p} = \mathfrak{p}_0 \supsetneq \cdots \supsetneq \mathfrak{p}_d$ in A. Note that $\varphi^{-1}(\mathfrak{q}_e) = \mathfrak{p}$ since $e = \dim B/\varphi(\mathfrak{p})B$. By applying going-down repeatedly to the chain $\mathfrak{p}_i$, we obtain a prime chain in B

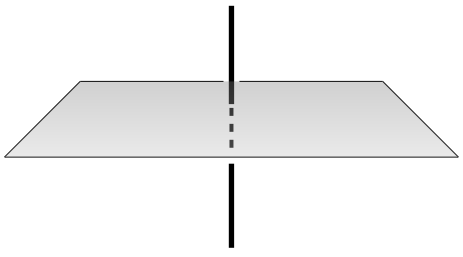
$$\mathfrak{q}_e \supsetneq \cdots \supsetneq \mathfrak{q}_{e+d}, \quad \varphi^{-1}(\mathfrak{q}_{e+i}) = \mathfrak{p}_i.$$

Concatenation with $\mathfrak{q}_0 \supsetneq \cdots$ gives $\dim(B) = d + e$. This shows (ii).

The first assertion of (iii) results from (ii). To show the remaining one, let us show $\varphi(\mathfrak{a})B \neq B$: if $\varphi^\sharp(\mathfrak{q}) = \mathfrak{p} \supset \mathfrak{a}$, then $\mathfrak{q} \supset \varphi(\mathfrak{a})B$. Next, take a minimal over-prime $\mathfrak{q} \supset \varphi(\mathfrak{a})B$ with $\operatorname{ht}(\mathfrak{q}) = \operatorname{ht}(\varphi(\mathfrak{a})B)$. With $\mathfrak{p} := \varphi^{-1}(\mathfrak{q}) \supset \mathfrak{a}$, we must have $\dim B_\mathfrak{q} \otimes \kappa(\mathfrak{p}) = \operatorname{ht}(\mathfrak{q}/\varphi(\mathfrak{p})B) = 0$ by the minimality of $\mathfrak{q}$. An application of (ii) yields

$$\operatorname{ht}(\varphi(\mathfrak{a})B) = \operatorname{ht}(\mathfrak{q}) = \operatorname{ht}(\mathfrak{p}) \geq \operatorname{ht}(\mathfrak{a}).$$

To obtain $\leq$, choose $\mathfrak{p} \supset \mathfrak{a}$ with $\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\mathfrak{a})$ and take $\mathfrak{q} \in \operatorname{Spec}(B)$ with $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$; this implies $\mathfrak{q} \supset \varphi(\mathfrak{p})B \supset \varphi(\mathfrak{a})B$. Upon shrinking $\mathfrak{q}$, we may even assume $\mathfrak{q}$ is minimal over $\varphi(\mathfrak{p})B$, i.e. $\operatorname{ht}(\mathfrak{q}/\varphi(\mathfrak{p})B) = 0$. Using (ii), this entails $\operatorname{ht}(\mathfrak{a}) = \operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\mathfrak{q}) \geq \operatorname{ht}(\varphi(\mathfrak{a})B)$. □



The minimal primes in a ring B may have different heights when the scheme $\operatorname{Spec}(B)$ is not equi-dimensional.

Going-down holds for flat φ by Theorem 4.1.3, therefore the dimension equality

$$\dim(B_{\mathfrak{q}}) = \dim(A_{\mathfrak{p}}) + \dim B_{\mathfrak{q}} \underset{A_{\mathfrak{p}}}{\otimes} \kappa(\mathfrak{p})$$

holds for flat ring homomorphisms.

Remark 6.1.2. In general, if B is a finitely generated algebra over Noetherian A such that $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is a closed map, the fiber dimension $\mathfrak{p} \mapsto \dim B/\mathfrak{p}B$ is an *upper semi-continuous function* on the target space $\operatorname{Spec}(A)$. More concretely, the fiber dimension is non-decreasing under specialization of $\mathfrak{p}$. Cf. [8, §14.3] or [11, (13.E)]. Try to understand this phenomenon intuitively.

Proposition 6.1.3. *Suppose B is integral over a subring A.*

(*i*) *We have* $\dim A = \dim B$.

(*ii*) *If we assume moreover that A, B are both Noetherian, then* $\operatorname{ht}(\mathfrak{q}) \leq \operatorname{ht}(\mathfrak{q} \cap A)$ *for every* $\mathfrak{q} \in \operatorname{Spec}(B)$.

(*iii*) *Furthermore, if going-down also holds for $A \hookrightarrow B$, we have* $\operatorname{ht}(J) = \operatorname{ht}(J \cap A)$ *for every ideal $J \subsetneq B$.*

Proof. Going-up holds and $\operatorname{Spec}(B) \twoheadrightarrow \operatorname{Spec}(A)$ in the situation of (i) by Theorem 4.1.4, hence $\dim B \geq \dim A$ by lifting prime chains. To prove $\leq$, observe that $\mathfrak{q} \subsetneq \mathfrak{q}'$ implies $\mathfrak{q} \cap A \subsetneq \mathfrak{q}' \cap A$ since there are no inclusion relations in the fibers of $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$.

As for (ii), note that $\operatorname{ht}(\mathfrak{q}) \leq \operatorname{ht}(\mathfrak{p}) + \operatorname{ht}(\mathfrak{q}/\mathfrak{p}B)$ where $\mathfrak{p} := \mathfrak{q} \cap A$; as the are no inclusion relations in fibers, the last term must be 0.

Now assume going-down and consider (iii). Take $\mathfrak{q} \in \operatorname{Spec}(B)$ with $\operatorname{ht}(\mathfrak{q}) = \operatorname{ht}(J)$. Put $\mathfrak{p} := \mathfrak{q} \cap A \supset J \cap A$. Again, since there are no inclusions in the fiber over $\mathfrak{p}$ of $\operatorname{Spec}(B) \twoheadrightarrow \operatorname{Spec}(A)$, we have $\dim(B_{\mathfrak{q}}/\mathfrak{p}B_{\mathfrak{q}}) = 0$. Proposition 6.1.1 (ii) implies $\operatorname{ht}(\mathfrak{q}) = \operatorname{ht}(\mathfrak{p})$, therefore $\operatorname{ht}(J) \geq \operatorname{ht}(J \cap A)$.

On the other hand, for any $\mathfrak{p} \supset J \cap A$ with $\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(J \cap A)$, since $A/J \cap A \hookrightarrow B/J$ is integral, there exists $\mathfrak{q} \supset J$ with $\mathfrak{q} \cap A = \mathfrak{p}$. Together with Proposition 6.1.1 (i) and $\operatorname{ht}(\mathfrak{q}/\mathfrak{p}B) = 0$, this implies $\operatorname{ht}(J) \leq \operatorname{ht}(\mathfrak{q}) \leq \operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(J \cap A)$ by (ii). □

6.2 Calculation for polynomial algebras

Let us apply the results from the previous section to elucidate the Krull dimension of polynomial algebras.

Theorem 6.2.1. *Let A be a Noetherian ring, we have* $\dim A[X_1, \dots, X_n] = \dim A + n$ *for any $n \geq 0$. In particular,* $\dim A[X_1, \dots, X_n] = n$ *if A is Artinian (eg. a field).*

Proof. Evidently we may assume $n = 1$. We shall apply Proposition 6.1.1 to $A \hookrightarrow B = A[X]$. Take any $\mathfrak{p} \in \operatorname{Spec}(A)$ and let $\mathfrak{q}$ be a maximal element in $\{\mathfrak{q}' \in \operatorname{Spec}(B) : \mathfrak{q} \cap A = \mathfrak{p}\}$. Put $\kappa := \kappa(\mathfrak{p})$. It suffices to show that $B_{\mathfrak{q}} \underset{A_{\mathfrak{p}}}{\otimes} \kappa$ has dimension one, since B is free hence flat over A, and Proposition 6.1.1 will imply

$$\dim B_{\mathfrak{q}} = \dim A_{\mathfrak{p}} + 1$$

and taking supremum over $\mathfrak{p} \in \operatorname{Spec}(A)$ gives the result.

Indeed, put $B_\mathfrak{p} := B[(A \setminus \mathfrak{p})^{-1}] = A_\mathfrak{p}[X]$ and $\mathfrak{q}' := \mathfrak{q}[(A \setminus \mathfrak{p})^{-1}] \in \operatorname{Spec}(B_\mathfrak{p})$. As $\mathfrak{q}' \supset \mathfrak{p}A_\mathfrak{p}$, we have $\overline{\mathfrak{q}'} := \mathfrak{q}' \supset \mathfrak{p}A_\mathfrak{p} \in \operatorname{Spec}(\kappa[X])$, and $\overline{\mathfrak{q}'}$ is maximal in the fiber over $\{0\}$ of $\operatorname{Spec}(\kappa[X]) \to \operatorname{Spec}(\kappa)$, i.e. in $\operatorname{MaxSpec}(\kappa[X])$. Localization in stages yields

$$B_\mathfrak{q} \underset{A_\mathfrak{p}}{\otimes} \kappa \simeq \frac{B_\mathfrak{q}}{\mathfrak{p}B_\mathfrak{q}} \simeq \left(\frac{B_\mathfrak{p}}{\mathfrak{p}A_\mathfrak{p}B_\mathfrak{p}}\right)_{\mathfrak{q}'} \simeq \kappa[X]_{\overline{\mathfrak{q}'}}.$$

As $\kappa[X]$ is a principal ideal domain which is not a field, every maximal ideal thereof has height one. Hence $\dim \kappa[X]_{\overline{\mathfrak{q}'}} = \operatorname{ht}(\mathfrak{q}') = 1$. □

Corollary 6.2.2. *Let $\Bbbk$ be a field, then for every $0 \leq i \leq n$ we have $\operatorname{ht}(X_1, \dots, X_i) = i$ in $\Bbbk[X_1, \dots, X_n]$.*

Proof. The prime chain $\{0\} \subset (X_1) \subsetneq \cdots \subsetneq (X_1, \dots, X_n)$ has length $n = \dim \Bbbk[X_1, \dots, X_n]$. Thus for each $0 \leq i \leq n$, the chain $\{0\} \subset (X_1) \subsetneq \cdots \subsetneq (X_1, \dots, X_i)$ has maximal length among all prime chains starting with $(X_1, \dots, X_i)$. □

Combined with Theorem 6.2.1, we see that for $\Bbbk$ a field, $R := \Bbbk[X_1, \dots, X_n]$ and $\mathfrak{p} := (X_1, \dots, X_i)$, the equality

$$\operatorname{ht}(\mathfrak{p}) + \dim R/\mathfrak{p} = \dim R.$$

holds. This will be generalized to finitely generated domains over $\Bbbk$.

We record another simple consequence for later use.

Corollary 6.2.3. *Let $\Bbbk$ be a field. Any $\Bbbk$-algebra A with n generators has finite dimension $\leq n$.*

Proof. Writing $A = \Bbbk[X_1, \dots, X_n]/I$ for some ideal I, we have $\dim A \leq \Bbbk[X_1, \dots, X_n]$ since every prime chain in A lifts to $\Bbbk[X_1, \dots, X_n]$. Now apply Theorem 6.2.1. □

6.3 Noether normalization and its consequences

Fix a field $\Bbbk$. A few preparatory results are in order.

Lemma 6.3.1. *Suppose $\Bbbk$ is a field and $t \in \Bbbk[X_1, \dots X_e] \setminus \Bbbk$. There exist $t_1, \dots, t_{e-1} \in \Bbbk[X_1, \dots, X_e]$ such that $\Bbbk[X_1, \dots, X_e]$ is finitely generated as a module over the $\Bbbk$-subalgebra $S := \Bbbk[t_1, \dots, t_{e-1}, t]$.*

Proof. We seek t_i of the form $X_i - X_e^{k^i}$ where k is a large integer. Then t can be uniquely expressed as a polynomial of $t_1, \dots, t_{e-1}, X_e$. We claim that upon modifying t by $\Bbbk^\times$, which is clearly harmless, one can choose k such that t is monic as an element of $\Bbbk[t_1, \dots, t_{e-1}][X_e]$, say of some degree δ. If this is the case,

$$t = X_e^\delta + \sum_{0 \leq j < \delta} (\text{polynomial in } t_1, \dots, t_{e-1})\, X_e^j$$

says that X_e is integral over S, and then $\Bbbk[X_1, \dots, X_e]$ is generated as an S-module by $1, X_e, \dots, X_e^{\delta-1}$.

To choose k, one stares at the expansion

$$X_1^{a_1}\cdots X_e^{a_e} = \left(t_1 + X_e^{k^1}\right)^{a_1}\cdots\left(t_{e-1} + X_e^{k^{e-1}}\right)^{a_{e-1}}\cdot X_e^{a_e} = X_e^{a_e+a_1k^1+\cdots+a_{e-1}k^{e-1}} + \text{mixed terms}.$$

If $k > \max\{a_1,\dots,a_e\}$, the exponent of X_e is simply the base k expression with digits $a_e, a_1, \dots, a_{e-1}$. Now write t as a linear combination of monomials $X_1^{a_1}\cdots X_e^{a_e}$ and expand them in terms of $t_1,\dots,t_{e-1},X_e$. From the observation above, different $(a_1,\dots,a_e)$ contributes a different exponent of X_e whenever $k \gg 0$. Adjusting t by $\Bbbk^\times$, we get the asserted property. □

Lemma 6.3.2. *Let $\mathfrak{a}$ be a nonzero ideal of a domain R, then $\dim(R/\mathfrak{a}) + 1 \le \dim R$.*

Proof. Any prime chain $\mathfrak{p}_0 \supsetneq \cdots \supsetneq \mathfrak{p}_n$ in R with $\mathfrak{p}_n \supset \mathfrak{a}$ can be extended to a prime chain length $n+1$, namely by adjoining $\mathfrak{p}_{n+1} := \{0\}$. □

Theorem 6.3.3 (E. Noether, M. Nagata)**.** *Let B be a finitely generated $\Bbbk$-algebra of dimension n. Consider a chain of proper ideals $I_1 \subsetneq \cdots \subsetneq I_m$, with $\dim(B/I_j) = d_j$ and $d_1 > \cdots > d_m \ge 0$. Then there exist a $\Bbbk$-subalgebra $A \subset B$ together with an isomorphism $A \simeq \Bbbk[X_1,\dots,X_n]$, satisfying*

- *B is a finitely generated A-module, in particular B is integral over A;*
- *$I_j \cap A \simeq (X_{d_j+1},\dots,X_n)$ under the isomorphism above, for each $1 \le j \le m$.*

Note that the assumption $I_j \subsetneq I_{j+1}$ is merely for convenience. Allowing $I_j = I_{j+1}$ and $d_j = d_{j+1}$ for some j is surely possible..

Proof. Write $B = \Bbbk[Y_1,\dots,Y_r]/J$, where $r \ge n$ (Corollary 6.2.3), and denote the preimage of I_j in $\Bbbk[Y_1,\dots,Y_r]$ by $\tilde{I}_j$. The first step is to reduce to the case $J = \{0\}$. To see this, we adjoin $\tilde{I}_0 = \{0\}$ (with $d_0 = n$) into the ideal chain; it may happen that $\tilde{I}_0 = \tilde{I}_1$, but that's harmless. Suppose we can find $\tilde{A} \subset \Bbbk[Y_1,\dots,Y_r]$, $\tilde{A} \simeq \Bbbk[X_1,\dots,X_r]$ with the required properties relative to $\tilde{I}_\bullet$. Taking quotient by J, we obtain the corresponding properties for $I_\bullet$. Indeed, the passage from $\tilde{A}$ to $A := \tilde{A}/(\tilde{A}\cap J)$ truncates the variables $X_{n+1},\dots,X_r$, whereas

$$I_j \cap A = \frac{\tilde{I}_j \cap (\tilde{A}+J)}{J} = \frac{(\tilde{I}_j\cap\tilde{A})+J}{J} \simeq \frac{\tilde{I}_j\cap\tilde{A}}{J\cap\tilde{A}};$$

try to convince yourself of the middle equality.

Secondly, having reduced to the case $B = \Bbbk[Y_1,\dots,Y_r]$ (thus $r = n$), it suffices to pick $x_1,\dots,x_n \in B$ such that

(a) B is finitely generated as a module over $A := \Bbbk[x_1,\dots,x_n]$, and

(b) $I_j \cap A \supset (x_{d_j+1},\dots,x_n)$ for all j.

Indeed, (a) implies $\mathrm{Frac}(A)$ and $\mathrm{Frac}(B)$ have the same transcendence degree n over $\Bbbk$, therefore $x_1,\dots,x_n$ must be algebraically independent over $\Bbbk$. On the other hand, $\dim(B/I_j) = \dim(A/I_j\cap A)$ by (a) and Proposition 6.1.3; but if $I_j\cap A \supsetneq (x_{d_j+1},\dots,x_n)$ then $A/I_j\cap A$ is a proper quotient of the domain $\Bbbk[x_1,\dots,x_{d_j}]$, therefore would have dimension $< d_j$ by Lemma 6.3.2.

We shall construct $x_1,\dots,x_n$ step by step. Suppose $0 \le e \le n$ and that we have produced elements $x_1',\dots,x_e'$ and $x_{e+1},\dots,x_n$ in B satisfying

(i) B is finitely generated as a module over $\Bbbk[x'_1, \dots, x'_e, x_{e+1}, \dots, x_n] =: S_e$;

(ii) $I_j \cap S_e \supset (x_{e+1}, \dots, x_n)$ when $d_j \leq e$;

(iii) $I_j \cap S_e \supset (x_{d_j+1}, \dots, x_n)$ when $d_j \geq e$ (with $j = 1, \dots, m$).

For the initial case $e = n$, simply take $x'_i := Y_i$. Our aim is $e = 0$. Let us explain the induction step from $e \geq 1$ to $e-1$. The prior argument based on transcendence degrees implies the algebraic independence among

$$x'_1, \dots, x'_e, x_{e+1}, \dots, x_n.$$

If $e \leq d_j$ for all j, we are done. Otherwise set $j := \min\{j' : e > d_{j'}\}$, we contend that

$$I_j \cap \Bbbk[x'_1, \dots, x'_e] \neq \{0\}.$$

If not, we would have $I_j \cap S_e = (x_{e+1}, \dots, x_n)$ since $I_j \cap S_e \supset (x_{e+1}, \dots, x_n)$ by (ii). We have $\dim(S_e/I_j \cap S_e) = \dim(B/I_j) = d_j$ by integrality, whilst $\dim(S_e/(x_{e+1}, \dots, x_n)) = e$. Contradiction.

Now take $x_e \in I_j \cap \Bbbk[x'_1, \dots, x'_e] \setminus \{0\}$. Note that $x_e \notin \Bbbk$ as $I_j \neq B$. By Lemma 6.3.1, we may choose $x''_1, \dots, x''_{e-1} \in \Bbbk[x'_1, \dots, x'_e]$ such that $\Bbbk[x'_1, \dots, x'_e]$ is finitely generated over $\Bbbk[x''_1, \dots, x''_{e-1}, x_e]$ as a module. It remains to verify that the new sequence

$$x''_1, \dots, x''_{e-1}, x_e, \dots, x_n$$

satisfies (i)—(iii) above with $e-1$ replacing e.

First, S_e is a finitely generated module over its subalgebra $\Bbbk[x''_1, \dots, x_n]$ by construction, hence so is B and (i) follows. Next, let $1 \leq j' \leq m$. If $d_{j'} > e-1$, the procedure above does not affect $x_{d_j+1}, \dots, x_n$, so they belong to $I_{j'} \cap \Bbbk[x''_1, \dots, x_n]$. If $d_{j'} < e$, setting $j := \min\{j'' : e > d_{j''}\}$ we have $j' \geq j$ and

$$I_{j'} \cap \Bbbk[x''_1, \dots, x_n] \supset I_j \cap \Bbbk[x''_1, \dots, x_n] \supset (x_{e+1}, \dots, x_n) + (x_e).$$

All in all, we obtain (ii) and (iii). □

Corollary 6.3.4 (Dimension formula)**.** *Let B be a finitely generated algebra over a field $\Bbbk$. Suppose B is a domain, then for all $\mathfrak{q} \in \operatorname{Spec}(B)$ we have*

$$\dim(B/\mathfrak{q}) + \operatorname{ht}(\mathfrak{q}) = \dim B.$$

Proof. Choose a subalgebra A of B as in Theorem 6.3.3 and put $\mathfrak{p} = \mathfrak{q} \cap A$. Since B is a domain and A is normal, the Cohen–Seidenberg Theorem 4.1.4 asserts the going-down property for $A \hookrightarrow B$. Proposition 6.1.3 implies that $\dim A = \dim B$, $\dim A/\mathfrak{p} = \dim B/\mathfrak{q}$ and $\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\mathfrak{q})$, so we are again reduced to the case $B = \Bbbk[X_1, \dots, X_n]$ and $\mathfrak{q} = (X_{d+1}, \dots, X_n)$. This is known by Corollary 6.2.2. □

The dimension formula allows us to compute $\dim B$ by choosing any prime $\mathfrak{q}$, a prime chain of longest length below $\mathfrak{q}$ (i.e. in $B_\mathfrak{q}$) and another one above $\mathfrak{q}$ (i.e. in $B/\mathfrak{q}$); their concatenation will then be a prime chain in B with maximal length $\dim B$. By applying the dimension formula to $\mathfrak{q}, \mathfrak{q}' \subset B$ and to $\mathfrak{q}'/\mathfrak{q} \subset B/\mathfrak{q}$, it follows that $\operatorname{ht}(\mathfrak{q}') = \operatorname{ht}(\mathfrak{q}) + \operatorname{ht}(\mathfrak{q}'/\mathfrak{q})$ for all $\mathfrak{q}' \supsetneq \mathfrak{q}$ in B.

For a general Noetherian domain B, we call a prime chain *maximal* if it is not properly contained in any prime chain. A priori, a maximal prime chain does not necessarily have length equal to $\dim B$. If

$$\forall \mathfrak{q}' \supset \mathfrak{q} : \text{primes}, \quad \operatorname{ht}(\mathfrak{q}') = \operatorname{ht}(\mathfrak{q}) + \operatorname{ht}(\mathfrak{q}'/\mathfrak{q}),$$

we say B is a *catenary* domain. This means that $\operatorname{ht}(\mathfrak{q}'/\mathfrak{q}) = \dim B_{\mathfrak{q}'}/\mathfrak{q}B_{\mathfrak{q}'}$ is the common length of all maximal prime chains between $\mathfrak{q}'$ and $\mathfrak{q}$. In particular, maximal prime chains in $B_{\mathfrak{q}'}$ are automatically longest. As shown above, finitely generated domains over a field are catenary. For a finer analysis of catenary and universally catenary rings, we refer to [11, §14].

Corollary 6.3.5. *Suppose B is a domain finitely generated over a field $\Bbbk$. Set $L := \operatorname{Frac}(B)$. Then $\dim B = \operatorname{tr.deg}_{\Bbbk}(L)$ and it is the common length of maximal prime chains.*

Proof. Choose a subalgebra A of B as in Theorem 6.3.3. Since the field $\operatorname{Frac}(B)$ is a finite extension of $\operatorname{Frac}(A)$ and $\dim A = \dim B$ by Proposition 6.1.3, the first assertion reduces immediately to the case $B = \Bbbk[X_1, \dots, X_n]$, which is obvious. As to the second assertion, consider a maximal prime chain $\mathfrak{q}_0 \supsetneq \cdots \supsetneq \mathfrak{q}_n = \{0\}$ in B. Maximality implies $\operatorname{ht}(\mathfrak{q}_i/\mathfrak{q}_{i+1}) = 1$ for all i and $\dim B/\mathfrak{q}_0 = 0$. Applying Corollary 6.3.4 repeatedly, we see

$$\dim B = \dim B/\mathfrak{q}_n = \dim B/\mathfrak{q}_{n-1} + \operatorname{ht}(\mathfrak{q}_{n-1}/\mathfrak{q}_n) =$$
$$\dim B/\mathfrak{q}_{n-2} + \operatorname{ht}(\mathfrak{q}_{n-1}/\mathfrak{q}_{n-2}) + \operatorname{ht}(\mathfrak{q}_{n-1}/\mathfrak{q}_n) = \cdots = \dim B/\mathfrak{q}_0 + \sum_{i=0}^{n-1} \operatorname{ht}(\mathfrak{q}_i/\mathfrak{q}_{i+1})$$

which equals n. □

Remark 6.3.6. Recall that finitely generated domains over an algebraically closed field $\Bbbk$ are objects "opposite" to the irreducible affine $\Bbbk$-varieties. It is instructive to make a comparison with the analytic theory when $\Bbbk = \mathbb{C}$. Let $\mathcal{X}$ be a compact connected complex manifold of (complex) dimension n. Denote by $\mathcal{M}(\mathcal{X})$ the field of meromorphic functions on $\mathcal{X}$. Siegel proved that $\operatorname{tr.deg}_{\mathbb{C}}(\mathcal{M}(\mathcal{X})) \leq n$. When $\mathcal{X}$ is a projective algebraic $\mathbb{C}$-variety, equality holds and we have $\mathcal{M}(\mathcal{X}) = \operatorname{Frac}(A)$ if $\operatorname{Spec}(A)$ is any open dense affine subscheme in $\mathcal{X}$. In general, the abundance of meromorphic functions on $\mathcal{X}$ is a subtle issue, cf. the case of Riemann surfaces ($n = 1$). Compact connected complex manifolds with $\operatorname{tr.deg}_{\mathbb{C}}(\mathcal{M}(\mathcal{X})) = \dim_{\mathbb{C}} \mathcal{X}$ are called *Moishezon manifolds*.

Non-algebraic Moishezon manifolds do exist, and Moishezon proved that a Moishezon manifold is projective, hence algebraic, if and only if it is Kähler. Following M. Artin and D. Knutson, one can enlarge the category of $\mathbb{C}$-schemes into that of *algebraic spaces* over $\mathbb{C}$, and there is an analytification functor $\mathcal{X} \mapsto \mathcal{X}_{\text{an}}$ that sends algebraic spaces of finite type over $\mathbb{C}$ to complex analytic varieties. M. Artin [2, §7] showed that the analytification establishes an equivalence between the category of smooth proper algebraic spaces of finite type over $\mathbb{C}$ and that of Moishezon manifolds. Therefore, such manifolds still retain an algebraic flavor: they are quotients of certain $\mathbb{C}$-schemes by étale equivalence relations.

Lecture 7

Serre's criterion for normality and depth

References: [8, §11] and [3, X.1]. Except in the last section, we will try to avoid the use of depth as in [8].

7.1 Review of discrete valuation rings

Let R be an integral domain.

Definition 7.1.1. A *discrete valuation* on a field K is a surjective map $v : K^\times \to \mathbb{Z}$ such that

- $v(xy) = v(x) + v(y)$, and
- $v(x+y) \geq \min\{v(x), v(y)\}$

for all $x, y \in K^\times$, where we set $v(0) = +\infty$ for convenience. We say a domain R with $K := \mathrm{Frac}(R)$ is a *discrete valuation ring*, abbreviated as DVR, if there exists a discrete valuation v such that

$$R = v^{-1}([0, +\infty]).$$

We say $t \in R$ is a *uniformizer* if $v(t) = 1$.

It follows immediately that $R^\times = v^{-1}(0)$. Uniformizers are unique up to $R^\times$. Note that $v(K^\times) = \mathbb{Z}$ implies that R cannot be a field.

Example 7.1.2. The ring $\mathbb{Z}_p$ of p-adic integers (p: prime number) together with the usual p-adic valuations are standard examples of DVR. The algebra of formal power series $\Bbbk[\![X]\!]$ are also DVR: the valuation of $\sum_n a_n X^n$ is the smallest n such that $a_n \neq 0$.

More generally, in the geometric context, discrete valuations can be defined by looking at the vanishing order of rational/meromorphic functions along subvarieties of codimension one with suitable regularities.

Lemma 7.1.3. *Let R be a discrete valuation ring with valuation v and uniformizer t. Every ideal $\mathfrak{a} \neq \{0\}$ of R has the form (t^r) for a unique $r \geq 0$. In particular, R is a local principal ideal domain which is not a field, hence is of dimension 1.*

Proof. Take $r := \min\{v(x) : x \in \mathfrak{a}\}$. □

In the exercises below, we assume R is a discrete valuation ring with valuation v.

Exercise 7.1.4. Show that t is a uniformizer if and only if it generates the maximal ideal of R.

Exercise 7.1.5. Reconstruct v from the ring-theoretic structure of R.

Recall that a regular local ring R with $\dim R = 1$ is a Noetherian local ring whose maximal ideal $\mathfrak{m}$ is principal and nonzero; elements generating $\mathfrak{m}$ are called the regular parameters for R.

Proposition 7.1.6. *Suppose t is a regular parameter in a regular local ring R of dimension one, then R is a domain, and every element $x \in R \setminus \{0\}$ can be uniquely written as $x = t^r u$ with $r \geq 0$ and $u \in R^\times$. This makes R into a discrete valuation ring by setting $v(x) = r$, for which t is a uniformizer.*

Therefore R is a discrete valuation ring. Conversely, every discrete valuation ring is regular local of dimension 1.

Proof. From Theorem 5.5.6 we know regular local rings are Noetherian domains. By applying Krull's Intersection Theorem (Corollary 4.5.10) to the powers of (t), we see that $r := \sup\{k \geq 0 : x \in (t)^k\}$ is finite. Write $x = t^r u$. Since $R^\times = R \setminus \mathfrak{m}$, we see $u \in R^\times$. As to uniqueness, suppose $t^r u = t^s w$ with $r \geq s$, then $t^{r-s} = u^{-1}w \in R^\times$ implies $r = s$, hence $u = w$ as R is a domain. As every element of $\mathrm{Frac}(R)^\times$ is uniquely expressed as $t^r u$ with $r \in \mathbb{Z}$, one readily checks that $v(t^r u) = r$ satisfies all the requirements of discrete valuation.

The converse direction has been addressed in Lemma 7.1.3. □

To recap, in dimension one we have

$$\text{regular local ring} \iff \text{discrete valuation ring}.$$

This will be related to normality later on.

Exercise 7.1.7. Explain that the regular local rings of dimension 0 are just fields.

7.2 Auxiliary results on the total fraction ring

Let R be a ring, henceforth assumed Noetherian. If there exist a non zero-divisor $t \in R$ and $\mathfrak{p} \in \mathrm{Ass}(R/(t))$, we say $\mathfrak{p}$ is *associated to a non zero-divisor*.

Lemma 7.2.1. *Let M be a finitely generated R-module. An element $x \in M$ is zero if and only if its image in $M_\mathfrak{p}$ is zero for every maximal element $\mathfrak{p}$ in* $\mathrm{Ass}(M)$.

Proof. Suppose $x \neq 0$. Since M is Noetherian, among ideals of the form $\mathrm{ann}(y)$ there is a maximal one containing $\mathrm{ann}(x)$, and we have seen in Lemma 2.2.3 that such an ideal $\mathfrak{p}$ belongs to $\mathrm{Ass}(M)$. Since $\mathrm{ann}(x) \subset \mathfrak{p}$, we have $x/1 \in M_\mathfrak{p} \setminus \{0\}$. □

Call a ring *reduced* if it has no nilpotent element except zero.

Lemma 7.2.2. *Suppose R is reduced, then* $\mathrm{Ass}(R)$ *consists of minimal primes.*

Proof. As R is reduced, $\{0\} = \sqrt{0_R}$ is the intersection of minimal prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ (all lying in $\mathrm{Ass}(R)$, hence finite in number). By the theory of primary decompositions, one infers that $\mathrm{Ass}(R) = \{\mathfrak{p}_1, \ldots\}$. □

For the next result, we denote by T the set of non zero-divisors of R. Recall that the *total fraction ring* $K(R)$ is $R[T^{-1}]$; this is the largest localization such that $R \to K(R)$ is injective, and $K(R) = \mathrm{Frac}(R)$ when R is a domain. The map $\mathfrak{p} \mapsto \mathfrak{p}K(R)$ sets up an order-preserving bijection $\mathrm{Ass}(R) \xrightarrow{\sim} \mathrm{Ass}(K(R))$: indeed, if $\mathfrak{p} \ni t$ for some $t \in T$, then $\mathfrak{p}$ cannot belong to $\mathrm{Ass}(R)$ because the union of $\mathrm{Ass}(R)$ equals $R \setminus T$.

Lemma 7.2.3. *Let R be reduced. Then $K(R) \xrightarrow{\sim} \prod_{\mathfrak{p}} K(R/\mathfrak{p})$ as R-algebras, where $\mathfrak{p}$ ranges over the minimal prime ideals of R. For any multiplicative subset $S \subset R$ there is a canonical isomorphism of $R[S^{-1}]$-algebras*

$$K(R[S^{-1}]) \xrightarrow{\sim} K(R)[S^{-1}].$$

In other words, the formation of total fraction ring commutes with localizations.

Proof. Each element in $K(R) = R[T^{-1}]$ is either a zero-divisor or invertible. The set of zero-divisors of $K(R)$ is the union of minimal prime ideals $\mathfrak{p}_i K(R)$ of $K(R)$ (where $\mathrm{Ass}(R) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ by an earlier discussion), therefore each prime ideal of $K(R)$ must equal some $\mathfrak{p}_i K(R)$, by prime avoidance (Proposition 1.1.5). Hence $\mathfrak{p}_1 K(R), \ldots, \mathfrak{p}_m K(R)$ are also the maximal ideals in $K(R)$, with zero intersection. Chinese Remainder Theorem entails that $K(R) \simeq \prod_{i=1}^{m} K(R)/\mathfrak{p}_i K(R)$. To conclude the first part, notice that $K(R)/\mathfrak{p}_i K(R) = (R/\mathfrak{p}_i)[T^{-1}]$; this is a field in generated by an isomorphic copy of $R/\mathfrak{p}_i$ since $\mathfrak{p}_i \cap T = \emptyset$, hence equals $\mathrm{Frac}(R/\mathfrak{p}_i)$.

As for the second part, one decomposes $K(R[S^{-1}])$ and $K(R)[S^{-1}]$ by the previous step, noting that

- $R[S^{-1}]$ is reduced;
- $\mathrm{Ass}(R[S^{-1}]) = \left\{\mathfrak{p}_i R[S^{-1}] : 1 \leq i \leq m,\ \mathfrak{p}_i \cap S = \emptyset\right\}$ consists of minimal primes;
- $K\left(R[S^{-1}]/\mathfrak{p}_i R[S^{-1}]\right) \simeq K(R/\mathfrak{p}_i) = K(R/\mathfrak{p}_i)[S^{-1}]$ when $\mathfrak{p}_i \cap S = \emptyset$, by the arguments above;
- $K(R/\mathfrak{p}_i)[S^{-1}] = \{0\}$ when $\mathfrak{p}_i \cap S \neq \emptyset$.

A term-by-term comparison finishes the proof. □

We use Lemma 7.2.3 to interchange $K(\cdot)$ and localizations in what follows.

Lemma 7.2.4. *Suppose R is reduced. Then $x \in K(R)$ belongs to R if and only if its image in $K(R)_{\mathfrak{p}} = K(R_{\mathfrak{p}})$ belongs to $R_{\mathfrak{p}}$ for every prime $\mathfrak{p}$ associated to a non zero-divisor.*

Proof. Only the "if" direction requires a proof. Write $x = a/t$ with t not a zero-divisor. Suppose that $a \notin (t)$, i.e. a does not map to zero in $R/(t)$. Lemma 7.2.1 asserts there exists $\mathfrak{p} \in \mathrm{Ass}(R/(t))$ such that a does not map to $0 \in (R/(t))_{\mathfrak{p}} = R_{\mathfrak{p}}/tR_{\mathfrak{p}}$. It follows that the image of a/t in $K(R_{\mathfrak{p}})$ does not lie in $R_{\mathfrak{p}}$. □

7.3 On normality

Fix a Noetherian ring R.

Exercise 7.3.1. Suppose R is a domain, $K := \mathrm{Frac}(R)$. If $R = \bigcap_{i\in I} R_i$ where $\{R_i \subset K\}_{i\in I}$ are subrings such that $\mathrm{Frac}(R_i) = K$ and R_i is normal, for each i, then R is normal.

Proposition 7.3.2. *Let R be a Noetherian domain. Then R is normal if and only if for every principal ideal $(t) \subset R$ and every $\mathfrak{p} \in \mathrm{Ass}(R/(t))$, the ideal $\mathfrak{p}R_\mathfrak{p}$ is principal.*

Proof. Assume the conditions above. To prove the normality of R, it suffices to use $R = \bigcap R_\mathfrak{p}$ where $\mathfrak{p}$ ranges over the primes associated to nonzero principal ideals (consequence of Lemma 7.2.4). Indeed, each $R_\mathfrak{p}$ is regular, hence normal by Proposition 7.1.6, therefore so is their intersection by the previous exercise.

Conversely, assume R is normal and let $\mathfrak{p} \in \mathrm{Ass}(R/(t))$ with $t \neq 0$, we have to show $\mathfrak{p}R_\mathfrak{p}$ is principal. Upon replacing R by $R_\mathfrak{p}$ and recalling how associated primes behave under localization, we may even assume R is local with maximal ideal $\mathfrak{p}$. Express $\mathfrak{p}$ as the annihilator of some $\bar{x} \in R/(t)$ with $x \in R$. Define the fractional ideal

$$\mathfrak{p}^{-1} := \{y \in \mathrm{Frac}(R) : y\mathfrak{p} \subset R\}.$$

It is an R-submodule of $\mathrm{Frac}(R)$ containing R. Define the R-submodule $\mathfrak{p}^{-1}\mathfrak{p}$ of $\mathrm{Frac}(R)$ in the obvious way. Clearly $\mathfrak{p} \subset \mathfrak{p}^{-1}\mathfrak{p} \subset R$. By maximality of $\mathfrak{p}$, exactly one of the $\subset$ is equality. If $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$, every element of $\mathfrak{p}^{-1}$ is integral over R, hence $\mathfrak{p}^{-1} \subset R$ by normality (integrality is "witnessed" by the module $\mathfrak{p}$). From $\mathfrak{p}x \subset (t)$ we see $x/t \in \mathfrak{p}^{-1} = R$; this would imply $\bar{x} = 0$ and $\mathfrak{p} = R$, which is absurd.

Therefore we must have $\mathfrak{p}\mathfrak{p}^{-1} = R$. This implies that $\mathfrak{p}y \not\subset \mathfrak{p}$ for some $y \in \mathfrak{p}^{-1}$, hence $\mathfrak{p}y = R$ since R is local. Hence $\mathfrak{p} = y^{-1}R \simeq R$ is principal. □

Corollary 7.3.3. *The following are equivalent for a local domain R:*

(*i*) *R is normal of dimension* 1*;*

(*ii*) *R is a regular local ring of dimension* 1*;*

(*iii*) *R is a discrete valuation ring.*

Proof. (iii) $\implies$ (i). We have seen that discrete valuation rings are principal ideal rings of dimension 1, therefore also normal by unique factorization property.

(i) $\implies$ (ii). Under the normality assumption, choose any $t \in R \setminus \{0\}$. Since $\dim R = 1$ and $\{0\}$ is a prime ideal, the associated prime of (t) can only be the maximal ideal $\mathfrak{m}$, which is principal by Proposition 7.3.2. This shows that R is regular local.

(ii) $\implies$ (iii) is included in Proposition 7.1.6. □

Corollary 7.3.4. *Let R be a Noetherian normal domain. Then*

$$R = \bigcap_{\mathrm{ht}(\mathfrak{p})=1} R_\mathfrak{p}$$

inside $\mathrm{Frac}(R)$.

Proof. Evidently $\subset$ holds. By Lemma 7.2.4 together with Proposition 7.3.2, R can be written as an intersection of $R_{\mathfrak{p}}$ where $\mathfrak{p}$ is associated to some non zero-divisor, such that $\mathfrak{p}R_{\mathfrak{p}}$ is principal; it suffices to show $\operatorname{ht}(\mathfrak{p}) = 1$. From $\mathfrak{p} \neq \{0\}$ we see $\operatorname{ht}(\mathfrak{p}) \geq 1$; on the other hand, by Hauptidealsatz or by the discussion on regular local rings, we see $\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\mathfrak{p}R_{\mathfrak{p}}) \leq 1$. □

7.4 Serre's criterion

Lemma 7.4.1. *Let R be a Noetherian ring. Suppose that*

- ◇ *the primes in $\operatorname{Ass}(R)$ are all minimal, and*
- ◇ *$R_{\mathfrak{p}}$ is a field for every minimal prime ideal $\mathfrak{p}$,*

then R is reduced.

Proof. Take a minimal primary decomposition $\{0\} = I_1 \cap \cdots \cap I_m$ with $\operatorname{Ass}(R/I_j) = \{\mathfrak{p}_j = \sqrt{I_j}\}$ and $\operatorname{Ass}(R) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$. By the properties of primary ideals, $\mathfrak{p}_j = \sqrt{I_j} \supset I_j$ for all j. By assumption each $\mathfrak{p}_j$ is minimal, and $R_{\mathfrak{p}_j}$ is a field. From the uniqueness of non-embedded components in primary decompositions, $I_j = \ker\left[R \to R_{\mathfrak{p}_j}\right]$ is a prime contained in $\mathfrak{p}_j$, hence $I_j = \mathfrak{p}_j$. We deduce that $\{0\} = \bigcap_{j=1}^{m} \mathfrak{p}_j$, thereby showing $\sqrt{0_R} = \{0\}$. □

Theorem 7.4.2 (J.-P. Serre)**.** *A Noetherian ring R is a finite direct product of normal domains if and only if the following two conditions hold.*

- ▷ ***R1*** *The localization of R at every prime ideal of height 1 (resp. 0) is a discrete valuation ring (resp. a field).*
- ▷ ***S2*** *For every non zero-divisor t of R, the primes in $\operatorname{Ass}(R/(t))$ are all of height 1; the primes in $\operatorname{Ass}(R)$ are all of height 0.*

The condition **R1** means regularity in codimension ≤ 1. The condition **S2** is often rephrased in terms of *depth*, which will be discussed in Proposition 7.5.11.

Proof. We begin with the $\Longrightarrow$ direction. Suppose $R = R_1 \times \cdots \times R_n$ where each R_i is a normal domain. As is well-known, $\operatorname{Spec}(R) = \bigsqcup_{i=1}^{n} \operatorname{Spec}(R_i)$ as topological spaces: to be precise, the elements of $\operatorname{Spec}(R)$ take the form $\mathfrak{p} = R_1 \times \cdots \times \mathfrak{p}_i \times \cdots \times R_n$, where $\mathfrak{p}_i \in \operatorname{Spec}(R_i)$. We have

$$\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\mathfrak{p}_i), \quad R_{\mathfrak{p}} \simeq (R_i)_{\mathfrak{p}_i}.$$

Furthermore, one easily checks that

$$\operatorname{Ass}(R/(t)) = \bigsqcup_{i=1}^{n} \operatorname{Ass}(R_i/(t_i)), \quad t = (t_1, \ldots, t_n) \in R$$

compatibly with the description above.

This reduces the verification of **S2** to the case of normal domains, which is addressed in Proposition 7.3.2. The condition **R1** is implied by Corollary 7.3.3 since normality is preserved under localizations.

Assume conversely **R1** and **S2**. They imply the conditions of Lemma 7.4.1, hence R is reduced. Now for every prime $\mathfrak{p}$ associated to a non zero-divisor, we have $\mathrm{ht}(\mathfrak{p}) = 1$ and $R_{\mathfrak{p}}$ is a normal domain by **R1** $\wedge$ **S2**. By Lemma 7.2.4 (as R is reduced), R is integrally closed in $K(R)$: indeed, if $x \in K(R)$ is integral over R, so is its image in $K(R_{\mathfrak{p}}) = K(R)_{\mathfrak{p}}$ for every $\mathfrak{p}$ as above, therefore lies in $R_{\mathfrak{p}}$. Decompose $K(R) = \prod_{i=1}^{m} K(R/\mathfrak{p}_i)$ as in Lemma 7.2.3. The idempotents $e_i \in K(R)$ associated to this decomposition are trivially integral over R: $e_i^2 - e_i = 0$, hence $e_i \in R$ for all i. It follows that $R = Re_1 + \cdots + Re_m \prod_{i=1}^{m} Re_i \subset K(R)$ and one easily checks that $Re_i = R/\mathfrak{p}_i$.

Finally, since R is integrally closed in $K(R)$, the decomposition above implies $R/\mathfrak{p}_i$ is integrally closed in $K(R/\mathfrak{p}_i)$. All in all, we have written R as a direct product of normal domains. □

Exercise 7.4.3. Recall that for an R-module M, a prime ideal $\mathfrak{p} \in \mathrm{Ass}(M)$ is called *embedded* if $\mathfrak{p}$ is not a minimal element in $\mathrm{Ass}(M)$. Show that for $M = R$, embedded primes are primes in $\mathrm{Ass}(R)$ with height > 0. For $M = R/(t)$ where t is not a zero-divisor, embedded primes are primes in $\mathrm{Ass}(R/(t))$ with height > 1. Use this to rephrase **S2** as follows: there are no embedded primes in $\mathrm{Ass}(R/(t))$ (t not a zero-divisor) or in $\mathrm{Ass}(R)$.

Exercise 7.4.4. Suppose a ring R is isomorphic to a direct product $\prod_{i\in I} R_i$. Show that R is a domain if and only if $|I| = 1$ (say $I = \{i_0\}$), and R_{i_0} is a domain.

Corollary 7.4.5. *A Noetherian domain R is normal if and only if **R1** and **S2** hold for R.*

Proof. Immediate from the previous exercise and Theorem 7.4.2. □

7.5 Introduction to depth

Based on [3], we give a brief account on the notion of depth. Let R be a ring and M be an R-module, $M \neq \{0\}$. Recall the Ext-functors

$$\mathrm{Ext}^n_R(X, Y) := H^n(R\mathcal{H}\mathrm{om}(X, Y)) = \mathrm{Hom}_{D^+(R\text{-Mod})}(X, Y[n]).$$

Definition 7.5.1 (Depth of a module)**.** Let I be a proper ideal of R. We define the *depth* of M relative to I as

$$\mathrm{depth}_I(M) := \inf\left\{n \geq 0 : \mathrm{Ext}^n_R(R/I, M) \neq 0\right\}$$

with values in $\mathbb{Z}_{\geq 0} \sqcup \{+\infty\}$.

Proposition 7.5.2. *For I, M as above, the following are equivalent:*

(*i*) $\mathrm{depth}_I(M) = 0$;

(*ii*) *for all $x \in I$, the homomorphism $M \xrightarrow{x} M$ is not injective;*

(*iii*) $\mathrm{Ass}(M) \cap V(I) \neq \emptyset$.

Proof. In each case we have $M \neq \{0\}$. If (i) holds, then $M \xrightarrow{x} M$ vanishes on the image of some nonzero $R/I \to M$, hence (ii). If (ii) holds, the union of $\mathrm{Ass}(M)$ will cover I, and (iii) follows by prime avoidance. Finally, suppose $\mathfrak{p} \in \mathrm{Ass}(M) \cap V(I)$, there is an embedding $R/\mathfrak{p} \hookrightarrow M$, which yields a non-zero $R/I \to M$. □

Definition 7.5.3. A sequence $x_1, \dots, x_n \in R$ is called an *M-regular sequence* of length n if $(x_1, \dots, x_n)M \subsetneq M$ and

$$0 \to M/(x_1, \dots, x_{k-1}) \xrightarrow{x_k} M/(x_1, \dots, x_{k-1})$$

is exact for all $1 \leq k \leq n$.

Lemma 7.5.4. *Let M be an R-module, $x_1, \dots, x_r$ be an M-regular sequence lying in an ideal $I \subsetneq R$. We have* $\mathrm{depth}_I(M) = r + \mathrm{depth}_I(M/(x_1, \dots, x_r)M)$.

Proof. The case $r = 1$ follows by staring at the long exact sequence attached to $0 \to M \xrightarrow{x_1} M \to M/x_1M \to 0$. The general case follows by induction on r. □

Theorem 7.5.5. *Assume R Noetherian, M finitely generated and $I \subsetneq R$.*

(*i*) $\mathrm{depth}_I(M)$ *is the supremum of the lengths of M-regular sequences with elements in I.*

(*ii*) *Suppose* $\mathrm{depth}_I(M) < +\infty$. *Every M-regular sequence with elements in I can be extended to one of length* $\mathrm{depth}_I(M)$.

(*iii*) *The depth of M relative to I is finite if and only if $V(I) \cap \mathrm{Supp}(M) \neq \emptyset$, or equivalently $IM \neq M$.*

Proof. To prove (i) and (ii), by the previous Lemma we are reduced to show that $\mathrm{depth}_I(M) > 0$ implies the existence of $x \in I$ which is not a zero-divisor of M; this follows from Proposition 7.5.2.

Now pass to the word "equivalently" in (iii). We have $M \neq IM$ if and only if $(M/IM)_\mathfrak{p} = M_\mathfrak{p}/I_\mathfrak{p}M_\mathfrak{p} \neq 0$ for some prime ideal $\mathfrak{p}$. That quotient always vanishes when $\mathfrak{p} \not\supset I$, in which case $I_\mathfrak{p} = R_\mathfrak{p}$. On the other hand, when $\mathfrak{p} \in V(I)$ we have $I_\mathfrak{p} \subset \mathrm{rad}(R_\mathfrak{p})$, thus the non-vanishing is equivalent to $M_\mathfrak{p} \neq \{0\}$ by Nakayama's Lemma 1.3.5.

The "if" direction of (iii) is based on the following fact

$$IM \neq M \implies \mathrm{depth}_I(M) < +\infty$$

which will be proved in the next lecture (Theorem 8.3.2) using *Koszul complexes*. As for the "only if" direction, $V(I) \cap \mathrm{Supp}(M) = \emptyset$ implies $I + \mathrm{ann}(M) = R$, but the elements in $I + \mathrm{ann}(M)$ annihilate each $\mathrm{Ext}^n(R/I, M)$, hence $\mathrm{depth}_I(M) = +\infty$. □

Corollary 7.5.6. *With the same assumptions, let $(x_1, \dots, x_r)$ be an M-regular sequence with $x_i \in I$. It is of length* $\mathrm{depth}_I(M)$ *if and only if* $\mathrm{Ass}(M/(x_1, \dots, x_r)M) \cap V(I) \neq \emptyset$.

Proof. The sequence has length $\mathrm{depth}_I(M)$ if and only if R-module $M/(x_1, \dots, x_r)M$ has depth zero, so it remains to apply Proposition 7.5.2. □

Jean-Louis Koszul (1921—2018) created the Koszul complexes in order to define a cohomology theory for Lie algebras; this device turns out to be a general, convenient construction in homological algebra, which will be discussed in the next lecture. The study of "Koszulness" in a broader (eg. operadic) context is now an active area of research. J.-L. Koszul is also a second-generation member of the Bourbaki group. Source: by Konrad Jacobs - Oberwolfach Photo Collection, ID 2273.

Corollary 7.5.7. *Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$, and $M \neq \{0\}$ a finitely generated R-module, then* $\operatorname{depth}_{\mathfrak{m}}(M) \leq \dim M$.

Proof. Consider the following situation: $x \in \mathfrak{m}$ is not a zero-divisor for $M \neq \{0\}$. In the discussion of dimensions, we have seen that $d(M) \geq d(M/xM) \geq d(M/xM) - 1$, where $d(\cdot)$ is the degree of Hilbert–Samuel polynomial; on the other hand, since the alternating sum of Hilbert–Samuel polynomials in $0 \to M \xrightarrow{x} M \to M/xM \to 0$ has degree $< d(M)$, we infer that $d(M/xM) = d(M) - 1$. Hence $\dim(M/xM) = \dim(M) - 1$. By relating depth to M-regular sequences, we deduce $\operatorname{depth}_{\mathfrak{m}}(M) \leq \dim M$. □

Definition 7.5.8 (Cohen–Macaulay modules)**.** Let R be a Noetherian ring. A finitely generated R-module M is called *Cohen–Macaulay* if

$$\operatorname{depth}_{\mathfrak{m}A_{\mathfrak{m}}}(M_{\mathfrak{m}}) = \dim M_{\mathfrak{m}}$$

for every $\mathfrak{m} \in \operatorname{MaxSpec}(R) \cap \operatorname{Supp}(M)$. We say R is a Cohen–Macaulay ring if it is Cohen–Macaulay as a module.

Example 7.5.9. Regular local rings are Cohen–Macaulay, although we do not prove this here. Another important class of Cohen–Macaulay rings is the algebra of invariants A^G where A is the algebra of regular functions on an affine $\Bbbk$-variety $\mathcal{X}$ with *rational singularities* (eg. $A = \Bbbk[X_1, \dots, X_n]$) with an action by a reductive $\Bbbk$-group G (finite

groups allowed), and we assume $\mathrm{char}(\Bbbk) = 0$. Here is the reason: Boutot [6] proved the GIT quotient $\mathcal{X}/\!/G$ has rational singularities as well, hence is Cohen–Macaulay; in characteristic zero this strengthens an earlier theorem of Hochster–Roberts. These algebras are interesting objects from the geometric, algebraic or even combinatorial perspectives.

Exercise 7.5.10. Show by using Proposition 7.5.2 that $\mathrm{depth}_{\mathfrak{m}}(R) = 0$ if R is local with maximal ideal $\mathfrak{m}$ and has dimension zero.

Proposition 7.5.11. *The condition* **S2** *in Theorem 7.4.2 is equivalent to*

$$\mathrm{ht}(\mathfrak{p}) \geq i \implies \mathrm{depth}_{\mathfrak{p}R_{\mathfrak{p}}}(R_{\mathfrak{p}}) \geq i$$

for all $\mathfrak{p} \in \mathrm{Spec}(R)$ *and* $i \in \{1, 2\}$.

Proof. Assume the displayed conditions. We first show that every $\mathfrak{p} \in \mathrm{Ass}(R)$ has height zero. Upon localization we may assume R local with maximal ideal $\mathfrak{p}$, thus $\mathfrak{p}$ has depth zero by Proposition 7.5.2; our conditions force $\mathrm{ht}(\mathfrak{p}) = 0$. Next, consider $\mathfrak{p} \in \mathrm{Ass}(R/(t))$ with t non zero-divisor. Note that t remains a non zero-divisor in $R_{\mathfrak{p}}$, and $\mathfrak{p}R_{\mathfrak{p}} \in \mathrm{Ass}(R_{\mathfrak{p}}/(t))$. Hence $\mathrm{depth}(R_{\mathfrak{p}}) = \mathrm{depth}(R_{\mathfrak{p}}/(t)) + 1 = 1$ since $\mathrm{depth}_{\mathfrak{p}}(R_{\mathfrak{p}}/(t)) = 0$ by Proposition 7.5.2. Our conditions force $\mathrm{ht}(\mathfrak{p}) \leq 1$ and $t \in \mathfrak{p}$ implies $\mathrm{ht}(\mathfrak{p}) > 0$.

Conversely, assume **S2**. Suppose $\mathrm{ht}(\mathfrak{p}) \geq 1$. If $R_{\mathfrak{p}}$ has depth zero then $\mathrm{Ass}(R_{\mathfrak{p}}) \cap V(\mathfrak{p}R_{\mathfrak{p}}) \neq \emptyset$, which implies $\mathfrak{p}R_{\mathfrak{p}} \in \mathrm{Ass}(R_{\mathfrak{p}})$ thus $\mathfrak{p} \in \mathrm{Ass}(R)$, contradicting **S2**. Next, suppose $\mathrm{ht}(\mathfrak{p}) \geq 2$. If $R_{\mathfrak{p}}$ has depth ≤ 1, the standard property

$$\forall i \geq 0, \quad \mathrm{Ext}^i_{R_{\mathfrak{p}}}(X_{\mathfrak{p}}, Y_{\mathfrak{p}}) \simeq \mathrm{Ext}^i_R(X, Y)_{\mathfrak{p}}$$

valid for Noetherian R and finitely generated R-modules X, Y, yields

$$0 \leq \mathrm{depth}_{\mathfrak{p}}(R) \leq \mathrm{depth}_{\mathfrak{p}R_{\mathfrak{p}}}(R_{\mathfrak{p}}) \leq 1.$$

If $\mathrm{depth}_{\mathfrak{p}}(R) = 0$, there exists of $\mathfrak{p}' \supset \mathfrak{p}$ and $\mathfrak{p}' \in \mathrm{Ass}(R)$ by Proposition 7.5.2, but **S2** implies $\mathrm{ht}(\mathfrak{p}) \leq \mathrm{ht}(\mathfrak{p}') = 0$ which is absurd. If $\mathrm{depth}_{\mathfrak{p}}(R) = 1$, there exists a non zero-divisor x in R such that $\mathrm{depth}_{\mathfrak{p}}(R/(x)) = 0$. The same argument furnishes $\mathfrak{p}' \supset \mathfrak{p}$ such that $\mathfrak{p}' \in \mathrm{Ass}(R/(x))$. Now **S2** implies $\mathrm{ht}(\mathfrak{p}) \leq \mathrm{ht}(\mathfrak{p}') = 1$, again a contradiction. □

Now the conditions **R1** and **S2** can be generalized to arbitrary $k \in \mathbb{Z}_{\geq 0}$:

▷ **Rk** $\mathrm{ht}(\mathfrak{p}) \leq k$ implies $R_{\mathfrak{p}}$ is a regular local ring, for every $\mathfrak{p} \in \mathrm{Spec}(R)$;

▷ **Sk** $\mathrm{depth}(R_{\mathfrak{p}}) \geq \min\{k, \mathrm{ht}(\mathfrak{p})\}$ for every $\mathfrak{p} \in \mathrm{Spec}(R)$.

One readily checks their compatibility with Proposition 7.5.11. Note that **S0** is trivial, whilst R is Cohen–Macaulay if and only if it satisfies **Sk** for all k.

Example 7.5.12. From Theorem 7.4.2, we see that any finite direct product of normal domains of dimension ≤ 2 is Cohen–Macaulay.

Exercise 7.5.13. Show that **S1** holds if and only if there are no embedded primes in $\mathrm{Ass}(R)$.

Lecture 8

Some aspects of Koszul complexes

This lecture is a faithful replay of the relevant sections of [4] and [3]; the main aim here is to complete the proof of Theorem 7.5.5. In what follows, we work with a chosen ring R. We impose no Noetherian or finiteness conditions here.

8.1 Preparations in homological algebra

For any R-module L, denote its *exterior algebra* over R by

$$\bigwedge L := \bigoplus_{n\geq 0} \bigwedge^n L.$$

It is the quotient of the tensor algebra $T(L) = \bigoplus_{n\geq 0}(T^n(L) := L^{\otimes n})$ by the graded ideal generated by the pure tensors

$$\cdots \otimes x \otimes x \otimes \cdots, \quad x \in L.$$

The multiplication operation in $\bigwedge L$ is written as $\wedge$. Note that $\bigwedge^0 L = T^0(L) = R$ by convention. The traditional notion of exterior algebras encountered in differential geometry is recovered when $\mathbb{Q} \subset R$.

Given $u \in \mathrm{Hom}_R(L, R)$, one can define the corresponding *contractions* $i_u : \bigwedge^{n+1} L \to \bigwedge^n L$, given concretely as

$$i_u(x_0 \wedge \cdots \wedge x_n) = \sum_{i=0}^{n} (-1)^i u(x_i) \cdot x_0 \wedge \cdots \widehat{x_i} \cdots \wedge x_n$$

where $\widehat{x_i}$ means x_i is omitted. It is routine to check that i_u satisfies $i_u \circ i_u = 0$, thereby giving rise to a chain complex.

Definition 8.1.1. Let L and u be as above. Define the corresponding *Koszul complex* as $K_\bullet(u) := (\bigwedge^\bullet L, i_u)$. For any R-module M, put

$$K_\bullet(u; M) := M \underset{R}{\otimes} K_\bullet(u),$$
$$K^\bullet(u; M) := \mathrm{Hom}_A(K_\bullet(u), M)$$

which is naturally a chain (resp. cochain) complex in positive degrees; here one regards M as a complex in degree zero. These definitions generalize to the case of any complex M, and are functorial in M.

The reader might have encountered the following result in differential geometry.

Proposition 8.1.2 (Homotopy formula)**.** *For any $x \in L$ and $\omega \in \bigwedge^n L$, we have*

$$i_u(x \wedge \omega) + x \wedge (i_u(\omega)) = u(x)\omega.$$

Proof. Consider $\omega = x_1 \wedge \cdots \wedge x_n$. Put $x_0 := x$. The left-hand side equals

$$\sum_{i=0}^{n} (-1)^i \cdot u(x_i) \cdots \wedge \widehat{x_i} \wedge \cdots$$

whereas the right-hand side equals

$$\sum_{i=1}^{n} (-1)^{i+1} \cdot u(x_i)x_0 \wedge \cdots \wedge \widehat{x_i} \wedge \cdots .$$

The terms with a $\widehat{x_i}$ (non-existant — hopefully this won't generate metaphysical issues) where $i > 0$ cancel out. We are left with $u(x_0)x_1 \wedge \cdots \wedge x_n = u(x)\omega$. □

Obviously, the same formula extends to all $\omega \in \bigwedge L$ by linearity.

Proposition 8.1.3. *Set $\mathfrak{q} := u(L)$, which is an ideal of R. Then $\mathfrak{q}$ annihilates each homology (resp. cohomology) of $K_\bullet(u; M)$ (resp. $K^\bullet(u; M)$). Again, this generalizes to general complexes M.*

Proof. Given $t \in \mathfrak{q}$, the homotopy formula implies that the endomorphism $\omega \mapsto t\omega$ of $K_\bullet(u)$ is homotopic to zero, hence so are the induced endomorphisms of $K_\bullet(u; M)$ and $K^\bullet(u; M)$ by standard homological algebra. □

Proposition 8.1.4. *Suppose L is projective over R and $0 \to M' \to M \to M'' \to 0$ is exact. Then there is a natural short exact sequence of complexes*

$$0 \to K^\bullet(u; M') \to K^\bullet(u; M) \to K^\bullet(u; M'') \to 0$$

which gives rise to a long exact sequence of cohomologies of the Koszul complexes in question.

Proof. Standard. It suffices to note that L is projective implies each graded piece $\bigwedge^n L$ of $\bigwedge L$ is projective as well. □

Exercise 8.1.5. Justify the assertion above concerning the projectivity of $\bigwedge^n L$. Hint: suppose L is a direct summand of a free module F, show that $\bigwedge^n L$ is a direct summand of $\bigwedge^n F$ and $\bigwedge^n F$ is free.

Similar properties hold for the homological version when L is flat over R. One needs the property that $\bigwedge^n L$ is flat if L is.

Exercise 8.1.6. Prove the assertion above concerning flatness of $\bigwedge^n L$. Consult the proof in [4, p.15] if necessary.

8.2 Auxiliary results on depth

We fix an ideal $I \subset R$.

Proposition 8.2.1. *For every family $\{M_\beta\}_{\beta \in \mathcal{B}}$ of R-modules, we have*

$$\operatorname{depth}_I \left(\prod_\beta M_\beta \right) = \inf_\beta \operatorname{depth}_I (M_\beta).$$

Proof. This follows from $\operatorname{Ext}^n_R(R/I, \prod_i M_i) = \prod_{i \in I} \operatorname{Ext}^n_R(R/I, M_i)$, as is easily seen by taking a projective resolution of R/I and using the fact the Hom_R preserves direct products in the second variable. □

Remark 8.2.2. By stipulation, the empty product is 0, the zero object of the category R-Mod. In parallel we define $\inf \emptyset := \infty$, so that Proposition 8.2.1 remains true in this case, since the zero module has infinite depth.

Proposition 8.2.3. *Suppose N is an R-module annihilated by some I^m, where $m \geq 1$. Then $\operatorname{Ext}^i_R(N, M) = 0$ whenever $i < \operatorname{depth}_I(M)$.*

Proof. To show $\operatorname{Ext}^i_R(N, M) = 0$ for $i < \operatorname{depth}_I(M)$, we begin with the case $m = 1$. This case follows by a dimension-shifting argument based on the short exact sequence

$$0 \to K \to (R/I)^{\oplus I} \to M \to 0,$$

together with induction on i (note that $\operatorname{Ext}^{<0}_R(N, M) = 0$ for trivial reasons). The case of general m follows by a standard *dévissage* using

$$0 \to JN \to N \to N/JN \to 0$$

and the associated long exact sequence. □

Lemma 8.2.4. *Suppose J is an ideal satisfying $J \supset I^m$ for some $m \geq 1$. Then $\operatorname{depth}_I(M) \leq \operatorname{depth}_J(M)$.*

Proof. From the previous Proposition, we have $\operatorname{Ext}^i_R(R/J, M) = 0$ for $i < \operatorname{depth}_I(M)$ since I^m annihilates R/J. The assertion follows upon recalling the definition of depth. □

The following technical results will be invoked in the proof of Theorem 8.3.2.

Proposition 8.2.5. *Let $C^\bullet$ be a cochain complex of R-modules such that $n \ll 0 \implies C^n = 0$. Let $h \in \mathbb{Z}$ such that for all integers $n \leq k \leq h$, the depth of C^n with respect to $J_k := \operatorname{ann}(H^k(C^\bullet))$ is $> k - n$, then*

$$H^{\leq h}(C^\bullet) = 0.$$

In what follows, we write $H^n = H^n(C^\bullet) = Z^n/B^n$ in the usual notation for homological algebra.

Proof. Assume on the contrary that there exists $k \leq h$ with $H^{<k} = 0$ whereas $H^k \neq 0$. Write $J = J_k$. As J annihilates the nonzero R-module H^k, the criterion of depth-zero modules (Proposition 7.5.2) implies that $\operatorname{depth}_J(H^k) = 0$. By assumption $\operatorname{depth}_J(C_k) > k-k = 0$, it follows that $\operatorname{depth}_J(Z_k) > 0$ since $Z_k \subset C_k$, by applying the aforementioned criterion of depth-zero. From the short exact sequence

$$0 \to B^k \to Z^k \to H^k \to 0$$

we deduce distinguished triangles in $D(R\text{-}\mathsf{Mod})$

$$\mathcal{H}\mathrm{om}(R/J, B^k) \to \mathcal{H}\mathrm{om}(R/J, Z^k) \to \mathcal{H}\mathrm{om}(R/J, H^k) \xrightarrow{+1},$$
$$\mathcal{H}\mathrm{om}(R/J, H^k)[-1] \to \mathcal{H}\mathrm{om}(R/J, B^k) \to \mathcal{H}\mathrm{om}(R/J, Z^k) \xrightarrow{+1}.$$

As the leftmost and rightmost terms of the last line are in $D^{\geq 1}(R\text{-}\mathsf{Mod})$, we see

$$\operatorname{depth}_J(B^k) \geq 1;$$

moreover, the piece $\operatorname{Ext}^0_R(R/J, Z^k) \to \operatorname{Ext}^0_R(R/J, H^k) \to \operatorname{Ext}^1_R(R/J, B^k)$ from the long exact sequence shows that $\operatorname{depth}_J(B^k) = 1$. Now for $n < k$ we have short exact sequences

$$0 \to \underbrace{B^n}_{=Z^n} \to C^n \to B^{n+1} \to 0.$$

Again, one infers from the distinguished triangle

$$\mathcal{H}\mathrm{om}(R/J, B^{n+1})[-1] \to \mathcal{H}\mathrm{om}(R/J, B^n) \to \mathcal{H}\mathrm{om}(R/J, C^n) \xrightarrow{+1},$$

the assumption $\operatorname{depth}_J(C^n) > k - n$ and descending induction on n that $n < k \implies \operatorname{depth}_J(B_n) = k - n + 1$. This is impossible since $B_{\ll 0} = 0$ has infinite depth. □

Corollary 8.2.6. *Let $I \subset R$ be an ideal, $C^\bullet$ be a cochain complex with $n \ll 0 \implies C_n = 0$, and $h \in \mathbb{Z}$. Suppose that $n \leq h$ implies $I \cdot H^n(C^\bullet) = 0$ and $\operatorname{depth}_I(C^n) > h - n$. Then $H^{\leq h}(C^\bullet) = 0$.*

Proof. For $k \leq h$ we have $J_k := \operatorname{ann}(H^k(C^\bullet)) \supset I$. Hence Lemma 8.2.4 entails that

$$n \leq k \leq h \implies \operatorname{depth}_{J_k}(C^n) \geq \operatorname{depth}_I(C^n) > h - n \geq k - n.$$

Now apply Proposition 8.2.5. □

8.3 Koszul complexes and depth

The simplest Koszul complexes are defined as follows. Given $x \in R$, we form the cochain complex in degrees $\{0, 1\}$

$$K(x) := \left[R \xrightarrow{x} R \right].$$

More generally, for any R-module M, viewed as a complex concentrated in degree zero, and a family $\mathbf{x} = (x_\alpha)_{\alpha\in\mathcal{A}}$ of element of R, we define the associated *Koszul complex* as

$$K^\bullet(\mathbf{x}; M) := K^\bullet(u; M),$$

where we take $u : R^{\oplus\mathcal{A}} \to R$ corresponding to $\mathbf{x}$ in Definition 8.1.1. Unfolding definitions, we have

$$K^h(\mathbf{x}; M) = \begin{cases} \mathrm{Hom}_R\left(\bigwedge^h(R^{\oplus\mathcal{A}}), M\right), & h \geq 0 \\ 0, & h < 0. \end{cases}$$

Therefore $K^h(\mathbf{x}; M)$ consists of families $m(\alpha_1, \dots, \alpha_h) \in M$ that are alternating in the variables $\alpha_1, \dots, \alpha_h \in \mathcal{A}$. The differential is

$$\begin{aligned} \partial^h : K^h(\mathbf{x}; M) &\longrightarrow K^{h+1}(\mathbf{x}; M) \\ m &\longmapsto \left[(\alpha_0, \dots, \alpha_h) \mapsto \sum_{j=0}^{h} (-1)^j x_{\alpha_j} \cdot m(\dots, \widehat{\alpha_j}, \dots)\right]. \end{aligned}$$

We shall abbreviate the cohomologies of $K^\bullet(\mathbf{x}; M)$ as the *Koszul cohomologies*.

When $\mathcal{A} = \{1, \dots, n\}$ we revert to

$$K^\bullet(x_1, \dots, x_n; M) := M \otimes K(x_1) \otimes \cdots \otimes K(x_n)$$

with the well-known sign convention. Also note that $R^{\oplus\mathcal{A}}$ is projective, hence the Proposition 8.1.4 can always be applied to Koszul cohomologies.

Let I denote the ideal generated by $\{x_\alpha : \alpha \in \mathcal{A}\}$. The reader is invited to verify that

- $K^\bullet\left(\mathbf{x}, \prod_{\beta\in\mathcal{B}} M_\beta\right) = \prod_{\beta\in\mathcal{B}} K^\bullet(\mathbf{x}; M_\beta)$ for any family $\{M_\beta\}_{\beta\in\mathcal{B}}$ of R-modules, and same for their cohomologies;
- the 0-th cohomology of $K^\bullet(\mathbf{x}; M)$ is $\mathrm{Hom}_R(R/I, M) = \{x \in M : Ix = 0\}$, the I-torsion part of M;
- if $|A| = n$, the n-th cohomology of $K^\bullet(\mathbf{x}; M)$ is M/IM.

These facts will cast in our later arguments.

Lemma 8.3.1. *Each cohomology of $K^\bullet(\mathbf{x}; M)$ is annihilated by I.*

Proof. Apply Proposition 8.1.3 by observing that $\mathfrak{q} = I$ in our setting. □

Theorem 8.3.2. *Let M be an R-module and $\mathbf{x} = \{x_\alpha\}_{\alpha\in\mathcal{A}}$ be a family of elements of R, which generate an ideal I of A. Then* $\mathrm{depth}_I(M)$ *equals*

$$\inf\{n \geq 0 : H^n(K^\bullet(\mathbf{x}; M)) \neq 0\} \in \mathbb{Z}_{\geq 0} \sqcup \{\infty\}.$$

Consequently, if $I \subset R$ is an ideal generated by elements $x_1, \dots, x_n$ and $IM \neq M$, then we have

$$\mathrm{depth}_I(M) \leq n.$$

Proof. Let $d := \operatorname{depth}_I(M)$. Since $K^h(\mathbf{x}; M)$ is a direct product of copies of M (possibly the empty product $= 0$), by Proposition 8.2.1 its depth equals either d or ∞. Combining Lemma 8.3.1 and Corollary 8.2.6 (with $h = d - 1$), we see that $H^{<d}(K^\bullet(\mathbf{x}; M)) = 0$. It remains to show $H^d(K^\bullet(\mathbf{x}; M)) \neq 0$ provided that $d < \infty$, which we assume from now onwards.

The case $d = 0$ is clear since there exists $\mathfrak{p} \in \operatorname{Ass}(M) \cap V(I)$, therefore $R/\mathfrak{p} \hookrightarrow M$ and $\exists x \in M$ with $\mathfrak{p}x \supset Ix = \{0\}$, whence $H^0(K^\bullet(\mathbf{x}; M)) \neq 0$. Now suppose $d \in \mathbb{Z}_{\geq 1}$ and assume $H^d(K^\bullet(\mathbf{x}; M)) = 0$. Take a free resolution $F_\bullet \to R/I \to 0$ and put $C^\bullet := \operatorname{Hom}_R(F_\bullet, M)$, so that

$$H^i(C^\bullet) \simeq \operatorname{Ext}^i_R(R/I, M), \quad i \geq 0.$$

Hence for $i < d$ we have short exact sequences

$$0 \to B^i \to C^i \to B^{i+1} \to 0$$

as usual; recall $B^i, Z^i \subset C^i$. Note that each C^i is a direct product of copies of M, hence $H^{\leq d}(K^\bullet(\mathbf{x}; C^i)) = 0$. Indeed, $H^{<d}(K^\bullet(\mathbf{x}; M)) = 0$ has been settled in the first step, whilst $H^d(K^\bullet(\mathbf{x}; M))$ is the hypothesis to be refuted. It then follows from the long exact sequence for Koszul cohomologies (Proposition 8.1.4) that

$$(s \leq d) \wedge (i < d) \implies H^s(K^\bullet(\mathbf{x}; B^{i+1})) \hookrightarrow H^{s+1}(K^\bullet(\mathbf{x}; B^i)).$$

Suppose $i < d$. As $B^0 = 0$, an iteration yields

$$H^{d-i}(K^\bullet(\mathbf{x}; B^{i+1})) \hookrightarrow \cdots \hookrightarrow H^{d+1}(K^\bullet(\mathbf{x}; B^0)) = 0.$$

In particular, $i = d - 1$ gives rise to $H^1(K^\bullet(\mathbf{x}; B^d)) = 0$. Hence the short exact sequence $0 \to B^d \to Z^d \to H^d \to 0$ (for $C^\bullet$) together with Proposition 8.1.4 give rise to

$$H^0(K^\bullet(\mathbf{x}; Z^d)) \twoheadrightarrow H^0(K^\bullet(\mathbf{x}; H^d)).$$

As $H^d := H^d(C^\bullet) \simeq \operatorname{Ext}^d_R(R/I, M)$ is nonzero and annihilated by I, the right-hand side is nonzero. Hence $H^0(K^\bullet(\mathbf{x}; Z^d)) \neq 0$ and then $H^0(K^\bullet(\mathbf{x}; C^d)) \neq 0$, as the zeroth Koszul cohomology is nothing but the I-torsion part.

Finally, recall that $C^d \neq \{0\}$ is a direct product of copies of M, consequently

$$H^0(K^\bullet(\mathbf{x}; M)) \neq 0.$$

However, this contradicts the earlier result that $H^{<d}(K^\bullet(\mathbf{x}; M)) = 0$ since $d \geq 1$. □

This yields an alternative characterization of depth. It also completes the proof of Theorem 7.5.5 as promised in the previous lecture.

《晚风》, 李桦, 木刻版画, 1963 年.

Bibliography

[1] Allen Altman and Steven Kleiman. *Introduction to Grothendieck duality theory*. Lecture Notes in Mathematics, Vol. 146. Springer-Verlag, Berlin-New York, 1970, pp. ii+185 (cit. on p. 25).

[2] M. Artin. "Algebraization of formal moduli. II. Existence of modifications". In: *Ann. of Math. (2)* 91 (1970), pp. 88–135. ISSN: 0003-486X (cit. on p. 71).

[3] N. Bourbaki. *Éléments de mathématique. Algèbre commutative. Chapitre 10*. Reprint of the 1998 original. Springer-Verlag, Berlin, 2007, pp. ii+187. ISBN: 978-3-540-34394-3; 3-540-34394-6 (cit. on pp. 2, 73, 78, 83).

[4] N. Bourbaki. *Éléments de mathématique. Algèbre. Chapitre 10. Algèbre homologique*. Reprint of the 1980 original [Masson, Paris; MR0610795]. Springer-Verlag, Berlin, 2007, pp. viii+216. ISBN: 978-3-540-34492-6; 3-540-34492-6 (cit. on pp. 83, 84).

[5] Nicolas Bourbaki. *Éléments de mathématique*. Algèbre commutative. Chapitre 8. Dimension. Chapitre 9. Anneaux locaux noethériens complets. [Commutative algebra. Chapter 8. Dimension. Chapter 9. Complete Noetherian local rings]. Masson, Paris, 1983, p. 200. ISBN: 2-225-78716-6 (cit. on p. 2).

[6] Jean-François Boutot. "Singularités rationnelles et quotients par les groupes réductifs". In: *Invent. Math.* 88.1 (1987), pp. 65–68. ISSN: 0020-9910. DOI: 10.1007/BF01405091. URL: http://dx.doi.org/10.1007/BF01405091 (cit. on p. 81).

[7] Winfried Bruns and Joseph Gubeladze. *Polytopes, rings, and K-theory*. Springer Monographs in Mathematics. Dordrecht: Springer, 2009, pp. xiv+461. ISBN: 978-0-387-76355-2. DOI: 10.1007/b105283. URL: http://dx.doi.org/10.1007/b105283 (cit. on p. 57).

[8] David Eisenbud. *Commutative algebra*. Vol. 150. Graduate Texts in Mathematics. With a view toward algebraic geometry. Springer-Verlag, New York, 1995, pp. xvi+785. ISBN: 0-387-94268-8; 0-387-94269-6. DOI: 10.1007/978-1-4612-5350-1. URL: http://dx.doi.org/10.1007/978-1-4612-5350-1 (cit. on pp. 2, 5, 12, 15, 21, 23, 25, 34, 36, 45, 51, 59, 67, 73).

[9] William Fulton. *Intersection theory*. Second. Vol. 2. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]. Springer-Verlag, Berlin, 1998, pp. xiv+470. ISBN: 3-540-62046-X; 0-387-98549-2. DOI: 10.1007/978-1-4612-1700-8. URL: https://doi.org/10.1007/978-1-4612-1700-8 (cit. on p. 49).

[10] Robin Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977, pp. xvi+496. ISBN: 0-387-90244-9 (cit. on p. 44).

[11] Hideyuki Matsumura. *Commutative algebra*. Second Edition. Vol. 56. Mathematics Lecture Note Series. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980, pp. xv+313. ISBN: 0-8053-7026-9 (cit. on pp. 2, 15, 19, 25, 44, 51, 65–67, 71).

[12] John Milnor. *Singular points of complex hypersurfaces*. Annals of Mathematics Studies, No. 61. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1968, pp. iii+122 (cit. on p. 27).

[13] David Mumford. *The red book of varieties and schemes*. expanded. Vol. 1358. Lecture Notes in Mathematics. Includes the Michigan lectures (1974) on curves and their Jacobians, With contributions by Enrico Arbarello. Springer-Verlag, Berlin, 1999, pp. x+306. ISBN: 3-540-63293-X. DOI: 10.1007/b62130. URL: http://dx.doi.org/10.1007/b62130 (cit. on p. 28).

[14] "Obituary: Tadasi Nakayama". In: *Nagoya Math. J.* 27.1 (1966), pp. i–vii. URL: http://projecteuclid.org/euclid.nmj/1118801606 (cit. on p. 10).

[15] Jean-Pierre Serre. "Géométrie algébrique et géométrie analytique". In: *Ann. Inst. Fourier, Grenoble* 6 (1955–1956), pp. 1–42. ISSN: 0373-0956 (cit. on p. 38).

[16] I. R. Shafarevich, ed. *Algebraic geometry. IV*. Vol. 55. Encyclopaedia of Mathematical Sciences. Linear algebraic groups. Invariant theory, A translation of ıt Algebraic geometry. 4 (Russian), Akad. Nauk SSSR Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1989 [MR1100483 (91k:14001)], Translation edited by A. N. Parshin and I. R. Shafarevich. Springer-Verlag, Berlin, 1994, pp. vi+284. ISBN: 3-540-54682-0. DOI: 10.1007/978-3-662-03073-8. URL: http://dx.doi.org/10.1007/978-3-662-03073-8 (cit. on p. 13).

[17] Angelo Vistoli. "Grothendieck topologies, fibered categories and descent theory". In: *Fundamental algebraic geometry*. Vol. 123. Math. Surveys Monogr. Amer. Math. Soc., Providence, RI, 2005, pp. 1–104 (cit. on p. 38).

Index

A
$\operatorname{ann}_R(M), \operatorname{ann}_R(x)$, 15
Artinian, 11
$\operatorname{Ass}(M)$, 16
associated prime, 16

B
blow-up algebra, 48

C
catenary, 71
Cayley–Hamilton theorem, 10
Chevalley's theorem, 44
Cohen–Macaulay module, 80
completion, 52
constructible subset, 43
coprimary module, 18

D
depth, 78, 87
dimension, 58
dimension formula, 70
discrete valuation ring, 73

E
embedded prime, 17
exterios algebra, 83

F
faithful functor, 36
faithfully flat, 31, 36
field of fractions, 6
filtration, 46
    $\mathfrak{a}$-adic, 47
finitely presented, 7
flat, 31

G
going-down, 39
going-up, 39
$\operatorname{gr}_F(M)$, 46
graded, 45

H
Hauptidealsatz, 63
height, 58
Hilbert's basis theorem, 11
Hilbert–Samuel polynomial, 58
homogeneous, 45

I
integral closure, 26
integrality, 25
invariant theory, 13

J
Jacobson radical, 10
Jacobson ring, 28

K
$K^\bullet(u; M)$, 84
$K^\bullet(\mathbf{x}; M)$, 87
Koszul complex, 83, 87
Krull's intersection theorem, 50

L
length, 11, 57
local ring, 3
localization, 5

M
$M[S^{-1}]$, 5
$\operatorname{MaxSpec}(R)$, 4
minimal prime ideal, 39
Moishezon manifolds, 71
multiplicative subset, 5

N
Nakayama's lemma, 10
nilpotent radical, 9
Noether normalization, 69
Noetherian, 11
normal, 26
Nullstellensatz, 13, 29

P
parameter ideal, 59
primary decomposition, 19
primary module, 18
prime avoidance, 4

R
reduced ring, 9, 74
Rees algebra, 49
regular local ring, 63
regular sequence, 79

S
SageMath, 23
Serre's criterion, 77
Spec(R), 4
Supp(M), 15
support, 15

T
topological ring, 51
    I-adic, 51
total fraction ring, 6

U
uniformizer, 73

V
$V(\mathfrak{a})$, 4
variety, 12

Z
Zariski topology, 4
zero divisor, 16
Zorn's Lemma, 3, 20, 40