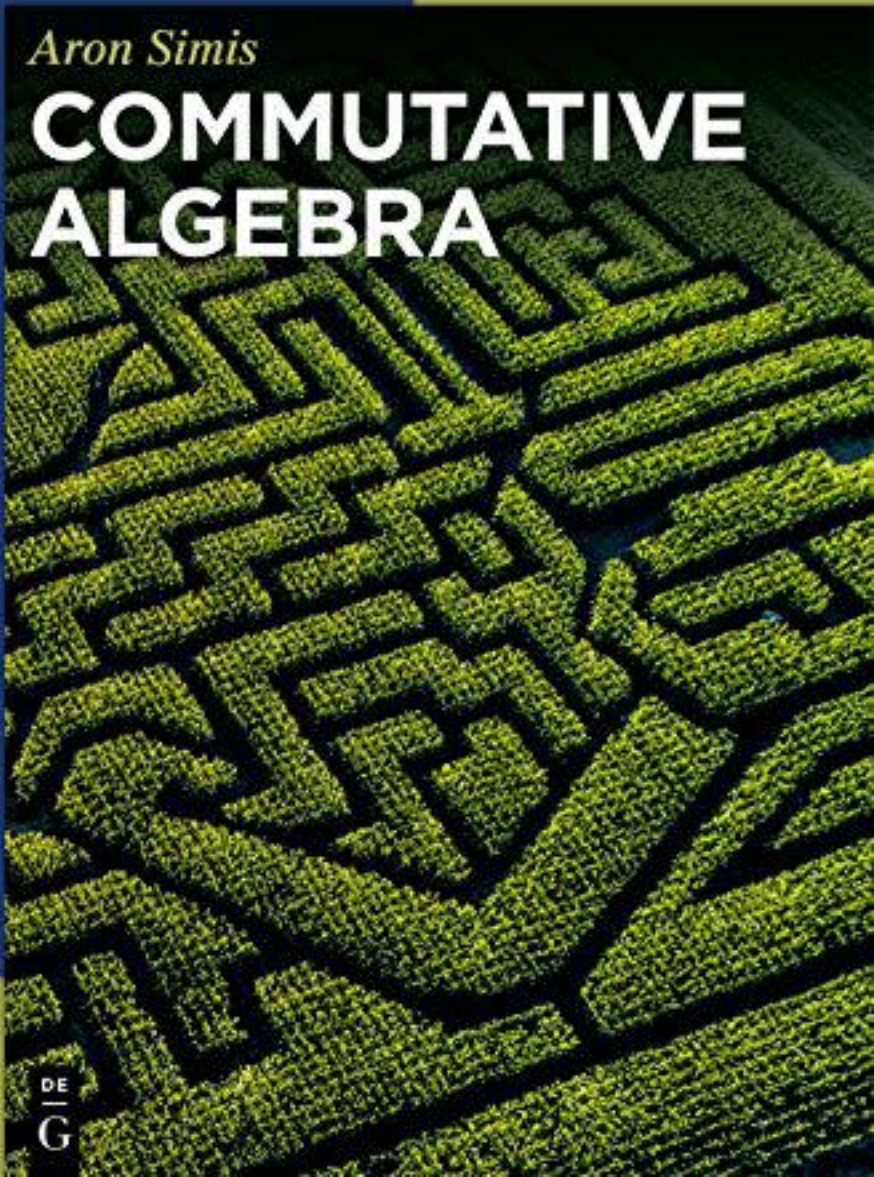
DE GRUYTER

GRADUATE

Aron Simis

COMMUTATIVE ALGEBRA



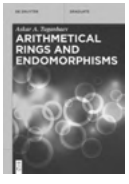
DE G

Aron Simis
Commutative Algebra

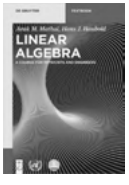
Also of Interest

Abstract Algebra. Applications to Galois Theory, Algebraic Geometry, Representation Theory and Cryptography
Celine Carstensen-Opitz, Benjamin Fine, Anja Moldenhauer, Gerhard Rosenberger, 2019
ISBN 978-3-11-060393-4, e-ISBN (PDF) 978-3-11-060399-6, e-ISBN (EPUB) 978-3-11-060525-9

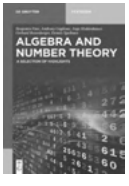
Sraffa and Leontief Revisited. Mathematical Methods and Models of a Circular Economy
Jean-François Emmenegger, Daniel L. Chable, Hassan A. Nour Eldin, Helmut Knolle, 2020
ISBN 978-3-11-063042-8, e-ISBN (PDF) 978-3-11-063509-6, e-ISBN (EPUB) 978-3-11-063509-6



Arithmetical Rings and Endomorphisms
Askar A. Tuganbaev, 2019
ISBN 978-3-11-065889-7, e-ISBN (PDF) 978-3-11-065982-5, e-ISBN (EPUB) 978-3-11-065915-3



Linear Algebra. A Course for Physicists and Engineers
Arak M. Mathai, Hans J. Haubold
ISBN 978-3-11-056235-4, e-ISBN (PDF) 978-3-11-056250-7, e-ISBN (EPUB) 978-3-11-056259-0



Algebra and Number Theory. A Selection of Highlights
Benjamin Fine, Anthony Gaglione, Anja Moldenhauer, Gerhard Rosenberger, Dennis Spellman
ISBN 978-3-11-051584-8, e-ISBN (PDF) 978-3-11-051614-2, e-ISBN (EPUB) 978-3-11-051626-5

Aron Simis

Commutative Algebra

DE GRUYTER

Mathematics Subject Classification 2010
Primary: 13-01, 13A02, 13A30, 13B02, 13B21, 13C05, 13C14, 13C15, 13C40, 13D02, 13D05, 13D07, 13D40, 13E05, 13E10, 13E15, 13H05, 13H10, 13H15, 13N05, 13N15; Secondary: 14A05, 14A10, 14B05, 14M05, 14M10, 14M12

Author
Prof. Dr. Aron Simis
Departamento de Matemática
Universidade Federal de Pernambuco
Av. Jornalista Aníbal Fernandes
50740-640 Pernambuco
Brazil
aron@dmat.ufpe.br

ISBN 978-3-11-061697-2
e-ISBN (PDF) 978-3-11-061698-9
e-ISBN (EPUB) 978-3-11-061707-8

Library of Congress Control Number: 2019955972

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.dnb.de.

Cover image: Alex Potemkin/E+/gettyimages.com
Typesetting: VTeX UAB, Lithuania
Printing and binding: CPI books GmbH, Leck

www.degruyter.com

Thanks

I wish to thank my earlier editorial contact in De Gruyter, Apostolos Damialis, without whom the idea of this book would never take off. It was a pleasure having Wolmer Vasconcelos and Yairon Cid-Ruiz look at a first draft. Special thanks go to Zaqueu Ramos, for his careful reading of a final version, pointing many doubtful passages and helping with the overall coherence of the book. Most of all, I thank my wife, Paula, for much endurance during the long days and nights of writing the book. Without her permanent patience and support, I would not be able to accomplish my task.

To Paula,
for endurance

https://doi.org/10.1515/9783110616989-201

Foreword

The objective of this book is to introduce the reader to the principles and practice of commutative algebra, pretty much in the spirit of W. Krull's celebrated *Idealtheorie* ([98]). That is to say, to compensate for the dry introductory material one puts an effort in giving some panorama as to how and why such concepts were created in the first place. Clearly, there is no intention to measure up to Krull's concise mastership, nor is this the immediate objective here. And yet, there seems to be plenty of opportunities to render parts of the text a mix of technicality and motivation.

There is obviously a large difference in style between Krull's book and many of the later books on commutative algebra, beyond the mere change in terminology from *theory of ideals* to *commutative algebra*, with *commutative rings* sort of hanging out halfway. Foremost is the fact that Krull was thoroughly acquainted with nearly all the existing literature on the subject in his time, most probably including the non-commutative theory. Being such a powerful connoisseur, he felt at ease to employ a mix of survey style with precise arguments throughout. Such a combination in writing a useful textbook is by no means a trivial endeavor.

Nowadays there is a different status-quo altogether because commutative algebra became a solid knowledge with very large contours that exceed even the marvelous account by Bourbaki. Writing a book on a sufficiently stable mathematical discipline is by no means an easy task. It is infinitely more terrifying than writing a manuscript on a specific mathematical problem, no matter how hot a topic. In fact, in writing the latter one is comfortably in the position of bringing into the subject whatever language data and methods seem fit to discuss the problem. No particular worry as to whether the potential readers are trained in this matter.

A discipline such as commutative algebra often has the air of a self-closed self-independent discipline, no matter how majestically it involves substantial parts of homology theory and lifts our hearts by bringing in the power of algebraic geometry or the taste of a computer calculation on the nose—a beautiful hard knuckle, no doubt about it and too self-sustained to be brought in the public at large. Aiming at writing a book which exhausts all contents of the discipline is temerarious, to say the least. So, how to decide about the essentials? This is a tough riddle, highly dependent on some personal view of the material and of its impact throughout.

This is about its content proper. A second psychological obstruction is the existence of so many wonderful books on the subject. And, in fact, why still another one? A perfectly reasonable question, at least vis-à-vis the authors of these books, most of whom so dear to me. As by the dictum of Carl Faith (according to T. Y. Lam), textbook writing must be one of the cruelest of self-inflicted tortures. So why do it? On top of it, why justify it? Well, for one reason one has to comply with the Editors' views. But apart from this, what else really?

Here is one piece of explanation, at least as concerns a certain style employed. Through all those years of teaching commutative algebra, I could spot pleasure in the

https://doi.org/10.1515/9783110616989-202

audience (mainly sophomores or later) when I motivated a theorem tying it to its early discoveries and the existing knowledge at the time. While trying to move this experience over to book, in writing it soon became clear that just a short discussion at the end of the chapter would not do it. Having this in mind, I decided to keep the classroom style throughout the book, by making one or two historic comments right on spot where a theorem is stated, without derailing from the ongoing core, while deferring historical circumstances to a lengthier assessment at the end of a chapter.

A second piece of explanation (expiation?) has to do with the shape of the book, as arranged into a more elementary part and a more advanced one. For one thing, it helps the newcomer to grasp first some down to earth material, with the foresight of learning more advanced matter later in the reading. A bit more of short history here and there, plus some exercises of concrete resolve, may also contribute overall.

I have decided to include two intermediary chapters, versing nonexhaustingly on topics usually detracted to appendices. My idea of an appendix, no matter how memorable it may be (such as some in Zariski–Samuel book), is that it often feels like a leftover instead of a body-part as it is.

As to the advanced part, I hope that there is enough material overseeing the basic advanced knowledge. The choice of topics is always a matter of personal outlook and, in this case, closer to my mathematical experience throughout the years. Overall, there is not much to depict about the chosen topics. I believe the contents speak for themselves and also make clear the choice of topics, as well as the order in which they are introduced. It is perhaps more useful for the reader if I list some topics that have been left out: completion, Gröbner bases and elimination theory, cohomology, spectral sequences, algebras with straightening law, semigroups. Some, though close to my heart, would not comply with the intended size of the book, others have been excelled by other people with much more competence. Again, there are subjects that one can deliver in a particular manner as a consequence of one's experience, others yield to a total disaster even before put in writing.

As a general healthy habit, there is an effort to keep the material in a logical ordering, but it often happens that a later result is called upon in order to close a proof or a remark is enhanced on spot about such a later result.

A final word concerns two aspects: the historic notes at the end of each chapter and the exercises. As to the first, I have tried as much as possible to visit the original sources and part of the literature au tour a particular subject or theorem. Often I have relied on other peoples' account of a specific topic. This is not a book on the history of commutative algebra, nor I am a connoisseur thereof. Yet, I hope the notes may be of some help, specially for a newcomer.

As for the exercises, I have put some effort in proposing problems that apply the theory to solve concrete questions (yes, with concrete polynomials, and so forth). I have tried to avoid filling up a list of exercises that complements too many theoretical results (an exception is Chapter 3 whose main objective is a review of concepts). From my teaching experience, students tend to stay away from this sort of exercises

because of the psychological feeling of an expected (boring?) sequel to the material already studied. Also, there is the question of giving hints to exercises. I believe this is a healthy practice, but should not be exaggerated lest the reader gets discouraged to find a personal path.

Recife,
Summer/Fall 2019

Contents

Part II

1 Basic introductory theory

1.1 Commutative rings and ideals

The most fundamental object of this book is a commutative ring having a multiplicative identity element. Throughout the text, one refers to it simply as a ring.

A *ring homomorphism* (or simply, a *homomorphism*) is a map $\varphi : R \to S$ between rings, which besides being compatible with the two operations, is also required to map the multiplicative identity element of R to the one of S. If no confusion arises, one usually denotes the multiplicative identity of any ring by 1, even if there is more than one ring involved in the discussion. A ring homomorphism $R \to S$ that admits an inverse ring homomorphism $S \to R$ is called an isomorphism. As is easily seen, any bijective homomorphism is an isomorphism.

The *kernel* of φ is the set $\ker \varphi := \{a \in R \mid \varphi(a) = 0\}$. It is easy to see that $\ker \varphi$ is an ideal of R and induces an injective homomorphism $R/\ker \varphi \hookrightarrow S$. Because of Proposition 1.1.2 below, one often moves over to the subring $R/\ker \varphi$ for the sake of an argument.

Given an arbitrary homomorphism $\varphi : R \to S$, one can move back and forth between ideals of S and of R: given an ideal $J \subset S$, the inverse image $\varphi^{-1}(J) \subset R$ is an ideal of R, while given an ideal $I \subset R$ one obtain the ideal of S generated by the set $\varphi(I)$. The first such move is called a *contraction*—a terminology that rigorously makes better sense when $R \subset S$; in the second move, the ideal generated by $\varphi(I)$ is called the *extended ideal* of I.

A subgroup of the additive group of a ring R is called a *subring* provided it is closed under the product operation of R and contains the multiplicative identity of R.

An element $a \in R$ is said to be a *zero-divisor* if there exists $b \in R$, $b \neq 0$, such that $ab = 0$; otherwise, a is called a *nonzero divisor*. In this book, a nonzero divisor will often be referred to as a *regular element*. A sort of extreme case of a zero-divisor is a *nilpotent* element a, such that $a^n = 0$ for some $n \geq 1$.

One assumes a certain familiarity with these notions and their elementary manipulation.

A terminology that will appear very soon is that of an *R-algebra* to designate a ring S with a homomorphism $R \to S$.

1.1.1 Ideals, generators

The abstract notion of ideal is due to R. Dedekind, as a culmination, one could say, of his long work in shaping up number theory.

A subset $I \subset R$ is an *ideal* when it satisfies the following conditions:

(i) I is a subgroup of the additive group of R.

(ii) If $b \in I$ and $a \in R$, then $ba \in I$.

https://doi.org/10.1515/9783110616989-001

The second condition is what makes a distinction from the notion of a subring, to come up shortly. It is easy to produce ideals at will at least in a theoretical way. The procedure depends on the following elementary concept.

Definition 1.1.1. Let $I \subset R$ be an ideal. A subset $S \subset I$ is named a *set of generators* of I if, equivalently:
- I is inclusion wise the smallest ideal of R containing S;
- I is the intersection of the family of all ideals of R containing S;
- Every element of I can be written in the form $c_1a_1+\cdots+c_ma_m$, for suitable elements $a_1, \ldots, a_m \in R$ and $c_1, \ldots, c_m \in S$.

Going the opposite direction, it is clear that an arbitrary subset $S \subset R$ of a ring generates an ideal $I \subset R$. One uses the notation $I = (S)$ to indicate this construction. In the case where $S = \{c_1, \ldots, c_m\}$ is a finite set, the notational symbols $I = (c_1, \ldots, c_m)$ and $I = c_1R + \cdots + c_mR = \sum_{i=1}^{n} c_iR$ are used interchangeably.

Thus, the main question about ideals is not how one finds them, but how they function departing from these abstract properties.

One notes that the set $\{0\}$ is an ideal; it is convenient to think of the empty set as being a set of generators of $\{0\}$. The next simplest kind of ideal is one generated by a single element of the ring—such ideals are called *principal ideals* and have an important role in the first steps of number theory and the elementary theory of divisors.

1.1.2 Ideals, residue classes

Let $I \subset R$ be an ideal in a ring R. Inspired by the old theory of integer number congruences, Dedekind and followers arrived at a second important abstraction, namely, the notion of the ring of residue classes with respect to I.

As a first step, like in classical number congruences, one introduces an equivalence relation on R by decreeing that two elements $a_1, a_2 \in R$ are equivalent (or congruent) with respect to (or modulo) I if $a_1 - a_2 \in I$. This originates the residue class set R/I whose elements are the congruence classes thus defined and installs by default the residue map $R \to R/I$. From elementary group theory, R/I acquires the structure of an Abelian group (the only possible such structure if one requires that the natural map $R \to R/I$ become a group homomorphism).

In order to endow R/I with a ring structure, one invokes the characteristic property of ideals to define a product of classes and such that the group homomorphism $R \to R/I$ become a ring homomorphism (there is only one way to produce this, an observation first made explicit by Krull in [98]).

One needs a notation for the residue class of an element $a \in R$ or, equivalently, for the image of $a \in R$ by the residue map. Rigorously, one should use $a + I$, but unfortunately this becomes increasingly cumbersome as calculations evolve. Therefore, it

is usual to put a bar over the element—$\overline{a}$ as it is—provided the ideal I is clear from the context.

One reason to consider these generalized congruences can be formulated in the following elementary result.

Proposition 1.1.2. *Let $R \twoheadrightarrow S$ be a surjective homomorphism of rings. Then there is an ideal $I \subset R$ such that $S \simeq R/I$ and, moreover, this establishes a bijection between the set of surjective ring homomorphisms with source R, up to isomorphisms of the target, and the set of ideals of R.*

The proof is left as a recap exercise, as in this book one assumes familiarity with the so-called theorems of homomorphism (usually listed as first, second, etc.). These theorems were first proved by R. Dedekind and E. Noether in a complete generality both for ideals and modules, also for groups.

The idea of residual structures is capital in number theory, in commutative algebra for even more reason. It gives rise to an iteration procedure for regular elements, as follows.

Definition 1.1.3. Let R be a ring. A sequence (yes, the order may be important) of elements $\{a_1, \ldots, a_n\} \subset R$ is a *regular sequence* if, for every $1 \leq i \leq n$, the residue of the element a_i in $R/(a_1, \ldots, a_{i-1})$ is a nonzero divisor.

(For $i = 1$, one takes the ideal $(a_1, \ldots, a_{i-1})$ to mean $\{0\}$.) The importance of this concept goes beyond any expectation, giving shape to a dramatic role in commutative algebra.

1.1.3 Ideal operations

Here, "operation" is to be understood in the sense of a rule to combining one or more ideals in order to obtain another ideal. One briefly recapitulates them as readers are supposed to be familiar with their nature from elementary ring theory courses.

1.1.3.1 Intersection of ideals

Given ideals $I, J \subset R$, the set theoretic intersection $I \cap J$ is already an ideal, as one readily verifies. Although a simple-minded operation, it is hard to come by in terms of generators if one aims to describe a set of generators of $I \cap J$ as functions of given sets of generators of the constituent ideals—at least in the form of some universal explicit expression (an exception is the case of ideals generated by monomials in a polynomial ring over a field). On the bright side, explicit machine calculation enacts one to reach the result.

The notion extends without further ado to the case of an arbitrary family of ideals. A deep question is to "decompose" a given ideal as the intersection of a family

of ideals sharing some common features. A facet of this problem will be tackled in Section 2.6.

1.1.3.2 Sum of ideals

The set theoretic union of two ideals $I, J \subset R$ is not an ideal, unless one of them is contained in the other. So, one takes the ideal generated by $I \cup J$—this is called the *ideal sum* of the two ideals and is denoted by $I + J$ or (I, J). The second notation was largely favored in parts of the classical literature and is the one to be employed in this book. On the other hand, the first notation and the terminology are largely justified by the fact that a typical element of $I + J$ has the form $a + a'$, with $a \in I$ and $a' \in J$, thus sharing the goodies of the notion of summing two subgroups of an additively written Abelian group or two subspaces of a vector space. In particular, an arbitrary expression $a+a'$ uniquely determines its summands if and only if $I \cap J = \{0\}$. In the case of Abelian groups or vector spaces, this condition implies direct sum $I \oplus J$. However, the burden carried by the ring multiplication and by the ideal theoretic main property cause the null intersection to be a somewhat rare phenomenon since it requires lots of zero-divisors in the ring.

In contrast to the case of ideal intersection, the ideal sum is easily obtained in terms of generators, namely, if $I = (S)$ and $J = (S')$ then $(I, J) = (S \cup S')$. Note that, since $S \cap S' \subset S \cup S'$, there is quite a bit of superfluous generators in the union. The ideal sum notion applies *ipsis literis* to an arbitrary family of ideals and appears quite often in the argument of a general proof and is a useful construction as such.

1.1.3.3 Product of ideals

Given ideals $I, J \subset R$, the set $\{ab \mid a \in I, b \in J\}$ of products is not an ideal either (unless at least one of them is principal). The ideal generated by this set is called the *ideal product* and is denoted by IJ. Here, the generators question is rather trivial for if $I = (S)$ and $J = (S')$ then the ideal product IJ is generated by the set $\{ss' \mid s \in S, s' \in S'\}$.

Note the relation of the product to the intersection: as IJ is contained both in IR and in JR, it follows that $IJ \subset I \cap J$. Thus, a measure of obstruction as to when $I \cap J = \{0\}$ holds is that $IJ = \{0\}$, which says that every element of one ideal is zero-divided by every element of the second ideal, a rather severe condition. At the other end of the spectrum, the equality $IJ = I \cap J$ seldom takes place, turning out to be rather a difficult condition of "transversality."

The ideal product extends easily to a finite family of ideals. A special nevertheless exceedingly important case is that of a constant family $\{I_i\}_{i=1}^m$, $I_i = I (1 \leq i \leq m)$. In this case, the ideal product is called the mth *power* of the ideal I and is naturally denoted by I^m. Note that if $I = (s_1, \ldots, s_n)$ then I^m is generated by the "monomials" of "degree" m in $s_1, \ldots, s_n$. The question as to how many of these monomial-like generators are actually superfluous turns out to be a rather deep question related to the notion of analytic independence of ideal generators—a tall order in modern commutative algebra.

Besides, the chain $R = I^0 \supset I = I^1 \supset I^2 \supset \cdots$ plus the multiplication rule $I^m I^n = I^{m+n}$ give rise to deep considerations in both commutative algebra and algebraic geometry. The two topics are in fact quite intertwined.

1.1.3.4 Quotient of ideals

This operation is perhaps less natural than all the previous ones. At a later stage of the book, it will be shown that it has the effect of sorting out the "components" of one ideal away from the second ideal. As a figure of speech, it is very roughly a formalization of "division without rest" from elementary arithmetic. In particular, the order in which the two ideals $I, J \subset R$ are given is relevant as opposed to the previous operations. One defines the *quotient ideal* of I by J as

$$I : J := \{a \in R \mid aJ \subset I\},$$

where $aJ = \{ab \mid b \in J\}$. It is easily seen that this is indeed an ideal. Albeit the vague resemblance to division in elementary arithmetic, it would perhaps be more accurate to call $I : J$ the (multiplicative) *conductor* of J in I.

For $I = \{0\}$, the quotient ideal $0 : J$ is called the *annihilator* of J. In general, passing to the residue class ring R/I, the quotient $I : J$ is nothing else than the inverse image in R of the annihilator of the ideal $(I, J)/I \subset R/I$.

Some of the elementary properties of the quotient are:

(a) $I : J = R$ if and only if $I \supset J$.
(b) $I \subset I : J$ and the equality holds if J contains some element whose residue class in R/I is not a zero-divisor. In particular, if I is a prime ideal and J is not contained in I then $I = I : J$.
(c) (Resemblance to exact division of numbers) If R is a factorial domain (UFD), $I = (a)$, $J = (b)$ being principal ideals, then $I : J$ is the (principal) ideal generated by the product of all factors of a that do not divide b.

Obtaining a set of generators of $I : J$ is a nontrivial matter. For a full treatment of this problem, one may have to resort to sophisticated tools, such as primary decomposition (Section 2.6).

1.1.3.5 The radical of an ideal

One source for the concept of radical of an ideal is the simplification process of switching from the complete factorization of an integer or a polynomial to its square-free factorization in which one omits any multiplicity higher than 1.

This crude idea underwent various stages, eventually ending up in the following formal definition: the *radical* of an ideal $I \subset R$ is the set $\{a \in R \mid \exists r \geq 0, a^r \in I\}$.

This is easily seen to be an ideal of R containing the ideal I. In this book, it is denoted by the symbol $\sqrt{I}$. An ideal is said to be *radical* if it coincides with its radical (same vocable, twisting the grammar). Clearly, the radical of an ideal is a radical ideal.

Determining a set of generators of $\sqrt{I}$ given a set of generators of I is a hard knuckle (an exception is the case of an ideal generated by monomials in a polynomial ring over a field). In order to express the radical of I, one needs a knowledge of other ideals related to I, the so-called minimal prime ideals associated to I. A prime ideal is an extremely relevant building part of the commutative algebra compound and will be reviewed next.

One of the nice properties of taking the radical of an ideal is the following:

$$\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}.$$

1.1.4 Prime and primary ideals

A prime ideal is the most notable instance of a radical ideal. In fact, the two notions are more deeply intertwined than is predicted by their formal definitions. It is not very clear who has the exact priority for the inception of this concept, with Kronecker claiming he had it before the Dedekind–Noether advances (see Historic note, Subsection 1.3.1).

Recall the formal definition.

Definition 1.1.4. An ideal $I \subset R$ is *prime* if it satisfies any of the following equivalent conditions:

(1) Given $a, b \in R$ such that $ab \in I$, then $a \in I$ or $b \in I$.
(2) Given ideals $J, J' \subset R$ such that $JJ' \subset I$, then $J \subset I$ or $J' \subset I$.
(3) The residue class ring R/I has no proper zero-divisors.

Recall that the third condition above is transcribed in the notion of an *integral domain*. Here, one assumes that in an integral domain $1 \neq 0$ (*i. e.*, the zero ring is not considered to be an integral domain). Likewise, for condition (3) to be equivalent to (1) and (2), one takes for granted that a prime ideal is always proper. This has the additional convenience that a prime ideal is always contained in a maximal ideal, by a suitable use of Zorn's lemma (Kuratowski–Zorn lemma: a partially ordered set such that every totally ordered subset has an upper bound, necessarily contains at least one maximal element).

Clearly, a prime ideal is a radical ideal. In fact, just as easily one sees that the intersection of an arbitrary collection of prime ideals is a radical ideal. There is a converse to this statement.

Proposition 1.1.5 (Krull). *The radical of an ideal is the intersection of the family of prime ideals containing it.*

Proof. Let $I \subset R$ be an ideal. Clearly, $\sqrt{I}$ is contained in any prime ideal that contains I. Conversely, let $u \in R \setminus \sqrt{I}$ and set $S = \{u^n \mid n \geq 0\}$. By assumption, $I \cap S = \emptyset$. By a ready

application of Zorn's lemma, one can find an ideal $P \subset R$ maximal in the (nonempty) family of ideals that contain I and do not intersect S. The proof will be completed if one shows that P is a prime ideal since then P will be a prime ideal containing I such that $u \notin P$. Thus, let $a, b \in R$ be such that $ab \in P$, but neither a nor b belongs to P. Then the ideals (P, a) and (P, b) are both strictly larger than P, hence by the maximality assumption both intersect S. Let m, n be suitable integers such that $u^m \in (P, a)$ and $u^n \in (P, b)$. Writing down these two conditions, multiplying them out and using the condition $ab \in P$ yields $u^{m+n} \in P$, contradicting the assumption $u \notin P$. □

In the previous proposition, one can restrict oneself to the subfamily of prime ideals which are minimal in the family of all prime ideals containing I. Still, in general, this family may turn out to be infinite. As will be shown later on, for a Noetherian ring this family is finite.

Taking the radical of an ideal $I \subset R$ resembles forgetting its built-in "multiplicities." Going somewhat in the opposite direction, one can so to say recover "infinitesimals" by introducing primary ideals.

Definition 1.1.6. A nonzero ring R is *primary* if every zero-divisor is nilpotent. An ideal I in a ring R is *primary* if R/I is a primary ring.

If $I \subset R$ is a primary ideal, it follows immediately that $\sqrt{I}$ is a prime ideal P. To enhance this fact, one then says that I is P-primary and that P is the associated prime of I. Thus, an ideal $I \subset R$ is P-primary whenever given elements $a, b \in R$ such that $ab \in I$, but $a \notin I$, then $b \in P$.

Here is a source of examples of primary ideals.

Proposition 1.1.7. *Let $I \subset R$ be an ideal whose radical is a maximal ideal $\mathfrak{m} \subset R$. Then I is an $\mathfrak{m}$-primary ideal.*

Proof. One proves: if $a, b \in R$ are such that $ab \in I$ and $b \notin \mathfrak{m}$, then $a \in I$. Since $\mathfrak{m}$ is a maximal ideal and $b \notin \mathfrak{m}$, one can write $1 = bc + x$, for some $c \in R$ and $x \in \mathfrak{m}$. Let $x^n \in I$. Raising both sides to the nth power and multiplying them by a yields $a = dab + ax^n$, for some $d \in R$. Therefore, $a \in I$. □

The above result is no longer true if "maximal" is replaced by "prime" (see Exercise 1.4.7)

1.1.5 A source of examples: monomial ideals

One of the most important examples of a ring in this book is a polynomial ring in n indeterminates, over a field k. Notation: $R = k[X_1, \ldots, X_n]$. This ring, along with its residue class rings will be thoroughly examined in forthcoming sections. Here, one wishes to single out a particular family of ideals in R, which has a distinctive role

throughout modern commutative algebra and its computational side. This is the class of monomial ideals, to be briefly surveyed now.

An ideal $I \subset R = k[X_1, \dots, X_n]$ is called a *monomial ideal* if it can be generated by a finite set of monomials $\mathbf{X}^{\mathbf{a}} = X_1^{a_1} \cdots X_n^{a_n}$, for varying $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{N}^n$. The *support* of a such a monomial $\mathbf{X}^{\mathbf{a}}$ is the set of variables X_i (or their respective indices) such that $a_i > 0$. Denote by $\sqrt{\mathbf{X}^{\mathbf{a}}}$ the product of the variables in the support of the monomial $\mathbf{X}^{\mathbf{a}}$.

Let $I \subset R$ be an ideal. A basic criterion for I to be a monomial ideal is that, whenever $f \in I$ then every nonzero term (= monomial affected by a coefficient from k) of f also belongs to I. Moreover, given a set $\mathbf{u}$ of monomial generators of a monomial ideal I, if $f \in I$ then every nonzero term of f is a multiple of some monomial in $\mathbf{u}$. This is besides a great facilitator in the calculations.

In particular, one advantage of a monomial ideal is that one needs not dancing around with different sets of minimal generators. Precisely, if G and H are sets of monomial generators of an ideal, which are both minimal with respect to divisibility (*i. e.*, if $u, v \in G$, then neither $u \notin (v)$, nor $v \notin (u)$), then $G = H$.

Given two monomials u, v, $\gcd(u, v)$ denotes their greatest common divisor and $\operatorname{lcm}(u, v)$, their least common multiple.

The class of monomial ideals is closed under most common ideal operations, certainly under the ones for arbitrary ideals.

Proposition 1.1.8. *Let $I, J \subset R$ denote monomial ideals, with respective sets of monomial generators* $\mathbf{u}$ *and* $\mathbf{v}$.

(i) *$I \cap J$ is generated by the set of monomials* $\operatorname{lcm}(u, v)$, *with $u \in \mathbf{u}$ and $v \in \mathbf{v}$.*

(ii) *If $v \in R$ is a single monomial, then $I : v$ is generated by the set of monomials* $u/\gcd(u, v)$, *with $u \in \mathbf{u}$. In particular, $I : J$ is the monomial ideal given as $\bigcap_{v \in \mathbf{v}} I : v$.*

(iii) *The radical of I is a monomial ideal, generated by the monomials $\sqrt{u}, u \in \mathbf{u}$.*

Proof. (i) Using the above criterion, it easily follows that $I \cap J$ is a monomial ideal. Moreover, it is clear that for any $u \in \mathbf{u}$ and any $v \in \mathbf{v}$, $\operatorname{lcm}(u, v) \in I \cap J$. The reverse inclusion is also clear since, by the above criterion, one can argue with a monomial in $I \cap J$.

(ii) The argument is similar: clearly, $u/\gcd(u, v) \in I : v$, for any $u \in \mathbf{u}$. The reverse inclusion follows from the fact that $I : J$ is a monomial ideal by the above criterion. To pass to $I : J$ use the general equality in Exercise 1.4.3, (1).

(iii) It is clear that $\{\sqrt{u} \mid u \in \mathbf{u}\} \subset \sqrt{I}$. Conversely, let $f \in \sqrt{I}$, say, $f^r \in I$ for some $r \geq 1$. One inducts on the number of nonzero terms of f. If f is a monomial, then f^r is a multiple of some $u \in \mathbf{u}$, hence f is a multiple of $\sqrt{u}$. If f has at least to nonzero terms, one can show that it has a term w such that w^r does not cancel against any other terms of f^r, and hence w^r is a nonzero term of f^r. Since I is a monomial ideal, $w^r \in I$, hence $w \in \sqrt{I}$. Now apply the inductive assumption to the polynomial $f - cu$ (for suitable $c \in k \setminus 0$). □

1.2 Algebras

Let R be a ring and let S be an R-algebra, by which one means a ring S endowed with a given ring homomorphism $R \to S$—called the *structural map* of the algebra. R is often called the *base ring* of the algebra and one talks about S as being an algebra over R, as if given freedom for S to be an algebra over another base ring.

Since the map from R to its image in S is rather trivial in terms of algebras, one typically assumes that R has been replaced by its image, so the structural homomorphism is injective. By a similar token, hitherto by an *R-subalgebra* of the R-algebra S one means a subring $T \subset S$ containing R.

The notion of set of generators of algebras is modeled after sets of indeterminates in a polynomial ring, but of course it reaches well beyond.

Definition 1.2.1. Let S be an R-algebra as above and let $T \subset S$ be an R-subalgebra. A *set of generators* of T is a subset $\mathfrak{E} \subset T$ satisfying any of the following equivalent conditions:

- T is the smallest R-subalgebra of S containing $\mathfrak{E}$ by inclusion
- T is the intersection of all R-subalgebras of S containing $\mathfrak{E}$
- Every element of T has an expression of the form

$$\sum_{i_1,\dots,i_r} a_{i_1,\dots,i_r} s_1^{i_1} \cdots s_r^{i_r},$$

with $a_{i_1,\dots,i_r} \in R$ and $s_1, \dots, s_r \in \mathfrak{E}$.

Verifying the above equivalences is straightforward. Conversely, given an arbitrary subset $\mathfrak{E} \subset S$ of an R-algebra S, one can reproduce the R-subalgebra generated by $\mathfrak{E}$ sticking to any one of these formulations. Following Kronecker's original notation, one adheres to the notation $R[\mathfrak{E}]$ for this subalgebra.

1.2.1 Polynomials and finitely generated algebras

If, in addition, $\mathfrak{E} = \{s_1, \dots, s_n\}$ happens to be a finite set, one sets $R[\mathfrak{E}] = R[s_1, \dots, s_n]$, a mnemonic *déja vu* of the polynomial ring in n indeterminates; in this case, $R[s_1, \dots, s_n]$ is said to be *finitely generated* (or *of finite type*) over R.

The following statement is also adaptable for infinitely generated algebras, but the use in this book is mainly in the finitely generated case.

Proposition 1.2.2. *Let $R \subset S$ be an R-algebra of finite type. Then there is an R-isomorphism $R[X_1, \dots, X_n]/I \simeq S$, for a suitable ideal I of the polynomial ring $R[X_1, \dots, X_n]$.*

The proof is an immediate consequence of the universal property of the polynomial ring $R[X_1, \dots, X_n]$ and of the first theorem of the homomorphism for rings (*cf.* Proposition 1.1.2).

A surjective homomorphism as in Proposition 1.2.2 and its kernel are respectively called a *polynomial presentation* and a *presentation ideal* of the R-algebra S. An alternative terminology for the presentation ideal is *ideal of relations*. It is understood that these notions are not uniquely defined by the algebra itself as they depend on the choice of a set of generators.

A remarkable case is that of an R-subalgebra of the polynomial ring $R[X_1, \ldots, X_n]$. Even in the case where $R = k$ is a field, the richness of the structure of the k-subalgebras is anything but easily understood. At first sight, a finitely generated k-subalgebra of $k[X_1, \ldots, X_n]$ resembles any other integral domain of finite type over k. However, this resemblance is misleading since, *e. g.*, there are cases when such an algebra may turn up to be isomorphic to the homogeneous coordinate ring of a so-called *unirational* projective variety.

1.2.2 The transcendence degree

In this part, one focus on integral domains of finite type over a field k. The results of this subsection are independent from the characteristic of the base field k. Since no other base ring will come up other than k itself, one will denote a k-algebra by the letter R (instead of S).

One uses freely the following notation, originally conceived by Kronecker and rigorously set by Steinitz ([148]) more than one century ago: if $K|k$ is a field extension, *i. e.*, k is a subfield of the field K, and $\mathfrak{X} \subset K$ is a subset, then $k(\mathfrak{X})$ denotes the smallest inclusionwise subfield of K containing k and $\mathfrak{X}$. If $\mathfrak{X}$ consists of a single element x one writes $k(x)$ for short.

Recall that such an element x is said to be *algebraic* over k provided it is a root of a nonzero polynomial in $k[X]$. The extension $K|k$ is algebraic if all of its elements are algebraic over k.

Given a field extension $K|k$, the *algebraic closure* of k in K is the set of elements of K which are algebraic over k. By the elementary theory of algebraic elements in a field extension, one knows that this is an intermediate ("Zwischenkörper" in the terminology of Steinitz) field between k and K. For lack of better notation, it is usually denoted by $\overline{k}$ if the ambient field K is fixed in the discussion. This construction has the formal properties of a closure operator; in particular, taking the closure of a closure does not do anything, *i. e.*, $\overline{(\overline{k})} = \overline{k}$. One says that k is *algebraically closed* in K if $\overline{k} = k$.

In this book, one assumes the elementary theory of algebraic extensions, a topic that is part of a general algebraic training no matter how tricky parts of Galois theory maybe (specially in prime characteristic), whereas the main focus in this part is the transcendental side of field theory in its relation to the underlying ring theoretic aspects.

Thus, let R stand for an integral domain of finite type over k. Let K denote the field of fractions of R. The resulting inclusion $k \subset K$ makes K into a *finitely generated field*

extension $K|k$: a finite set of generators of R over k will generate K as a field extension of k as well.

Given a field extension $K|k$, a finite subset $\mathfrak{X} = \{x_1, \dots, x_n\} \subset K$ is said to be *algebraically independent* over k if the surjective k-homomorphism $k[X_1, \dots, X_n] \twoheadrightarrow k[\mathfrak{X}]$ mapping X_i to x_i $(1 \leq i \leq n)$ is injective.

Though this definition sounds repetitive, as it asserts that an algebraically independent set is essentially a set of indeterminates, its role will become clear as one progresses in the theory. This notion can be extended to possibly infinite sets by requiring that every finite subset have the property.

The next notion plays for finitely generated field extensions a similar role as a vector basis does for vector spaces—in fact, both are particular cases of a more general matroid theory phenomenon, but one will refrain from bringing it up here. As finitely generated extensions include finite extensions as a special case, one must allow for the new notion to encode this flexibility. The most general statement goes like the following.

Definition 1.2.3. A *transcendence basis* of a field extension $K|k$ is a subset $\mathfrak{B} \subset K$ satisfying the following conditions:
(i) $\mathfrak{B}$ is algebraically independent.
(ii) The extension $K|k(\mathfrak{B})$ is algebraic.

If $K|k$ is further finitely generated and $\mathfrak{X} \subset K$ contains a transcendence basis, then $K|k(\mathfrak{X})$ is in fact a finite extension. One of the main goals here is to prove that any subset $\mathfrak{X} \subset K$ such that $K|k(\mathfrak{X})$ is algebraic contains a transcendence basis and this is necessarily a finite set in case $K|k$ is finitely generated.

Proposition 1.2.4. *Let $K|k$ be a field extension, let $\mathfrak{X} \subset K$ be such that the extension $K|k(\mathfrak{X})$ is algebraic. If $\mathfrak{U} \subset K$ is any algebraically independent subset, then there exists a subset $\mathfrak{X}' \subset \mathfrak{X}$ such that $\mathfrak{X}' \cap \mathfrak{U} = \emptyset$ and $\mathfrak{X}' \cup \mathfrak{U}$ is a transcendence basis of $K|k$.*

Proof. The proof will tacitly assume that $\mathfrak{X}$ is a finite set—this is honestly a minor point and the reader will have no problem in extending the argument to the general case by an appropriate form of Zorn's lemma. Consider the family of subsets $\mathfrak{X}' \subset \mathfrak{X}$ such that $\mathfrak{X}' \cap \mathfrak{U} = \emptyset$ and $\mathfrak{X}' \cup \mathfrak{U}$ is algebraically independent (such subsets do exist since $\emptyset$ is one of them). Take one such subset $\mathfrak{X}'$ with largest number of elements. One claims that the extension $K|k(\mathfrak{X}' \cup \mathfrak{U})$ is algebraic. By the well-known fact on the transitivity of algebraic extensions, it suffices to show that every element of $\mathfrak{X}$ is algebraic over $k(\mathfrak{X}' \cup \mathfrak{U})$. But if $x \in \mathfrak{X} \setminus \mathfrak{X}' \cup \mathfrak{U}$ is transcendental over $k(\mathfrak{X}' \cup \mathfrak{U})$, then the whole set $\mathfrak{X}' \cup \mathfrak{U} \cup \{x\}$ is algebraically independent over k (*cf.* Exercise 1.4.12). This contradicts the choice of $\mathfrak{X}'$ as now $\mathfrak{X}' \cup \{x\}$ is strictly larger and still belongs to the family. □

As a consequence, one sees that for an extension $K|k$, any subset $\mathfrak{U}$ such that $K|k(\mathfrak{U})$ is algebraic contains a transcendence basis of $K|k$. In particular, any ordinary

set of generators of $K|k$ contains such a basis. This gives us plenty of transcendence bases to pick.

Next is the main result on transcendence bases, to wit, that any two such bases of the same field extension $K|k$ have the same cardinality. This is quite parallel to the analogue for linear bases of vector spaces—by suitably replacing "linear span" by "algebraic closure"—and hinges in fact on the same basic matroid-like principle which one now proceeds to introduce.

Lemma 1.2.5. *Let $K|k$ be a field extension and let $\mathfrak{U} \subset K$ be an arbitrary subset. Given elements $x, y \in K$ such that $y \in \overline{k(\mathfrak{U} \cup \{x\})} \setminus \overline{k(\mathfrak{U})}$, then $x \in \overline{k(\mathfrak{U} \cup \{y\})}$.*

Proof. As the reader can verify, one may assume that $\mathfrak{U}$ is a finite set, say, $\mathfrak{U} = \{x_1, \ldots, x_r\}$. By hypothesis, y is algebraic over $k(x_1, \ldots, x_r, x)$. By suitably clearing denominators, one can assume that there exists a polynomial $F = F(X_1, \ldots, X_r, X, Y) \in k[X_1, \ldots, X_r, X, Y]$ (please, note the capital letters) such that $F(x_1, \ldots, x_r, x, Y) \neq 0$ and $F(x_1, \ldots, x_r, x, y) = 0$. If one shows that $F(x_1, \ldots, x_r, X, y) \neq 0$, this will prove that x is algebraic over $k(\mathfrak{U} \cup \{y\})$. Thus, write F in the variable X with coefficients $G_i = G_i(X_1, \ldots, X_r, Y)$. Since F is by hypothesis a polynomial of positive degree in Y and y is transcendental over $k(x_1, \ldots, x_r)$ then some $G_j \neq 0$ for $j \geq 1$ and again $G_j(x_1, \ldots, x_r, y) \neq 0$. Therefore, $F(x_1, \ldots, x_r, X, y) \neq 0$, as was required. □

Next is the main result of this part. To avoid fiddling around with Zorn's lemma, one sticks to finitely generated field extensions. (The use of this axiom or alike—such as Zermelo's axiom or the Axiom of Choice—was very much under discussion at Steinitz writing, as one can read in the introduction of [148].)

Theorem 1.2.6 (Invariance of the transcendence degree). *Let $K|k$ be a finitely generated field extension. Then all transcendence bases of $K|k$ are finite and have the same number of elements.*

Proof. By a special case of Proposition 1.2.4 one can assume that $K|k$ has a finite transcendence basis $\mathfrak{B}$. Let $\mathfrak{B}' \subset K$ be an arbitrary transcendence basis of $K|k$. It clearly suffices to show that $\mathfrak{B}'$ is finite and has same number of elements as $\mathfrak{B}$. Set $\mathfrak{B} = \{x_1, \ldots, x_m, x_{m+1}, \ldots, x_n\}$, where $\mathfrak{B} \cap \mathfrak{B}' = \{x_1, \ldots, x_m\}$. One proceeds by induction on the difference $n - m$.

For $n - m = 0$, one has $\mathfrak{B} \subset \mathfrak{B}'$ and, forcefully, $\mathfrak{B} = \mathfrak{B}'$ otherwise some element of $\mathfrak{B}'$ would be algebraic over $\mathfrak{B}$ and yet not belonging to it, and this would contradict the algebraic independence of $\mathfrak{B}'$.

By the inductive hypothesis, the result holds for any finite transcendence basis $\mathfrak{B}_1$ of $K|k$ such that $\mathfrak{B}_1 \cap \mathfrak{B}'$ has $m + 1$ elements. As above, one can assume that $\mathfrak{B} = \{x_1, \ldots, x_m, x_{m+1}, \ldots, x_n\}$, where $\mathfrak{B} \cap \mathfrak{B}' = \{x_1, \ldots, x_m\}$, only now $n > m$; say, x_{m+1} appears effectively in $\mathfrak{B}$. Since x_{m+1} is not algebraic over $k(\mathfrak{B} \setminus \{x_{m+1}\})$ and $\mathfrak{B}'$ is a transcendence basis then $\mathfrak{B}' \not\subset \overline{k(\mathfrak{B} \setminus \{x_{m+1}\})}$ (why?). So, let $y \in \mathfrak{B}' \setminus \overline{k(\mathfrak{B} \setminus \{x_{m+1}\})}$ and set $\mathfrak{B}_1 = \mathfrak{B} \setminus \{x_{m+1}\} \cup \{y\}$. Clearly, $\mathfrak{B}_1$ has as many elements as $\mathfrak{B}$ and $\mathfrak{B}_1 \cap \mathfrak{B}'$ has $m+1$ elements.

One claims moreover that $\mathfrak{B}_1$ is a transcendence basis of $K|k$. Indeed, it is certainly algebraically independent over k since y is a transcendental over $k(\mathfrak{B} \setminus \{x_{m+1}\})$ (once more, by Exercise 1.4.12). Next, by the same token and by Lemma 1.2.5, one has $x_{m+1} \in \overline{k(\mathfrak{B}_1)}$. This implies that $\mathfrak{B} \subset \overline{k(\mathfrak{B}_1)}$, hence $K = \overline{k(\mathfrak{B})} \subset \overline{k(\mathfrak{B}_1)}$, as required.

Applying the inductive hypothesis one is lead to conclude that $\mathfrak{B}_1$ and $\mathfrak{B}'$, hence also $\mathfrak{B}$ and $\mathfrak{B}'$, have the same number of elements. □

One is thus lead to a basic numerical invariant of a finitely generated field extension.

Definition 1.2.7. The *transcendence degree* of a finitely generated field extension $K|k$ is the common cardinality of all its transcendence bases. The notation is $\mathrm{trdeg}_k(K)$ or $\mathrm{trdeg}(K|k)$.

Now let R be a finitely generated domain over a field k and let K denote its field of fractions. One defines the transcendence degree of R over k to be the transcendence degree of K over k. Clearly, $K|k$ is generated by any finite set of generators of R over k, hence $\mathrm{trdeg}_k(R)$ is a (finite) number. Likewise, by Proposition 1.2.4, any finite set of generators of R over k contains a transcendence basis of $K|k$.

1.2.3 Basic properties of the transcendence degree

However difficult recognizing whether a certain set is algebraically independent, there are some basic steps that come to help.

Proposition 1.2.8 (Modding out irreducible polynomials). *Let $B = k[X_1, \ldots, X_n]$ be a polynomial ring over a field k and let $f \in B$ denote a nonzero irreducible polynomial. Then* $\mathrm{trdeg}_k(B/(f)) = n - 1$.

Proof. First, $\mathrm{trdeg}_k(B) = n$ since $\{X_1, \ldots, X_n\}$ is a transcendence basis of B over k. Write $f = \sum_{j=0}^{m} f_j(X_1, \ldots, X_{n-1}) X_n^j$. One can assume that $m > 0$ and $f_m(X_1, \ldots, X_{n-1}) \neq 0$ (how?). Let x_i denote the class of X_i modulo (f). Then $\sum_{j=0}^{m} f_j(x_1, \ldots, x_{n-1}) x_n^j = 0$, showing that $\mathrm{trdeg}_k(B/(f)) \leq n - 1$. On the other hand, $\{x_1, \ldots, x_{n-1}\}$ is algebraically independent over k. Indeed, otherwise an equation of algebraic dependence would yield a nonzero polynomial $g \in k[X_1, \ldots, X_{n-1}]$ such that $g \in (f)$, which is absurd since f has a nonzero term involving X_n. □

The preceding proposition has no obvious generalization to arbitrary prime ideals. However, one can state the following weak version.

Proposition 1.2.9 (Going modulo a prime ideal). *Let B be a finitely generated domain over a field k and let $P \subset B$ be a prime ideal. Then* $\mathrm{trdeg}_k(B/P) \leq \mathrm{trdeg}_k(B)$, *with equality (if and) only if $P = \{0\}$.*

Proof. Let $\operatorname{trdeg}_k(B/P) = n$. Pick elements $x_1, \dots, x_n \in B$ whose residue classes in B/P form a transcendence basis of B/P over k. Then the set $\{x_1, \dots, x_n\}$ is algebraically independent over k, since a nonzero algebraic relation of its elements is obviously also one of the respective residue classes in B/P. This shows the stated inequality.

As for the relevant implication in the equality statement, since one is assuming that $\operatorname{trdeg}_k(B/P) = \operatorname{trdeg}_k(B)$, then $\{x_1, \dots, x_n\}$ is actually a transcendence basis of B over k by the invariance of the transcendence degree. Suppose that there is a non-zero element $z \in P$. Then z is algebraic over the subfield $k(x_1, \dots, x_n)$. Multiplying out by a common denominator, there is a nonzero polynomial $F(X_1, \dots, X_n, Z) \in k[X_1, \dots, X_n, Z]$ such that $F(x_1, \dots, x_n, z) = 0$. Write $F = \sum_{j=0}^{m} F_j(X_1, \dots, X_n)Z^j$. One can assume that F has minimum possible degree in the variable Z, in which case necessarily $F_0(x_1, \dots, x_n) \neq 0$ (why?), hence also $F_0(X_1, \dots, X_n) \neq 0$.

On the other hand, taking residue classes modulo P, one obtains

$$\overline{0} = \overline{F(x_1, \dots, x_n, z)} = \sum_{j=0}^{m} F_j(\overline{x_1}, \dots, \overline{x_n})\overline{z}^j.$$

Since $z \in P$, then $\overline{z} = \overline{0}$, hence $F_0(\overline{x_1}, \dots, \overline{x_n}) = \overline{0}$. But the classes $\overline{x_1}, \dots, \overline{x_n}$ were originally assumed to be algebraically independent over k. Therefore, $F_0(X_1, \dots, X_n) = 0$—a contradiction. □

Dedekind's result on multiplying out degrees of successive algebraic extensions has its counterpart in transcendental extensions in terms of addition.

Proposition 1.2.10 (Additivity). *Let $k \subset L \subset K$ be fields. Then* $\operatorname{trdeg}_k(K) = \operatorname{trdeg}_k(L) + \operatorname{trdeg}_L(K)$.

Proof. Let $\mathfrak{B}$ (resp., $\mathfrak{B}'$) be a transcendence basis of $L|k$ (resp., of $K|L$). First, $\mathfrak{B} \cup \mathfrak{B}'$ is algebraically independent over k which can easily be proved directly from the definition or else by using Exercise 1.4.12. In particular, the cardinality of this set is the sum of the cardinality of $\mathfrak{B}$ and the cardinality of $\mathfrak{B}'$. This is half of what is claimed.

Next, by using the basic property of the (relative) algebraic closure, one has $K = \overline{L(\mathfrak{B}')} = \overline{\overline{k(\mathfrak{B})}(\mathfrak{B}')} = \overline{k(\mathfrak{B})(\mathfrak{B}')} = \overline{k(\mathfrak{B} \cup \mathfrak{B}')}$. This shows that $\mathfrak{B} \cup \mathfrak{B}'$ is a transcendence basis of $K|k$ and concludes the proof. □

For two unrelated subextensions, one has the following weaker result.

Proposition 1.2.11 (Subadditivity). *Let $K|k$ be a field extension and let $L_1, L_2 \subset K$ subfields containing k. Then* $\operatorname{trdeg}_k(L) \leq \operatorname{trdeg}_k(L_1) + \operatorname{trdeg}_k(L_2)$, *where $L \subset K$ is the subfield of K generated by L_1 and L_2.*

Proof. Let $\mathfrak{B}_1$ (resp., $\mathfrak{B}_2$) be a transcendence basis of $L_1|k$ (resp., of $L_2|k$). As in the proof of the previous proposition, one can see that $L = \overline{k(\mathfrak{B}_1 \cup \mathfrak{B}_2)}$—the details are left to the reader. The only highlight here is that though $\mathfrak{B}_1 \cup \mathfrak{B}_2$ may not be altogether

algebraically independent over k, by Proposition 1.2.4 it contains a subset which is a transcendence basis of $L|k$. This proves the stated inequality. □

1.3 Historic note

1.3.1 Terminology

It is curious that, historically, the germ of the notion of an abstract ideal somewhat preceded that of an abstract ring. It is well known that this first originated in the work of Kummer on algebraic numbers, later extended and reformulated by Dedekind. Although claimed by Kronecker that he had this notion long before (mid XIX probably), the full development of the theory can be attributed to Dedekind (see History 1.3.2 for further conflicting mathematical philosophies of these two great authors). At the other end, none of these mathematicians ever cared to establish the idea of an abstract ring. The latter first appeared in a paper of E. Noether, where she attributed to her student, Fraenkel, a first full definition of a ring in abstract. This late appearance is understandable in the light of the fact that most mathematicians at the time were interested in "concrete" *Integritätsbereiche* coming either from arithmetic or algebraic geometry, from Kronecker and Dedekind all the way to Hilbert.

Another piece of the missing link is the idea of a ring homomorphism. Surely, ring extensions were common, so subconsciously the idea of a homomorphism was implicit but not in the apparel of a map. The failure to fully uncovering the idea of a map may explain why the idea of formally comparing ideals via a homomorphism would not be current practice. The idea and terminology of contraction of an ideal from an overring was first used by E. Noether [120, No. 31, Section 1, p. 534 (original p. 87)] who attributes it to H. Grell. If P is a prime ideal, then its contraction to a subring is also prime. This is partly the reason to favor prime ideals over maximal ideals as the latter fail to be stable under contraction in general (see however the next chapter where maximal ideals are stable under contraction for a suitable class of rings, thus making possible to develop algebraic geometry over an algebraically closed field).

1.3.2 Early roots

Roots of commutative algebra can be found throughout the late part of the eighteenth century and first half of the nineteenth century. Along the same period, the theory of matrices and determinants was still stumbling and only became a solid theory toward the end of the nineteenth century: the terminology "matrix" was used for the first time in 1850 by Sylvester.

The notion of ideal through its axiomatic definition is due to R. Dedekind. According to the best sources, the terminology has been dug out of the efforts of Kummer

to deal with the failure of unique factorization in algebraic number ring extensions of $\mathbb{Z}$.

Kronecker claimed he already had in the 1850s the main features of ideal and module theory, including a reasonably definite notion of a prime ideal (*cf.* the Festchrift in honor of Kummer's Fünfzigjahr, in Kronecker's Gesammtwerke, where he says he had long before suggested the concept to others, Dedekind included). In a paper, he introduced the idea of the sum of two ideals and the notion of "decomposable" ideals in the sense of being the ideal product of two others. It seems that he had at the time considered some version of primary or prime decomposition, but it is not clear he had the correct notion.

Kronecker already uses the concepts of a field and of an integral domain (named *Rationalitätbericht* and *Ganzhaliggebericht*, resp.). In this respect, he uses the respective notation $(\mathfrak{S}_1, \mathfrak{S}_2, \ldots)$ and $[\mathfrak{S}_1, \mathfrak{S}_2, \ldots]$, our modern notation for field and ring extensions being reminiscent of his. However, because Kronecker considered only finitely generated ideals, he seemed to have completely missed the relevance of the Noetherian assumptions only later clarified by E. Noether.

Kronecker and Dedekind were contemporaneous scientists of enormous mathematical caliber and strong personality, not sharing the same philosophical approach toward mathematics. Both approaches left an enormous legacy to modern algebra, and mathematics as a whole. They developed at length the various questions around the notion of a module, with the difference that Dedeking was more focused on a particular class of modules—what nowadays are called *fractional ideals* in the field of fractions of an integral domain. In fact, his interest was solely in the case where the domain was the integral closure of the ring of integers in a finite extension of the field of rational numbers. Notation was a flagrant difference in the two mathematicians' styles. While Kronecker always chose a tautological notation, Dedekind's preference was a unique letter, mostly the capitalized first letter of a notion name (*e. g.*, *K* for Körper). In a sense, the philosophy of Kronecker's approach to notational convention was to become well established throughout the time, no matter how cumbersome it looks from our modern view. Here is a tiny example: the term "Bereich" (domain) used by Kronecker became universal, in fact invariant in the translation to other languages. Dedekind's "Körper" on the other hand, became "corps" in French, "field" in English, while in Spanish both "cuerpo" and "campo" seem to fight each other.

The theory of field extensions was set on firm ground some years after Kronecker and Dedekind in the long paper of Steinitz ([148]). For the first time, the modern notation (or most of it) is clearly taken up in this work, whose reading is fluent even at the student level. Many of the later written accounts of field theory, in arbitrary characteristic, certainly had learned from Steinitz, whether making this explicit or not.

One example of Kronecker's legacy was his fundamental work on the factorization of a polynomial, still very much quoted in the algorithmic theory of factorization of multivariate polynomials. Theoretically, its significance lies in that it is first princi-

ples in the more encompassing theory of factoring a radical ideal into its prime ideal components.

The impact of introducing prime ideals into commutative algebra cannot be exaggerated. Historically, they came up even before the general concept of a ring had been established ([116]). It is somewhat disappointing that even after Noether's and Krull's monumental collection of results involving prime ideals ([120], [116], [117], [118], [98], [99]), most published books in general ring theory would not give them the deserved place, perhaps failing to foresee the remarkable role they would come to play in both commutative algebra and algebraic geometry. At any rate, with E. Lasker, E. Noether, F. S. Macaulay, B. L. van der Waerden, W. Gröbner, W. Krull and an additional handful of algebraists, prime ideals became increasingly germane and turned out to be one of the most fundamental concepts of the whole theory.

1.4 Exercises

Exercise 1.4.1. Prove the so-called second theorem of homomorphism: given ideals $J \subset I \subset R$ of a ring R, there is a natural ring isomorphism $(R/J)/(I/J) \simeq R/I$. As an illustration, show that, for any prime number p, the ring $\mathbb{Z}[X]/(p, X)$ is isomorphic to the field with p elements.

Exercise 1.4.2. Let I, J be ideal of a ring R. Show that $IJ \subset I \cap J$ and that the equality holds up to taking radicals. Can you express in elementary ways the fact that the two ideals have to be "sufficiently apart" in order to have equality on the nose (where the worst possible degeneration is when $I \subset J$)?

Exercise 1.4.3. Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ be ideals of a ring R.

(1) Prove the following equalities:
   - $\mathfrak{a} : (\mathfrak{b}, \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}) \cap (\mathfrak{a} : \mathfrak{c})$
   - $\mathfrak{a} : (\mathfrak{b}\mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}$
   - $(\mathfrak{a} \cap \mathfrak{b}) : \mathfrak{c} = (\mathfrak{a} : \mathfrak{c}) \cap (\mathfrak{b} : \mathfrak{c})$

(2) Prove the following inclusions and verify that they are equalities up to taking radical:
   - $(\mathfrak{a} \cap \mathfrak{b}, \mathfrak{c}) \subset (\mathfrak{a}, \mathfrak{c}) \cap (\mathfrak{b}, \mathfrak{c})$
   - $(\mathfrak{a} \cap \mathfrak{b})\mathfrak{c} \subset (\mathfrak{a}\mathfrak{c}) \cap (\mathfrak{b}\mathfrak{c})$
   - $(\mathfrak{a}\mathfrak{b}, \mathfrak{c}) \supset (\mathfrak{a}, \mathfrak{c})(\mathfrak{b}, \mathfrak{c})$
   - $\mathfrak{a} \cap (\mathfrak{b}, \mathfrak{c}) \supset (\mathfrak{a} \cap \mathfrak{b}, \mathfrak{a} \cap \mathfrak{c})$
   - $\mathfrak{a} \cap (\mathfrak{b}\mathfrak{c}) \supset (\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a} \cap \mathfrak{c})$.

Exercise 1.4.4. Given a ring R, let $I \subset R$ be an ideal and $a \in R$ an element.

(1) Prove the equality $(a) \cap I = (I : (a))a$.

(2) Assume that a is a regular element and let $b \in R$ be a regular element on $R/(a)$ (*i. e.*, the sequence $\{a, b\}$ is regular). Show that $If : (g) = (I : (g))f$.

Exercise 1.4.5. Let k denote a field and let $R = k[X_1, \dots, X_n]$ stand for the polynomial ring in n indeterminates over k. Show that, for any $d \geq 1$, the ideal generated by the monomials of degree d cannot be generated by less than $\binom{n-1+d}{n-1}$ elements.

Exercise 1.4.6. Let k be a field. Decompose each of the following ideals as the intersection of a set of finitely many prime ideals:
(1) $I = (XY, XZ, YZ) \subset k[X, Y, Z]$; and, more generally:
(2) $I = ((X_1 \cdots X_n)/X_i \mid 1 \leq i \leq n) \subset k[X_1, \dots, X_n]$
(3) $I = (X_i X_j \mid 1 \leq i < j \leq n) \subset k[X_1, \dots, X_n]$.

Exercise 1.4.7. Let $I = (X^2, XY) \subset k[X, Y]$ (k a field). Then $\sqrt{I} = (X)$, while $XY \in I$, but $X \notin I$ and $Y \notin (X)$.

Exercise 1.4.8. Let $I = (X^2 + YZ, Y^2 + XZ, Z^2 + XY) \subset \mathbb{Q}[X, Y, Z]$.
(1) Prove that I is a primary ideal and find its radical.
(2) Change the plus sign in one (resp., two, three) of the above equations. Explain the outcome.

Exercise 1.4.9. Consider the so-called *circulant* matrix

$$\mathcal{M} = \begin{pmatrix} X & Y & Z \\ Y & Z & X \\ Z & X & Y \end{pmatrix}$$

and let $I \subset \mathbb{Q}[X, Y, Z]$ denote the ideal generated by the partial derivatives of $f = \det(\mathcal{M})$.
(1) Show that I is generated by the 2×2 subdeterminants of any two columns or rows of $\mathcal{M}$.
(2) Confront with one of the ideals of the previous exercise.
(3) Show that $P = (x - y, y - z)$ is a minimal prime over I.
(4) Prove that I is a radical ideal, but not prime.

Exercise 1.4.10. Let $\varphi : R \to S$ stand for a ring homomorphism. Given an ideal $I \subset R$ (resp., $J \subset S$), the *extended ideal* of I (resp., the *contracted ideal* of J) is the ideal of S generated by the set image $\varphi(I)$ (resp., the ideal $\varphi^{-1}(J) \subset R$). Even if φ is not injective, it is common practice to denote these two operations by IS and $J \cap R$, respectively. With this convention:
(1) $I \subset IS \cap R$ and $(J \cap R)S \subset J$.
(2) Give examples where the inclusions of the previous item are proper.
(3) (Cone principle) et R be a commutative ring, let $I \subset R$ be an ideal and let X be an indeterminate over R. Then there is a natural ring isomorphism $R[X]/IR[X] \simeq (R/I)[X]$.

(4) (Monoidal extension) If R is a domain with field of fractions K, $a, b \in R (b \neq 0)$ and $S = R[a/b] \subset K$, then the contraction to R of the extended ideal aS contains the ideal $(a, b)R$. Moreover, if $aR \cap bR = (ab)R$ then $aS \cap R = (a, b)R$.

Exercise 1.4.11. Let k be a field and let $S = k[T^2 - 1, T^3] \subset R = k[T]$ (T an indeterminate).

(1) Write an explicit irreducible defining polynomial $f \in k[X, Y]$ of S over k.
(2) Show that S is equally generated by $\{T^2, T^3\}$ as a k-algebra, but the two ideals generated in S are quite different in nature—the first is the unit ideal, the second is a maximal ideal.
(3) In general, let $f_1, \ldots, f_m \in k[T_1, \ldots, T_r]$ be arbitrary polynomials in the indeterminates $T_1, \ldots, T_r$ and let $S = k[f_1, \ldots, f_m] \subset k[T_1, \ldots, T_r]$. Show that S admits a (possibly modified) set of generators over k that generates a maximal ideal of S.

Exercise 1.4.12. Let $K|k$ be a field extension. Show: for any algebraically independent subset $\mathfrak{U} \subset K$ and any element $x \in K$, the following are equivalent:

(1) $\mathfrak{U} \cup \{x\}$ is algebraically independent
(2) x is transcendent over $k(\mathfrak{U})$.

Exercise 1.4.13. Let $f_1, \ldots, f_m$ denote k-linearly independent homogeneous polynomials of the same positive degree in the polynomial ring $R = k[X_1, \ldots, X_n]$.

(1) Show that the k-subalgebra $S = k[f_1, \ldots, f_m] \subset R$ cannot be generated by less than m elements.
(2) More exactly, any set of generators of S is obtained from $\{f_1, \ldots, f_m\}$ applying an invertible k-linear transformation of k^m.
(3) Deduce that if $m > n$ then S is not isomorphic to a polynomial ring over k.

Exercise 1.4.14. Let k denote a field of characteristic zero.

(1) Prove: if $f \in R = [X_1, \ldots, X_n]$ is not a constant, then $\partial f / \partial X_i \neq 0$ for at least one i.
(2) Generalize: if $\{f_1, \ldots, f_m\} \subset R$ is algebraically independent over k then the Jacobian matrix $(\partial f_j / \partial X_i)_{1 \leq i \leq n}^{1 \leq j \leq m}$ has maximum rank (*i. e.*, m).
(Hint: induct on m.)

Exercise 1.4.15. Compute the transcendence degree and find a transcendence basis over a field k of the following k-domains of finite type:

(1) $k[X_1, \ldots, X_n]/\mathfrak{m}$, where $\mathfrak{m}$ is an arbitrary maximal ideal.
(2) $k[X, Y, Z]/(Z - f(X, Y), g(X, Y))$, where $f(X, Y)$, $g(X, Y)$ do not involve Z and $g(X, Y)$ irreducible over k.
(3) $k[X, Y, Z, W]/(XW - YZ, Y^2 - XZ, Z^2 - YW)$.

2 Main tools

2.1 Rings of fractions

Introduced by H. Grell [63], rings of fractions would soon become a very useful tool in ring theory. It is nearly impossible to develop or follow parts of commutative algebra without resorting in a way or another to fractions.

2.1.1 Definitions

Let R stand for a ring. A subset $\mathfrak{S} \subset R$ such that, for any $a, b \in \mathfrak{S}$ also $ab \in \mathfrak{S}$, is called *multiplicatively closed*. In order to avoid a disturbing zero denominator in fractions to be introduced below, one assumes that a multiplicatively closed set does not contain 0 (consequently, does not contain any nilpotents either).

The outset goal is to define a new ring S and a homomorphism $\iota : R \to S$ such that the elements of $\mathfrak{S}$ become units in S and S is generated by the image of R and the inverses of these units. As expected, the construction involves a universal property that makes S essentially unique.

The set $\mathfrak{a} := \bigcup_{u\in\mathfrak{S}}(0 : u)$ is easily seen to be an ideal of R. Besides, the elements of $\mathfrak{S}$ are nonzero divisors modulo $\mathfrak{a}$. Define a relation $\equiv$ on $R \times \mathfrak{S}$ by decreeing:

$$(a, s) \equiv (b, t) \quad \text{if and only if} \quad at - bs \in \mathfrak{a}.$$

Clearly, $\equiv$ is reflexive and symmetric. It is also transitive: if $(a, s) \equiv (b, t) \equiv (c, u)$ then $at - bs \in \mathfrak{a}$ and $bu - ct \in \mathfrak{a}$; multiplying the first (resp., the second) inclusion by u (resp., by s) and adding the results yields $t(au - cs) \in \mathfrak{a}$, hence $au - cs \in \mathfrak{a}$ by the above characteristic property of $\mathfrak{a}$. This shows that $(a, s) \equiv (c, u)$.

Since $\equiv$ is an equivalence relation, one can consider the quotient set $\mathfrak{S}^{-1}R := (R \times \mathfrak{S})/\equiv$ of this equivalence relation. Then one equips $\mathfrak{S}^{-1}R$ with a commutative ring structure such that the quotient map $\iota : R \to \mathfrak{S}^{-1}R$ is a homomorphism. In fact, requiring this and further that $\mathfrak{S}^{-1}R$ be generated by the image $\iota(R)$ and the inverses of the elements of $\iota(\mathfrak{S})$ make very natural the operations known since high school.

One briefly explains how this comes about. First, denoting the class of a pair (a, s) by a/s—a well-established notation—these requirements force the equalities

$$\iota(s)^{-1}\iota(a) = \iota(s)^{-1}\frac{a}{1} = \left(\frac{s}{1}\right)^{-1}\frac{a}{1} = \frac{1}{s}\frac{a}{1}.$$

Therefore, if $\iota(s)^{-1}\iota(a) = a/s$ is going to hold true it would better be because $(1/s)(a/1) = a/s$, so this indicates at least how to multiply out generators. Thus, after harmless identification, one must have

$$st(a/s + b/t) = \iota(s)\iota(t)\big(\iota(s)^{-1}\iota(a) + \iota(t)^{-1}\iota(b)\big) = \iota(a)\iota(t) + \iota(b)\iota(s) = at + bs,$$

https://doi.org/10.1515/9783110616989-002

which imposes us the general rule of addition. The argument for the general multiplication rule is similar and easier.

It is now routine to verify that the rules of addition and multiplication give well-defined operations on $\mathfrak{S}^{-1}R$.

Examples of multiplicatively closed sets are:

1. $\mathfrak{S} = \{s^n : n \geq 0\}$, where s is a nonnilpotent element of R.
2. The set of regular elements of R.
3. Given a prime ideal $P \subset R$, $R\backslash P$ is a multiplicatively closed set. More generally, if $\{P_\alpha\}_\alpha$ is a family of prime ideals, $R\backslash \bigcup_\alpha P_\alpha$ is multiplicatively closed.

Remark 2.1.1. It is interesting to note that the multiplicatively closed set $\mathfrak{S}$ in the second and third examples above has the following property: if a, b are elements of R such that $ab \in \mathfrak{S}$ then both a and b belong to $\mathfrak{S}$. A multiplicatively closed set having this property is often said to be saturated. An application of Zorn's lemma shows that, conversely, any saturated multiplicatively closed set is of the shape in the third example. In particular, the set of zero-divisors of R is a union of prime ideals—this property will be studied in more detail when R is a Noetherian ring.

2.1.2 General properties of fractions

One collects in a few propositions the main operational properties of the present notion.

As many constructions in commutative algebra, fractions also enclose a certain universal property.

Proposition 2.1.2 (Universal property). *Given a ring S and a homomorphism $\varphi : R \to S$ such that the elements of $\varphi(\mathfrak{S}) \subset S$ are invertible, then there is a unique homomorphism $\pi : \mathfrak{S}^{-1}R \to S$ such that $\varphi = \pi \circ \iota$.*

Proof. The following commutative diagram of ring homomorphisms encapsulates pictorially the main contents:

$$\begin{array}{ccc} R & \xrightarrow{\iota} & S^{-1}R \\ \varphi \searrow & \curvearrowright & \swarrow \pi \\ & S & \end{array}$$

For the existence, set $\pi(a/s) := \varphi(a)(\varphi(s))^{-1}$. This makes sense since by assumption $\varphi(s)$ is invertible in S. To see that this is a well-defined map, let $a/s = b/t$. Then, by construction, $at - bs \in \mathfrak{a}$. Say, $at - bs = a \in \mathfrak{a}$. By definition, $au = 0$ for some $u \in \mathfrak{S}$. Therefore, $\varphi(a)\varphi(u) = \varphi(au) = 0$, hence $\varphi(a) = 0$ again by the assumption that the elements of $\varphi(\mathfrak{S})$ are invertible in S. It follows that $\varphi(a)\varphi(t) = \varphi(b)\varphi(s)$, as was to be shown.

Since $\iota(a) = a/1$, the relation $\varphi = \pi \circ \iota$ is obvious.
Uniqueness is left to the reader. □

Note that the ideal $\mathfrak{a}$ is the kernel of the natural homomorphism $\iota : R \longrightarrow \mathfrak{S}^{-1}R$. Thus, ι is injective if and only if the elements of $\mathfrak{S}$ are regular. When $\mathfrak{S}$ is the whole set of regular elements of R, the ring $\mathfrak{S}^{-1}R$ is called the *total ring of fractions* of R. For many purposes, this ring is as good as the field of fractions in the case R is a domain.

One next studies the behavior of ideals under the taking of fractions.

Proposition 2.1.3 (Ideal behavior). *Let $\mathfrak{S}$ stand for a multiplicatively closed subset of R and let $I \subset R$ and $J \subset \mathfrak{S}^{-1}R$ be ideals.*

(i) *If $I \cap \mathfrak{S} \neq \emptyset$, then $\mathfrak{S}^{-1}I = \mathfrak{S}^{-1}R$; the converse holds when $\mathfrak{S}$ is saturated* (*see Remark* 2.1.1).

(ii) *J is the extended ideal of its inverse image, i. e., $J = \mathfrak{S}^{-1}\iota^{-1}(J)$, where $\mathfrak{S}^{-1}I \subset \mathfrak{S}^{-1}R$ denotes the extension of I in $\mathfrak{S}^{-1}R$ via ι.*

(iii) *Letting $J = \mathfrak{S}^{-1}I \subset \mathfrak{S}^{-1}R$, one has*

$$\iota^{-1}(J) = \bigcup_{s \in \mathfrak{S}} (I : s). \tag{2.1.3.1}$$

In particular, $I = \iota^{-1}(J)$ if and only if every element of $\mathfrak{S}$ is regular on R/I. If, moreover, $\mathfrak{S}$ is the set of the powers of a nonnilpotent element $a \in R$ then $\iota^{-1}(J) = I : (a)^{\infty}$, the so-called saturation *of I by the principal ideal (a).*

(iv) *Taking residual classes commutes with fractions. Precisely, there is a natural ring isomorphism*

$$\overline{\mathfrak{S}}^{-1}(R/I) \simeq (\mathfrak{S}^{-1}R)/(\mathfrak{S}^{-1}I),$$

where $\overline{\mathfrak{S}}$ is the set of residues of the elements of $\mathfrak{S}$.

Proof. (i) The assertion is obvious. For the converse, suppose that $1 \in \mathfrak{S}^{-1}I$, say, $1 = a/s$, for some $a \in I$, $s \in \mathfrak{S}$. Then $ta \in \mathfrak{S}$ for some $t \in \mathfrak{S}$. If $\mathfrak{S}$ happens to be saturated then $a \in \mathfrak{S}$ as well.

(ii) Let $a/s \in J$; then $a/1 \in J$ also, hence $a \in I := \iota^{-1}(J)$ by definition. Thus, $a/s \in \mathfrak{S}^{-1}I$.

(iii) Let $a \in \bigcup_{s \in \mathfrak{S}} (I : s)$. Then $\iota(a) = a/1 \in \mathfrak{S}^{-1}I = J$, *i. e.*, $a \in \iota^{-1}(J)$. The reverse inclusion is similar.

The second assertion is now obvious.

(iv) Apply the universal property of fractions to the composite map $R \twoheadrightarrow R/I \to \overline{\mathfrak{S}}^{-1}(R/I)$ to get a map $\mathfrak{S}^{-1}R \to \overline{\mathfrak{S}}^{-1}(R/I)$. The rest is routine. □

One has seen that the hypothesis that $I \cap \mathfrak{S} = \emptyset$ is necessary in order that $\mathfrak{S}^{-1}I$ be a proper ideal of $\mathfrak{S}^{-1}R$. For prime and primary ideals, one can be more precise.

Proposition 2.1.4 (Behavior of primary ideals). *Let $P \subset R$ be a prime ideal such that $P \cap \mathfrak{S} = \emptyset$ and let $\mathfrak{P} \subset R$ stand for a P-primary ideal. Then:*
(i) $\mathfrak{P} = \iota^{-1}(\mathfrak{S}^{-1}\mathfrak{P})$.
(ii) *$\mathfrak{S}^{-1}P$ is a prime ideal of $\mathfrak{S}^{-1}R$ and $\mathfrak{S}^{-1}\mathfrak{P}$ is $\mathfrak{S}^{-1}P$-primary.*
(iii) *The first two items induce a bijection between the set of primary ideals of $\mathfrak{S}^{-1}R$ and the set of primary ideals of R having empty intersection with $\mathfrak{S}$.*

Proof. (i) Clearly, $\mathfrak{P} \subset \iota^{-1}(\mathfrak{S}^{-1}\mathfrak{P})$. Conversely, let

$$a \in \iota^{-1}(\mathfrak{S}^{-1}\mathfrak{P}) = \bigcup_{u \in \mathfrak{S}} (\mathfrak{P} : u),$$

where one has used (2.1.3.1). Then $au = 0$ for some $u \in \mathfrak{S}$. Since $u \notin P$ by assumption, then $a \in \mathfrak{P}$.

(ii) The proof that $\mathfrak{S}^{-1}P$ is a prime ideal of $\mathfrak{S}^{-1}R$ will be subsumed in the next argument, by assuming that $\mathfrak{P}$ is prime.

Let $(a/s)(b/t) \in \mathfrak{S}^{-1}\mathfrak{P}$ such that $b/t \notin \mathfrak{S}^{-1}\mathfrak{P}$. By item (i), $b \notin \mathfrak{P}$. Write $(a/s)(b/t) = c/u$, with $c \in \mathfrak{P}$ and $u \in \mathfrak{S}$. Then $abu - cst = v \in \mathfrak{a}$. Multiplying through by some $v \in \mathfrak{S}$ such that $av = 0$, one obtains $abuv = cstv \in \mathfrak{P}$. But $uv \notin P$ by assumption. Therefore, $ab \in \mathfrak{P}$ and since $b \notin \mathfrak{P}$ then $a \in P$, hence $a/s \in \mathfrak{S}^{-1}P$, as required.

(iii) The following diagram may be helpful:

$$\begin{array}{ccccccc} R & \xrightarrow{\iota} & \mathfrak{S}^{-1}R & \supset \mathfrak{Q} & \rightsquigarrow & \iota^{-1}(\mathfrak{Q}) & \subset R \\ \cup & & \cup & & & & \\ \mathfrak{P} & \rightsquigarrow & \mathfrak{S}^{-1}\mathfrak{P} & & & & \end{array}$$

The details are left to the reader. □

Most rings of fractions $\mathfrak{S}^{-1}R$ are infinitely generated as an R-algebra. An exception is the following.

Example 2.1.5. Let $a \in R$ be a nonnilpotent element of a ring and let $\mathfrak{S} \subset R$ denote the multiplicatively closed set of the powers of a. Then one has an isomorphism of R-algebras $R[t]/(1 - at) \simeq \mathfrak{S}^{-1}R$, where t is a variable over R mapping to $1/a$.

Here is a proof: first, clearly, $1 - at$ maps to zero. Conversely, let $f(t) = a_0 + a_1 t + \cdots + a_d t^d \in R[t]$ be such that $f(1/a) = 0$. Multiplying by a^d, yields the relation

$$a(a_0 a^{d-1} + \cdots + a_{d-2}a + a_{d-1}) = -a_d.$$

Set $b_{d-1} := a_0 a^{d-1} + \cdots + a_{d-2}a + a_{d-1}$, $a_d = -b_{d-1}a$. Repeat to get $a(a_0 a^{d-2} + \cdots + a_{d-2}) = b_{d-1} - a_{d-1}$ and set $b_{d-2} := a_0 a^{d-2} + \cdots + a_{d-2}$, so $a_{d-1} = b_{d-1} - b_{d-2}a$. Continuing this way, one eventually finds $\{b_0, b_1, \ldots, b_{d-1}\}$, with $a_i = b_i - b_{i-1}a$, for $i = 1, \ldots, d-1$, and $a_0 = b_0$, $a_d = -b_{d-1}a$.

Thus, setting $g(t) = b_0 + b_1 t + \cdots + b_{d-1}t^{d-1}$, it obtains $f(t) = g(t)(1 - at)$, as required. □

2.1.3 Local rings and symbolic powers

If $P \subset R$ is a prime ideal and $\mathfrak{S} = R\backslash P$, then the ring $\mathfrak{S}^{-1}R$ contains a unique maximal ideal, namely $\mathfrak{S}^{-1}P$.

Denote $\mathfrak{S}^{-1}R = R_P$, calling it the *local ring* of R at P. Similarly, given an ideal $I \subset R$, set $\mathfrak{S}^{-1}I = I_P$. In this notation, the unique maximal ideal of R_P is P_P and, in particular, the prime ideals of R_P correspond bijectively to those of R contained in P. The passage from R to R_P via the natural homomorphism $\iota : R \longrightarrow R_P$ is called *localization at* P. (The newcomer is recommended not to use this terminology for other rings of fractions.)

The field R_P/P_P is called the *residue field* of P and has a major role in the theory. Taking $\mathfrak{T} = R/P - \{\overline{0}\}$, this field is isomorphic to $\mathfrak{T}^{-1}(R/P)$, the field of fractions of R/P.

Motivated by this, one introduces the following terminology.

Definition 2.1.6. A ring is *local* if it has a unique maximal ideal.

Quite often such a ring is called *quasi-local*, while *local* is used in the case where R is moreover Noetherian (next chapter). Here, no such distinction in terminology will be made. A more relaxed condition requires that the ring have only finitely many maximal ideals, in which case it is called *semilocal*. Often a property of a local ring can be extended to a semilocal ring.

One great advantage of working with a Noetherian local ring R is that the notion of minimal number of generators of an ideal $I \subset R$ is well-defined in the sense that any set of generators with no superfluous elements has the same cardinality. Such a property is better understood in terms of passage to the associated $(R/\mathfrak{m})$-vector space $I/\mathfrak{m}I$, where $\mathfrak{m} \subset R$ denotes the unique maximal ideal of R. The main result in this regard is Lemma 2.5.24, which delivers the basic techniques to handle these rings.

One important application of localization at a prime ideal is given by the notion of symbolic powers (see Theorem 2.4.9 for its geometric impact). The definition is surprisingly simple.

Definition 2.1.7. Let R be a ring and let $P \subset R$ denote a prime ideal. Given an integer $s \geq 1$, the *sth symbolic power* of P is the inverse image in R of the ideal $P^s R_P$ via the structural map $R \to R_P$.

The notation is $P^{(s)}$. It has the following properties:

- $P^{(s)}$ contains the ordinary sth power of P
- $P^{(s)}$ is a P-primary ideal
- $P^{(s)}$ is the smallest P-primary ideal containing P^s.

The first of these properties is clear, while the last two follow immediately from Proposition 2.1.4(iii).

The notion is immediately generalizable to a radical ideal $I = P_1 \cap \cdots \cap P_r$, P_i a prime ideal, by letting $I^{(s)}$ designate the inverse image of $I^s\mathfrak{S}^{-1}R$ via the structural map $R \to \mathfrak{S}^{-1}R$, where $\mathfrak{S} = R \setminus \cup_i P_i$. Using further techniques to be introduced later, it is

possible to show that $I^{(s)} = \bigcap_i P_i^{(s)}$. Drawing on primary decompositions (Section 2.6), one can extend symbolic powers to any ideal having no *embedded associated primes* (Section 2.5.17).

In the terminology of primary components, $P^{(s)}$ is the primary component of P^s relative to the unique minimal prime of R/P^s, while R/P^s will have embedded primary components in general.

2.2 Integral ring extensions

Throughout this section, one focus on an inclusion of rings $R \subset S$, usually called a *ring extension*. The material classically evolved from number theory via rings of integers. Recall that a ring of integers is the integral closure of the ring $\mathbb{Z}$ in a finite field extension of $\mathbb{Q}$. The notion considered here is exactly the same, only in a more general environment.

2.2.1 Preliminaries

Let $R \subset S$ be a ring extension.

An element $b \in S$ is said to be *integral* over R if it is a root of a MONIC polynomial $f(X) \in R[X]$. Equivalently, b is integral over R if the kernel of the R-algebra map $R[X] \to S$, such that $X \mapsto b$, contains a monic polynomial. If this is the case, the resulting relation obtained by substituting for b is called an *equation of integral dependence*.

The following criterion of integrality opens the gates to the theory. One should note its similarity to a well-known test for algebraic elements in a field extension. To state it, one recurs to the notion of a module and of a set of generators (see Chapter 3). Although it may look abstruse to introduce this notion at this early point, think about the elegance and quickness it affords in the argument below.

Proposition 2.2.1. *Let $R \subset S$ be a ring extension and let $b \in S$. The following conditions are equivalent:*
(i) *b is integral over R.*
(ii) *The subring $R[b] \subset S$ is a finitely generated R-module.*
(iii) *$R[b]$ is contained in a subring $T \subset S$ which is a finitely generated R-module.*

Proof. (i) $\Rightarrow$ (ii) Say, $b^n + a_1 b^{n-1} + \cdots + a_0 = 0$, where $a_i \in R$. Clearly, then $b^n \in \sum_{i=0}^{n-1} Rb^i$, the latter meaning the R-linear combinations of the powers $1, b, \ldots, b^{n-1}$, *i. e.*, the R-submodule generated by them. By recurrence, multiplying both members of the above equation of integral dependence by b yields $b^m \in \sum_{i=0}^{n-1} Rb^i$ for every $m \geq 0$. This gives $R[b] = \sum_{i=0}^{n-1} Rb^i$, as stated.

(ii) $\Rightarrow$ (iii) Obvious.

(iii) ⇒ (i) Say, $T = \sum_{j=1}^{n} Rs_j$. Write the products bs_j in terms of these generators to get a homogeneous linear system

$$\begin{aligned}(b - a_{1,1})s_1 + a_{1,2}s_2 + \cdots + a_{1,n}s_n &= 0\\ a_{2,1}s_1 + (b - a_{2,2})s_2 + \cdots + a_{2,n}s_n &= 0\\ &\ddots\\ a_{n,1}s_1 + a_{n,2}s_2 + \cdots + (b - a_{n,n})s_n &= 0,\end{aligned} \tag{2.2.1.1}$$

for certain $a_{i,j} \in R$. This translates into a T-linear map $T^n \xrightarrow{\varphi} T^n$, where φ is the matrix of coefficients in (2.2.1.1). Since $\psi := (s_1 \dots s_n)^t$ is a solution of this system, one has a sequence of T-linear maps $T \xrightarrow{\psi} T^n \xrightarrow{\varphi} T^n$ such that $\varphi \circ \psi = 0$. Therefore, the rank of φ is at most $n - \operatorname{rank}(\psi)$ (see Definition 3.3.5 for the general notion of rank of matrices and maps between free modules).

But since $1 \in T = \sum_j Rs_j \subset I_1(\psi) \subset T$, where $I_1(\psi)$ denotes the ideal of T generated by the 1×1 minors of ψ, then ψ has rank at least (in fact, exactly) 1. Consequently, φ has rank $\leq n - 1$, hence $\det(\varphi) = 0$. Expanding $\det(\varphi)$ yields an equation of integral dependence for b. □

Remark 2.2.2. The above scheme to prove the implication (iii) ⇒ (i) is often called the "determinantal trick" of H. Prüfer, who first used it in [125]. The last implication in the proof is also a consequence of the classical cofactor relation

$$\operatorname{diag}(\Delta, \dots, \Delta) = C(\varphi) \cdot \varphi,$$

where $\Delta = \det(\varphi)$ and $C(\varphi)$ is the matrix of cofactors of φ. Multiplying both sides of this relation by $(s_1, \dots, s_n)^t$ yields $\Delta s_j = 0$, for every j. Then use again that the s's generate T and $1 \in T$ since T is a subring.

Definition 2.2.3. The extension $R \subset S$ is *integral*, or that S is *integral over* R, if every element of S is integral over R.

Some easy consequences are stated in the next proposition.

Proposition 2.2.4. *Let $R \subset S$ be a ring extension.*

(i) (Integral closure) *The set of elements of S integral over R form a subring, called the* integral closure *of R in S.*

(ii) (Transitivity of integrality) *If $R \subset T \subset S$ is an intermediate extension, then S is integral over R if and only if S is integral over T and T is integral over R. In particular, the integral closure of R in S is integrally closed.*

(iii) (Ring change) *For any ideal $J \subset S$, the induced homomorphism $R/J \cap R \to S/J$ is injective and, as such, is an integral extension.*

Proof. (i) It suffices to prove that if $s_1, s_2 \in S$ are integral over R then so are $s_1 + s_2$ and $s_1 s_2$. By Proposition 2.2.1 ((i) $\Rightarrow$ (ii)), the subring $R[s_1, s_2] = R[s_1][s_2]$ is a finitely generated R-module. Since $s_1 + s_2, s_1 s_2 \in R[s_1, s_2]$, Proposition 2.2.1 ((iii) $\Rightarrow$ (i)) applies.

(ii) The "only if" implication is obvious. Let then $s \in S$. Since s is integral over T, the T-module $T[s]$ is finitely generated by Proposition 2.2.1 ((i) $\Rightarrow$ (ii)). Let $b_1, \ldots, b_m \in T$ denote the coefficients in an equation of integral dependence of s over T. Adjoining these elements successively to R and using the assumption that T is integral over R, it follows again from Proposition 2.2.1 that the subring $R[b_1, \ldots, b_m]$ is a finitely generated R-module. Since s is actually integral over $R[b_1, \ldots, b_m]$, the ring $R[b_1, \ldots, b_m, s]$ is still a finitely generated R-module. But since $R[s] \subset R[b_1, \ldots, b_m, s]$, Proposition 2.2.1 ((iii) $\Rightarrow$ (i)) applies to conclude that s is integral over R.

(iii) Injectivity is old history, while integrality follows immediately since an equation of integral dependence over R yields one over $R/J \cap R$ by mapping to S/J. □

An integral domain is called *integrally closed* (or *normal*) if it coincides with its integral closure in its field of fractions.

Remark 2.2.5. Had one defined integrality for any ring homomorphism $\varphi : R \to S$ (not necessarily injective) to mean integrality of S over the image of R, one would have that, given an ideal $I \subset R$ then the induced ring map $R/I \to S/IS = S/\varphi(I)S$ is still integral in the sense explained. Note, however, that this map is injective if and only if $I = IS \cap R$.

2.2.2 The Cohen–Seidenberg theorems

Next is a fundamental property of integral extensions $R \subset S$ with respect to multiplicatively closed subsets $\mathfrak{S} \subset R$. This single theorem unifies all other related results, often proved separately (*cf.* [36] for the main source).

Theorem 2.2.6 (Unified Cohen–Seidenberg theorem). *Let $R \subset S$ be an integral extension, let $\mathfrak{S} \subset R$ be a multiplicatively closed subset and let $Q \subset S$ be a prime ideal not intersecting $\mathfrak{S}$. Then $Q \cap R$ does not intersect $\mathfrak{S}$ and the following conditions are equivalent:*

(i) *Q is maximal among the ideals of S not intersecting $\mathfrak{S}$.*

(ii) *$Q \cap R$ is maximal among the ideals of R not intersecting $\mathfrak{S}$.*

Proof. Clearly, $Q \cap R$ does not intersect $\mathfrak{S}$ since $(Q \cap R) \cap \mathfrak{S} = Q \cap \mathfrak{S}$.

(i) $\Rightarrow$ (ii) Assuming the contrary, let $Q \cap R \subsetneq I$, where $I \subset R$ is an ideal not intersecting $\mathfrak{S}$. Say, $a \in I \setminus (Q \cap R)$. Clearly, $a \notin Q$, so $Q \subset (Q, a)$ is a proper inclusion, hence $(Q, a) \cap \mathfrak{S} \neq \emptyset$ by assumption. Thus, let $\mathfrak{s} \in (Q, a) \cap \mathfrak{S}$, say, $\mathfrak{s} = q + ab$, with $q \in Q$ and $b \in S$. Since $R \subset S$ is integral, there is an equation of integral dependence for b over R

$$b^n + a_1 b^{n-1} + \cdots + a_{n-1} b + a_n = 0, \quad a_i \in R.$$

Multiplying out by a^n, yields an equation of integral dependence for ab over R. Taking in account the form of $\mathfrak{s}$, one can see that the element $c =: \mathfrak{s}^n + (a_1 a)\mathfrak{s}^{n-1} + \cdots + a_n a^n$ belongs to Q and, clearly, to R, hence $c \in Q \cap R \subset I$. On the other hand, c is of the form $\mathfrak{s}^n + a'a$, for a suitable $a' \in R$. Since $a \in I$ to start with, then $\mathfrak{s}^n \in I$. Since $\mathfrak{S}$ is multiplicatively closed, then $\mathfrak{s}^n \in S$. Therefore, $\mathfrak{s}^n \in I \cap \mathfrak{S}$, thus contradicting the assumption $I \cap \mathfrak{S} = \emptyset$.

(ii) $\Rightarrow$ (i) Assume to the contrary, namely, that there is an ideal $J \supsetneq Q$ in S such that $J \cap \mathfrak{S} = \emptyset$. Let $b \in J \setminus Q$. Since the induced injective homomorphism $\overline{R} = R/Q \cap R \hookrightarrow \overline{S} = S/Q$ is an integral extension as well (Proposition 2.2.4(iii)), one has an equation of integral dependence for $\overline{b}$ over $\overline{R} = R/Q \cap R$, say

$$\overline{b}^n + \overline{a}_1\overline{b}^{n-1} + \cdots + \overline{a}_{n-1}\overline{b} + \overline{a}_n = \overline{0}, \quad a_i \in R, \tag{2.2.6.1}$$

with n minimal possible. One then claims that $\overline{a}_n$ is a nonzero element of $\overline{R}$. For otherwise the product $\overline{b}(\overline{b}^{n-1} + \overline{a}_1\overline{b}^{n-2} + \cdots + \overline{a}_{n-1}) = -\overline{a}_n = \overline{0}$ and since $\overline{S}$ is a domain one must have $\overline{b}^{n-1} + \overline{a}_1\overline{b}^{n-2} + \cdots + \overline{a}_{n-1} = \overline{0}$, thus yielding an equation with smaller leading exponent.

Thus, $a_n \notin Q \cap R$. But, clearly $a_n \in J \cap R$ as follows from (2.2.6.1) and the assumption that $b \in J$. Therefore, by the main hypothesis, there must be some element $\mathfrak{s} \in \mathfrak{S}$ belonging to $J \cap R$ as well, thereby contradicting the assumption $J \cap \mathfrak{S} = \emptyset$. □

Remark 2.2.7. I learned the argument in the first implication above from the proof of [93, Theorem 44], although there it is used in a slightly different context.

Most known properties of integral extensions, generally known as the Cohen–Seidenberg theorems (though the priority is Krull's), follow at once from the above general theorem.

Corollary 2.2.8 ("Contraction of maximal ideals"). *Let $R \subset S$ be an integral extension. Then the contraction of a prime $Q \subset S$ to R is a maximal ideal if and only if it is maximal. In particular, in an integral extension $R \subset S$ of domains, S is a field if and only if R is a field.*

Proof. Take $S = \{1\}$ in Theorem 2.2.6. □

Corollary 2.2.9 ("Incomparability"). *Let $R \subset S$ be an integral extension and let $Q \subset J \subset S$ be ideals of S, of which Q is prime. If $Q \cap R = J \cap R$, then $Q = J$.*

Proof. Let $\mathfrak{S} = R \setminus (Q \cap R)$. Surely, $\mathfrak{S}$ is multiplicatively closed, $Q \cap R$ does not meet $\mathfrak{S}$ and is maximum among the ideals not meeting $\mathfrak{S}$. Clearly, $Q \cap \mathfrak{S} = (Q \cap R) \cap \mathfrak{S} = \emptyset$ and, similarly, $J \cap \mathfrak{S} = (J \cap R) \cap \mathfrak{S} = \emptyset$, since $J \cap R = Q \cap R$ by assumption. By Theorem 2.2.6, $Q = J$. □

Corollary 2.2.10 ("Lying over"). *Let $R \subset S$ be an integral extension and let $P \subset R$ be a prime ideal. Then there is a prime ideal $Q \subset S$ contracting to P.*

Proof. Let $\mathfrak{S} = R \setminus P$. Consider the set of the ideals of S not meeting $\mathfrak{S}$. This is a nonempty (because the zero ideal is a member) partially ordered set which is clearly inductive. Let Q be a maximal member therein. Arguing as in the proof of Proposition 1.1.5, one sees that Q is necessarily a prime ideal. Moreover, since $\mathfrak{S} = R \setminus P$, then $Q \cap R \subset P$. By Theorem 2.2.6 ((i) implies (ii)), the contraction $Q \cap R$ must be maximal among the ideals of R not meeting $\mathfrak{S}$. Thus, $P = Q \cap R$. □

Corollary 2.2.11 ("Going up"). *Let $R \subset S$ be an integral extension, let $P \subset P' \subset R$ be prime ideals and let $Q \subset S$ be a prime ideal contracting to P. Then there exists a prime ideal $Q' \subset S$ containing Q and contracting to P'.*

Proof. Since the extension $R/P \subset S/Q$ is integral, by Corollary 2.2.10 there is a prime of S/Q contracting to the prime P'/P of R/P. But any such prime is of the form Q'/Q, for a suitable prime $Q' \subset S$. It is now immediate to check that Q' is a solution of the problem. □

2.2.3 Integral closure of ideals

The subject was originally approached by H. Prüfer, later taken up by several authors, including Krull. One important source of problems is the theory of complete ideals in 2-dimensional regular local rings developed by O. Zariski in [169, Appendix 5], while a full update is in the book [150], parts of which were used in its essence in the following brief account.

Definition 2.2.12. Let R be a ring and $I \subset R$ an ideal. An element $a \in R$ is said to *integral over I* if it satisfies a polynomial $f(x) \in R[x]$ of the form

$$x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0,$$

for some $a_i \in I^i$, for all i.

The following is an analogue of Proposition 2.2.1.

Proposition 2.2.13. *Let R be a ring and $I \subset R$ an ideal. Given $a \in R$, the following are equivalent:*

(i) $a \in \tilde{I}$.

(ii) *There exists a finitely generated R-module M such that $a \in IM :_R M$ and such that $0 :_R M \subset \sqrt{0} :_R a$.*

Proof. (i) ⇒ (ii) Since an equation of integral dependence of a involves finitely many elements of I, it is clear that there exists a finitely generated subideal $J \subset I$ such that a is still integral over it. But an equation of integral dependence of a of degree n implies that $a^n \in (J^n, J^{n-1}, \ldots, Ja^{n-1}) = J(J,a)^{n-1}$. From this follows that $(J,a)^n \subset J(J,a)^{n-1}$,

hence

$$a(J,a)^{n-1} \subset (J,a)^n \subset J(J,a)^{n-1} \subset I(J,a)^{n-1}.$$

Setting $M := (J,a)^{n-1}$ is a solution of the problem, since if $b \in R$ kills M then in particular it kills a^{n-1}, hence $b \in \sqrt{0} :_R a$.

(ii) $\Rightarrow$ (i) Apply the same method as in the proof of Proposition 2.2.1, (iii) $\Rightarrow$ (i), to a finite set of generators of M, using the hypothesis $aM \subset IM$, obtaining a certain square matrix $\mathcal{A}$. Then use the idea in Remark 2.2.2 to derive $\det(\mathcal{A})M = 0$ and then apply the remaining hypothesis to get an equation of integral dependence of the form $(a\det(\mathcal{A}))^l = 0$ for some l. □

The set of all elements of R integral over I is called the *integral closure* (in R) of I, here denoted $\tilde{I}$. By extension, any intermediate ideal $I \subset J \subset \tilde{I}$ will be said to be integral over I.

Corollary 2.2.14. *The integral closure of an ideal is an ideal.*

Proof. If $a \in \tilde{I}$, the clearly $ba \in \tilde{I}$ (multiply an equation of integral dependence of a throught by b). Thus, it suffices to show that the sum of two integral a, b elements over I is integral over I. Let $n \geq m$ be the degrees of respective equations of integral dependence. Since again both equations involve but finitely many elements of I then, as in the proof of the proposition, one can take M to be $(J,a)^{n-1}$ and $(J,a)^{m-1}$, respectively. Since $(J,a)^{m-1} \subset (J,a)^{n-1}$, condition (i) of the proposition is satisfied for $a+b$ with $M = (J,a)^{n-1}$. □

Naturally, the ideal I is said to be integrally closed if $I = \tilde{I}$. The terminology *normal ideal* has a different meaning for ideals as for rings; it means that all powers of the ideal are integrally closed.

By a similar token, one can verify that, for any ideal $I \subset R$, its integral closure is an integrally closed ideal. In other words, $\widetilde{(\tilde{I})} = \tilde{I}$. As in Proposition 2.2.4 (ii), it suffices to prove transitivity.

Proposition 2.2.15. *Given ideals $I \subset I' \subset I'' \subset R$, then I'' is integral over I if and only if I' is integral over I and I'' is integral over I'.*

Proof. One direction is obvious. For the other direction, let $a \in I''$. As before, one reduces to the case where a is integral over a finitely generated subideal $J' \subset I'$. Say, $J' = (b_1, \ldots, b_m)$. Similarly, one can choose a finitely generated subideal $J \subset I$ such that every b_i is integral over it. Although one can choose an appropriate R-module satisfying condition (ii) of Proposition 2.2.13 in order to complete the proof, it may be more useful at this point to introduce the following criterion.

Claim 1 (Reduction criterion). An element $a \in R$ is integral over an ideal J if and only if there exists an integer $n \geq 1$ such that $(J,a)^n = J(J,a)^{n-1}$.

One direction has been shown in the proof of Proposition 2.2.13, as a consequence of an equation of integral dependence of degree n. The reverse implication is similar.

The condition in the above claim is expressed by saying that J is a *reduction* of (J, a).

Claim 2 (Transitivity of reductions). For any ideals $\mathfrak{a} \subset \mathfrak{b} \subset \mathfrak{c} \subset R$, if $\mathfrak{a}$ is a reduction of $\mathfrak{b}$ and $\mathfrak{b}$ is a reduction of $\mathfrak{c}$ then $\mathfrak{a}$ is a reduction of $\mathfrak{c}$.

Write $\mathfrak{a}\mathfrak{b}^n = \mathfrak{b}^{n+1}$ and $\mathfrak{b}\mathfrak{c}^m = \mathfrak{c}^{m+1}$. By iteration, one can see that $\mathfrak{c}^{m+n+1} = \mathfrak{b}^{n+1}\mathfrak{c}^m$, hence $\mathfrak{c}^{m+n+1} = \mathfrak{a}\mathfrak{b}^n\mathfrak{c}^m \subset \mathfrak{a}\mathfrak{c}^{m+n}$, as required.

Applying to the present situation, J is a reduction of (J, b_1) and by iteration yields that J is a reduction of (J, J'). By the same token, J' is a reduction of (J', a). Since J is also finitely generated, again by iteration, (J, J') is a reduction of (J, J', a). By transitivity, J is a reduction of (J, J', a) and, since $(J, a) \subset (J, J', a)$, then J is a reduction of (J, a). Thus, by the first claim, a is integral over J, hence over I, too. □

Remark 2.2.16. The notion of reduction came up above as a compact means to express properties of the integral closure. A more decisive role is given in Subsection 7.3.3.

Next are some basic properties of the integral closure, most of easy verification.

Properties 2.2.17. Let $I \subset R$ be an ideal.

(1) $\tilde{I} \subset \sqrt{I}$.
(2) Every radical (particularly, prime) ideal is integrally closed.
(3) (Contraction) If $R \subset S$ is a ring extension and $J \subset S$ is an integrally closed ideal then $J \cap R$ is integrally closed in R.
(4) (Fractions) If I is integrally closed in R, then $\mathfrak{S}^{-1}I$ is integrally closed in $\mathfrak{S}^{-1}R$.
(5) (Local nature) I is integrally closed in R if and only if I_P is integrally closed in R_P for every prime (resp., maximal) ideal $P \subset R$.
(6) (Modular nature) An element $a \in R$ belongs to $\tilde{I}$ if and only if for every minimal prime ideal $\wp$ of R, the residue of a in $R/\wp$ belongs to $\widetilde{(I, \wp)/\wp}$.

Of all the above properties, the one that deserves a more detailed scrutiny is (6). One implication is easy, namely, that $a \in \tilde{I}$ implies $(a, \wp)/\wp \in \widetilde{(I, \wp)/\wp}$. Since an arbitrary ring R may have infinitely many minimal primes, the converse is not constructive. In the case where R has only finitely many minimal prime ideals $\wp_1, \ldots, \wp_r$ (*e. g.*, as will be seen later, when R is Noetherian), then one proceeds as follows: for each $i = 1, \ldots, r$ choose a polynomial $p_i(x)$ of integral dependence for a over $R/\wp_i$. Evaluating at a, one gets $p_i(a) \in \wp_i$ for every i, hence $\prod_i p_i(a) \in \prod_i \wp_i \subset \bigcap_i \wp_i$. Therefore, a suitable power of this product is zero. Letting $p(x)$ be such that $p(a) = \prod_i p_i(a)$ then a suitable power of $p(x)$ gives integral dependence for a in R.

An ideal $I \subset R$ is said to be *normal* is all its powers are integrally closed. This notion can be translated into ring theoretic integral closeness, namely, one defines the *Rees algebra* of I to be the subring $\mathcal{R}_R(I) := R[It] \subset R[t]$, generated by the elements of the form $at, a \in I$. Then it can be seen that I is normal if and only if $R[It]$ is integrally

closed in $R[t]$. Rees algebras constitute a key construction both in ideal theory as in the problem of resolution of singularities in algebraic geometry; see Section 7.3.

2.3 Krull dimension and Noether normalization

The basic element of this part is a finite *chain* of prime ideals

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n. \tag{2.3.0.1}$$

The *length* of the chain (2.3.0.1) is the integer n. The next definition mimics somewhat the version of the dimension of a vector space by means of chains of subspaces. Yet, its impact is far greater allowing for introducing new invariants not found in the case of vector spaces.

Definition 2.3.1. The *height* of a prime ideal $P \subset R$ is the maximum of the lengths of chains of prime ideals whose top is P:

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = P.$$

One denotes this maximum by $\operatorname{ht}(P)$ or $\operatorname{ht} P$. A chain of primes as above is said to be *saturated* if no prime ideal can be properly inserted in the chain so as to increase its length. There is no offhand reason for $\operatorname{ht}(P)$ to be actually a (finite) number. There are two types of obstruction: first, in principle a given chain may not be extended to a (finite) saturated one; second, there may be saturated chains of ever increasing length. Later one will show that for certain rings—Noetherian rings—$\operatorname{ht}(P) < \infty$ for any prime, but this is by no means a trivial result.

An alternative terminology is often used: the *codimension* of P (denoted $\operatorname{cod} P$). This is a slight abuse inherited from the special case where $\operatorname{ht} P$ is a true codimension in the ambient ring R and will mainly be used in those cases.

By a similar token, one can introduce the following notion.

Definition 2.3.2. The (*Krull*) *dimension* of the ring R is the maximum of the heights of its prime ideals.

The dimension of R will be denoted $\dim R$. Like for height, there is even less chance that an arbitrary ring have finite Krull dimension, as prime ideals might turn out to admit ever increasing heights. There are even examples of Noetherian rings with infinite Krull dimension (see Example 2.5.9).

This notion can be extended to an arbitrary ideal $I \subset R$ by setting

$$\operatorname{ht} I := \min\{\operatorname{ht} P \mid P \supset I \text{ a prime ideal}\}.$$

Clearly, one may restrict to the minimal prime overideals of I in R—when R is Noetherian, these will be finitely many (Proposition 2.5.20).

2.3.1 Behavior in integral extensions

The following fundamental result follows immediately from the Krull/Cohen–Seidenberg theorems.

Corollary 2.3.3. *If $R \subset S$ is an integral extension, then* $\dim R = \dim S$.

Proof. The equality is to be interpreted in the sense that if one of the sides is infinite then so is the other. Given a chain of primes in S its contraction to R yields a chain of primes in R by Corollary 2.2.9. This shows that $\dim S \leq \dim R$. Conversely, given a chain of primes in R, by Corollary 2.2.10 and Corollary 2.2.11, one obtains a chain of primes in S contracting to the given chain. This shows that $\dim R \leq \dim S$. □

Remark 2.3.4. One notes that Corollary 2.2.9 can actually be applied to deduce that, in an integral extension $R \subset S$ one has $\mathrm{ht}(Q) \leq \mathrm{ht}(Q \cap R)$, for every prime $Q \subset S$. The reverse inequality fails in general because lifting "bottom-to-top" a chain of primes $P_0 \subsetneq \cdots \subsetneq P_n = Q \cap R$ of maximum length from R to be S may not give a chain of primes all contained in Q. If one can lift "top-to-bottom" then the reverse inequality holds—a result known as "going-down." Unfortunately, this result is somewhat restrictive and will not be specially discussed here.

2.3.2 Noether normalization and the dimension theorem

The following result is due to E. Noether (see History 2.8.3 below).

Theorem 2.3.5 (Noether normalization). *Let R denote a finitely generated algebra over a field k. Then there exists a finite algebraically independent subset $\mathfrak{A}$ of R such that R is integral over the k-subalgebra $k[\mathfrak{A}]$.*

Proof. The proof given here only works in the case where k has an infinite number of elements—the case where k is a finite field will be left to the curious reader.

Write $R = k[x_1, \ldots, x_n]$ and induct on n. If $n = 0$, take $\mathfrak{A} = \emptyset$. Assume that $n \geq 1$. If the set $\{x_1, \ldots, x_n\}$ is algebraically independent over k (*i. e.*, R is a polynomial ring over k), then one is done with $\mathfrak{A} = \{x_1, \ldots, x_n\}$. Thus, assume that $\{x_1, \ldots, x_n\}$ is algebraically dependent over k.

Take a nonzero polynomial F in the polynomial ring $k[X_1, \ldots, X_n]$ (note the capital X's) such that $F(x_1, \ldots, x_n) = 0$. One may assume that the term in X_n does not vanish.

Claim. Let $\mathfrak{a}_i = x_i - c_i x_n$, for $i = 1, \ldots, n-1$ and $c_i \in k$. Then, for suitable choice of the c_i's, R is integral over its subalgebra $k[\mathfrak{a}_1, \ldots, \mathfrak{a}_{n-1}]$.

Note that, by the inductive assumption, the content of the claim is all that is needed. Thus, one proceeds to prove the claim. Note that $x_i = \mathfrak{a}_i + c_i x_n$, so substituting upon $F(x_1, \ldots, x_n) = 0$ gives $F(\mathfrak{a}_1 + c_1 x_n, \ldots, \mathfrak{a}_{n-1} + c_{n-1} x_n, x_n) = 0$. Let $f(X_1, \ldots, X_n)$ denote

the term of F of highest degree in X_n. Then, expanding the left-side as a polynomial in x_n, the term of highest degree has the form $x_n^r f(c_1, \ldots, c_{n-1}, 1)$, for some integer $r \geq 1$. Therefore, since $f(c_1, \ldots, c_{n-1}, 1) \in k$, provided this coefficient does not vanish, one gets an equation of integral dependence of x_n over the subalgebra $k[\mathfrak{a}_1, \ldots, \mathfrak{a}_{n-1}]$, as required in the claim.

In order to make sure that $f(c_1, \ldots, c_{n-1}, 1) \neq 0$ for suitable choice of the c_j's is where the assumption that k is infinite comes in. Indeed, suppose that $f(c_1, \ldots, c_{n-1}, 1)$ vanishes for any choice of $(c_1, \ldots, c_{n-1}) \in k^{n-1}$. Thus, one is saying that the nonzero polynomial $g = f(X_1, \ldots, X_{n-1}, 1)$ in $n-1$ variables vanishes for every $(c_1, \ldots, c_{n-1}) \in k^{n-1}$, an infinite vector space. From this, one can derive the existence of a nonzero polynomial in one variable over the same k with an infinite set of roots, which is absurd. □

Remark 2.3.6. One observes that, in the notation of the theorem, R is a finitely generated *module* over $k[\mathfrak{A}]$ (see Section 3). This allows to bringing in typical module-theoretic questions, such as the rank, number of generators and the question as to when this module is free. An additional point is the scrambling of the originally given finite set of generators of R as a k-algebra to end up with a finite set of generators of R as a $k[\mathfrak{A}]$-algebra.

Next follows one of the basic theorems of finitely generated algebras over a field. Although possibly guessed by several mathematicians, its general version is attributed to E. Noether.

Theorem 2.3.7 (Noether dimension theorem). *If R is a finitely generated domain over a field k, then* $\operatorname{trdeg}_k(R) = \dim R$.

Proof. The inequality $\operatorname{trdeg}_k(R) \geq \dim R$ is easy: given an arbitrary chain of primes $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_m$ in R then $\operatorname{trdeg}_k R/P_i > \operatorname{trdeg}_k R/P_{i+1}$ for every $0 \leq i \leq m-1$, by Proposition 1.2.9. For the reverse inequality, using Theorem 2.3.5 and Corollary 2.3.3, one is reduced to the case of a polynomial ring $R = k[X_1, \ldots, X_n]$. Since $\{0\} \subset (X_1) \subset (X_1, X_2) \subset \cdots \subset (X_1, \ldots, X_n)$ is a chain of prime ideals, the inequality $\operatorname{trdeg}_k(R) \leq \dim R$ follows. □

One should observe that an analogous result holds for any finitely generated algebra over a field k in terms of its *minimal primes*, a subject to be approached in Section 2.5.2.

2.3.3 Complements to Noether's theorem

One reason Noether was busy with the normalization lemma in various forms is that she was looking at the finite behavior of the integral closure of a finitely generated k-domain. Here, one states two of these results without proof. The original source is of course Noether's own papers, as reproduced in a modern language in [168]. The

reader will note that the statements below involve the notion of field separability and a familiarization with finitely generated modules and their sets of generators.

Theorem 2.3.8 ([168, Chapter V, S. 4, Theorem 7]). *Let R be an integrally closed domain, with field of fractions K and let $F|K$ be a finite separable extension. If S is the integral closure of R in F, then there exists a K-vector basis $\{x_1, \dots, x_n\}$ of F such that S is contained in the R-module $\sum_i Rx_i$.*

Theorem 2.3.9 ([168, Chapter V, S. 4, Theorem 9]). *Let R be a finitely generated domain over a field k and let F be a finite field extension of the field of fractions of R. Then the integral closure of R in F is a finitely generated k-algebra and a finitely generated R-module.*

2.4 Nullstellensatz

Now one connects normalization with various forms of the celebrated *Nullstellensatz* (theorem of the zero locus) of Hilbert. The first result below appears as a lemma on [168]. Thereon, one refers to it as Zariski lemma, but since there are so many of these in various topics, one would better call it the Zariski theorem of zeros. It allows for an elegant approach amidst the fuzziness of the earlier geometric arguments.

Theorem 2.4.1 (Zariski Nullstellensatz). *Let R be a finitely generated algebra over a field k. If R is itself a field, then $R|k$ is an algebraic extension.*

Proof. By Theorem 2.3.5, R is integral over a polynomial ring $S \subset R$, hence S is a field by Corollary 2.2.8 and the intermediate field extension $R|S$ is algebraic. In particular, $\dim S = 0$. Then, by Theorem 2.3.7, S is a field with transcendence degree 0 over k, *i. e.*, $S|k$ is an algebraic extension. Therefore, so is $R|k$ as a composite of algebraic extensions. □

The following consequence is often called the theorem of zeros of O. Goldman.

Theorem 2.4.2 (Goldman Nullstellensatz). *Let $R \subset S$ be an extension of finitely generated algebras over a field k. Then the contraction to R of any maximal ideal of S is a maximal ideal.*

Proof. Let $\mathfrak{m} \subset S$ be a maximal ideal and let $\mathfrak{n} := \mathfrak{m} \cap R$ denote its contraction to R. Note the induced inclusions $k \subset R/\mathfrak{n} \subset S/\mathfrak{m}$, with $S/\mathfrak{m}$ a finitely generated k-algebra and a field. By Theorem 2.4.1, the field extension $(S/\mathfrak{m})|k$ is algebraic, *i. e.*, $S/\mathfrak{m}$ has finite vector dimension over k. Therefore, so does its vector subspace $R/\mathfrak{n}$. Then by Theorem 2.3.7, as a finitely generated k-algebra it has Krull dimension 0, hence must be a field. □

An immediate consequence of Goldman's approach is the following result, which gives the generators structure of a maximal ideal in a polynomial ring over a field.

Theorem 2.4.3 (Structure of maximal ideals). *An ideal of the polynomial ring $k[X_1, \dots, X_n]$ is maximal if and only if it can be generated by n polynomials of the form*

$$f_1 = f_1(X_1), \quad f_2 = f_2(X_1, X_2), \quad \dots, \quad f_n = f_n(X_1, \dots, X_n),$$

where for every $1 \leq i \leq n$, the subideal $(f_1, \dots, f_i)$ is a prime ideal in the subring $k[X_1, \dots, X_i]$.

Proof. The "if" implication, by induction on n, is left to the reader.

Conversely, assume that $\mathfrak{m} \subset k[X_1, \dots, X_n]$ is a maximal ideal and induct on n once more. One could start from $n = 0$, where $\mathfrak{m} = \{0\}$ is generated by the empty set. But let us be brave and start from $n = 1$. Then $\mathfrak{m}$ is a principal ideal generated by an irreducible polynomial, so one is done here.

Thus, assume that $n \geq 2$. By Theorem 2.4.2, the contraction $\mathfrak{n} = \mathfrak{m} \cap k[X_1, \dots, X_{n-1}]$ is a maximal ideal. By the inductive hypothesis, $\mathfrak{n}$ has the stated shape of generators in $n - 1$ variables. Set $K := k[X_1, \dots, X_{n-1}]/\mathfrak{n}$, which is a field, and consider the principal ideal domain $K[X_1]$. The image of $\mathfrak{m}$ in this ring is still a maximal ideal, so must be generated by an irreducible element that lifts to a polynomial $f_n \in \mathfrak{m}$. This additional element completes the desired set of generators of $\mathfrak{m}$. □

Remark 2.4.4.

(i) Note that, in particular, if k is algebraically closed then

$$\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n),$$

for certain $a_i \in k$. To see this, one can start from the leftmost generator and see that it has the form $X_1 - a_1$, hence $k[X_1]/(X_1 - a_1) \simeq k$, and so forth.
Of course this information could have been lifted directly from Theorem 2.4.1.

(ii) The set of generators of a maximal ideal as in the above result is a special strong case of a more general notion of a regular sequence introduced earlier, which plays a central role in more advanced topics of the theory (see Section 5.3).

To go on toward the classical Nullstellensatz proved by Hilbert, one observes that it lies at the core of the following simple observation: letting $\mathfrak{m} \subset k[X_1, \dots, X_n]$ be a maximal ideal, write

$$K := k(x_1, \dots, x_n) = k[x_1, \dots, x_n] = k[X_1, \dots, X_n]/\mathfrak{m},$$

where x_i is the residue of X_i modulo $\mathfrak{m}$. Then, for every $g \in \mathfrak{m}$ one has $g(x_1, \dots, x_n) = 0$. That is to say, every element of $\mathfrak{m}$ vanishes at the n-tuple $(x_1, \dots, x_n) \in K^n$. Then, to get the full language of the Nullstellensatz, one just has to introduce a new terminology, where such n-tuples are called *points* (or *zeros*) of the *algebraic variety* of the ideal $\mathfrak{m}$.

In addition, since the elements x_is are algebraic over k, K is contained in an algebraic closure of k. This is to be kept in mind as a fundamental hypothesis regarding points of a variety.

Definition 2.4.5. Let $\mathfrak{E} \subset k[X_1, \dots, X_n]$ denote a subset and let K denote the algebraic closure of the field k. The *algebraic variety* (or simply, the *variety*) of $\mathfrak{E}$ is the collection of all n-tuples $(a_1, \dots, a_n) \in K^n$ such that $g(a_1, \dots, a_n) = 0$ for every $g \in \mathfrak{E}$.

Note that the variety of a set $\mathfrak{E}$ is the same as the variety of the ideal generated by $\mathfrak{E}$. Therefore, one usually talks about varieties of ideals instead.

The following result is often called the *Weak Nullstellensatz*, but here one adopts an ad hoc terminology in order to avoid incurring in a historic distortion.

Theorem 2.4.6 (Hilbert Nullstellensatz, first form). *Let $I \subset k[X_1, \dots, X_n]$ denote an ideal and let K denote the algebraic closure of the field k. Then the variety of I is nonempty if (and only if) I is a proper ideal.*

Proof. The "only if" implication is obvious. Conversely, if I is a proper ideal it is contained in some maximal ideal. Therefore, one can assume at the outset that I is a maximal ideal, say, $I = \mathfrak{m}$ for visual emphasis. Writing $k[x_1, \dots, x_n] = k[X_1, \dots, X_n]/\mathfrak{m}$, Theorem 2.4.1 implies that the n-tuple $(x_1, \dots, x_n)$ belongs to K^n and is clearly a point of the variety of $\mathfrak{m}$. □

From this, one gets the full form of the Nullstellensatz as devised by Hilbert. The usual proof uses the so-called Rabinowitsch trick, a simple result related to the construction of rings of fractions (Section 2.1).

Theorem 2.4.7 (Hilbert Nullstellensatz, strong form). *Let $I \subset k[X_1, \dots, X_n]$ denote a an ideal and let K denote the algebraic closure of the field k. Then the set of elements vanishing at all points of the variety of I is the radical of I.*

Proof. Set $V(I) \subset K^n$ for the variety of I. It is an easy exercise to see that if $g \in \sqrt{I}$ and $(a_1, \dots, a_n) \in V(I)$ then $g(a_1, \dots, a_n) = 0$. Conversely, let $g \in k[X_1, \dots, X_n]$ vanish on the points of $V(I)$. Introduce a new variable Y over $k[X_1, \dots, X_n]$ and consider the ideal $J := (I, 1 - Yg)$ of the polynomial ring $k[X_1, \dots, X_n, Y]$.

Claim. $V(J) = \emptyset$ (in K^{n+1}).

Indeed, let $p = (a_1, \dots, a_n, b) \in V(J)$. Then any element of I in particular vanishes at p, which means that $(a_1, \dots, a_n) \in K^n$ is a point of $V(I)$. By hypothesis, g vanishes at the latter, hence Yg vanishes at p. But then $1 - Yg$ cannot vanish at p, which is a contradiction.

By Theorem 2.4.6, one has $1 \in J$. Say,

$$1 = h_1 f_1 + \cdots + h_m f_m + h(1 - Yg), \tag{2.4.7.1}$$

for suitable $f_1, \dots, f_m \in I$ and $h_1, \dots, h_m, h \in k[X_1, \dots, X_n, Y]$.

One may clearly assume that $g \neq 0$. Now consider the $k[X_1, \dots, X_n]$-algebra homomorphism

$$k[X_1, \dots, X_n, Y] = k[X_1, \dots, X_n][Y] \longrightarrow k[X_1, \dots, X_n][1/g] \subset k(X_1, \dots, X_n),$$

mapping $Y \mapsto 1/g$. Applying this homomorphism to both sides of (2.4.7.1) and setting $\mathbf{X} = \{X_1, \ldots, X_n\}$ for simplicity, one finds

$$1 = h_1(\mathbf{X}, 1/g) f_1(\mathbf{X}) + \cdots + h_m(\mathbf{X}, 1/g) f_m(\mathbf{X}). \tag{2.4.7.2}$$

Note that in (2.4.7.2) there are only finitely many denominators (powers of g). Clearing denominators by multiplying through by a sufficiently high power g^r yields $g^r \in I$, hence $g \in \sqrt{I}$, as required. □

Remark 2.4.8. The variety of an ideal is only well-defined when one fixes the extension $K|k$, where the smaller field k is the field of coefficients of the polynomials—often called the *ground* field—and the larger field K is the field of coordinates of the points. In the above theorems, one assumed that K is the algebraic closure of k, but everything goes through as well by just assuming that K is an algebraically closed field containing k. In any case, in the latter situation, K already contains an isomorphic copy $\overline{k}$ of the algebraic closure of k. It can be shown that the points of the variety in $\overline{k}^n$ (so-called *algebraic points*) already determine the variety over K.

One closes this section with yet another famous lemma by Zariski.

Given a prime ideal $P \subset k[X_1, \ldots, X_n]$, by collecting the result of Theorem 2.4.7 and the details of Remark 2.4.4 (i), one reads: if a polynomial vanishes at all points of the variety defined by P then it belongs to P (in geometric language: it vanishes on the *generic point* of the variety). Algebraically, it translates into the property that P is the intersection of the maximal ideals containing it:

$$P = \bigcap_{\mathfrak{m} \supset P} \mathfrak{m}.$$

Of course, the family of these maximal ideals is infinite, unless P itself is a maximal ideal. This formulation is actually equivalent to Hilbert's theorem, at least in the prime ideal case.

Zariski generalized this as follows: he first introduced a topology on the affine space over k (called the *Zariski topology*) where the closed sets are the algebraic varieties. Thus, he had a notion of density. On the other hand, following the classical Italian school of algebraic geometry, he was aware that there are functions well-defined on the variety which are not necessarily polynomials. Then he asked: if such a function vanishes to order $\geq s > 0$ at a dense subset of (closed) points of the variety, is it the case that it already vanishes at the generic point to the same order?

He proved that this is indeed so. The algebraic version of this result is as follows.

Theorem 2.4.9 (Zariski main lemma on holomorphic functions). *Let P denote a prime ideal in the polynomial ring $k[X_1, \ldots, X_n]$ over a field and let $\mathcal{N}$ stand for a dense set of maximal ideals containing P, e. g., $\mathcal{N}$ could be the whole set of maximal ideals containing P. Then, for any integer $s \geq 1$, one has*

$$P^{(s)} = \bigcap_{\mathfrak{m}\in\mathcal{N}} \mathfrak{m}^s,$$

where $P^{(s)}$ denotes the sth symbolic power of P (cf. Section 2.1.7).

The original proof of Zariski is quite involved. Simpler proofs have been given since ([53]). Both Zariski and Nagata became interested in symbolic powers from the geometric point of view. They in fact proved a result that makes the computation of these ideals somewhat effective, in terms of vanishing partial derivatives. For a totally effective method, see [143].

Beyond the geometric interest, symbolic powers had historically a remarkable overture through Krull's approach to the proof of the principal ideal theorem (see the proof of Theorem 2.5.25).

2.5 Dimension theory I

2.5.1 Noetherian and Artinian rings

2.5.1.1 Noetherian rings

The starting principle of this part is as follows.

Lemma 2.5.1. *The following conditions for a ring R are equivalent:*

(i) (Finite basis) *Every ideal of R is finitely generated.*

(ii) (Ascending chain condition) *Every chain of ideals $I_1 \subset I_2 \subset \cdots$ is stationary, i. e., there exists an index i such that $I_i = I_{i+1} = \cdots$.*

(iii) (Maximum condition) *Every nonempty family of ideals of R has a maximal element (i. e., an ideal belonging to the family not contained properly in any other ideal in the family).*

Proof. (i) $\Rightarrow$ (ii) Let $I_1 \subset I_2 \subset \cdots$ be given. The set union $I := \bigcup_i I_i$ is easily seen to be an ideal of R. By assumption, $I = (a_1, \ldots, a_m)$ for certain $a_i \in R$. Forcefully then, there is an index i such that I_i contains the set $\{a_1, \ldots, a_m\}$. Therefore, $I \subset I_i$, hence clearly $I_i = I_{i+1} = \cdots$.

(ii) $\Rightarrow$ (iii) Let there be given a nonempty family $\mathcal{F}$ of ideal s of R. Pick some I belonging to $\mathcal{F}$. If I is a maximal element in $\mathcal{F}$, done. Otherwise, choose I_2 in $\mathcal{F}$ properly containing $I_1 := I$. Proceeding this way, one finds a sequence of proper inclusions $I_1 \subset I_2 \subset \cdots$. By assumption, this sequence stabilizes, say, at index $i \geq 1$. Then I_i is a maximal element in $\mathcal{F}$.

(iii) $\Rightarrow$ (i) Let $I \subset R$ be an ideal. Consider the family $\mathcal{F}$ of finitely generated ideals of R contained in I. Clearly, $\mathcal{F}$ is nonempty since, *e. g.*, the zero ideal (generated by the empty set) belongs to it. By assumption, $\mathcal{F}$ has a maximal element, say, $J \subset I$. Claim: $J = I$. For let $b \in I$ be an arbitrary element. Then the enlarged ideal (J, b) still belongs to $\mathcal{F}$. But J is maximal, hence $(J, b) = J$, *i. e.*, $b \in J$. □

Definition 2.5.2. A ring R satisfying the equivalent conditions of Lemma 2.5.1 is called *Noetherian* (after Emmy Noether).

The equivalence of (i) and (ii) was established by Noether ("Noethersche Teilerkettensatz") inspired by a previous idea of Dedekind that used chains of ideals, while condition (iii) was first noted by E. Artin. Krull kept the terminology O-Ring (O for "Ober," referring to an ideal being an "overideal" of another along the chain) even in the second edition of his book (prefaced by him in 1967).

The maximum condition devised by Artin is very useful to obtaining special properties of a Noetherian ring. Here is one example.

Proposition 2.5.3. *In a Noetherian ring R, every ideal contains a product of finitely many prime ideals. In particular, $\{0\}$ is the intersection of finitely many prime ideals.*

Proof. Suppose that the family $\mathcal{F}$ of ideals of R not containing any product of finitely many prime ideals is nonempty. Let $I \subset R$ be a maximal element of $\mathcal{F}$. In particular, I is not a prime ideal, hence there exist ideals J_1, J_2 of R, each properly containing I, such that $J_1 J_2 \subset I$. Since I is a maximal element of $\mathcal{F}$, neither J_1 nor J_2 belongs to $\mathcal{F}$. Therefore, each of these ideals contains a product of finitely many prime ideals and so does I. This is a contradiction. □

The above proof is taken from [37, Proof of Theorem 1] although it is quite possible that it already appears among E. Noether's papers.

The main source of examples of Noetherian rings comes from the next fundamental result, originally due to Hilbert ([72, Theorem I]) in the case where the coefficient ring is a field and for homogeneous ideals.

Theorem 2.5.4 (Hilbert basis theorem). *Let R be a Noetherian ring. Then the polynomial ring $R[X]$ is Noetherian.*

Proof. Suppose $\mathfrak{a} \subset R[X]$ is a nonfinitely generated ideal. Then by recursion (using the axiom of choice or a little less) there is an infinitely countable set $\{f_1, f_2, \ldots\} \subset \mathfrak{a}$ of polynomials such that if $\mathfrak{b}_n$ is the ideal generated by $f_1, \ldots, f_{n-1}$ then $f_n \in \mathfrak{a} \setminus \mathfrak{b}_n$ is of minimal degree. It is clear that $\{\deg(f_1), \deg(f_2), \ldots\}$ is a nondecreasing sequence of nonnegative integers. Let a_n denote the leading coefficient of f_n and let $\mathfrak{b}$ be the ideal in R generated by $a_1, a_2, \ldots$. Since R is Noetherian, the chain of ideals $(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \ldots$ is stationary. Thus $\mathfrak{b} = (a_1, \ldots, a_{N-1})$ for some integer N. So, in particular, $a_N = \sum_{i<N} u_i a_i$, for certain $u_i \in R$.

Now, the polynomial $g = \sum_{i<N} u_i X^{\deg(f_N)-\deg(f_i)} f_i$, whose leading term is equal to that of f_N, belongs to $\mathfrak{b}_N$. However, $f_N \notin \mathfrak{b}_N$, which means that $f_N - g \in \mathfrak{a} \setminus \mathfrak{b}_N$ has degree less than f_N, contradicting the minimality. □

From the aesthetic point of view, the proof is slightly imbalanced since the hypothesis uses condition (i) of Lemma 2.5.1, while the ultimate contradiction invokes condition (ii) of that lemma. Additional discussion on this proof is given in History 2.8.5.

There exist many other proofs, often in the search of a shortest possible argument. Some of these are suggested in the exercises.

Corollary 2.5.5. *Let R be a Noetherian ring. Then every finitely generated R-algebra is Noetherian.*

The proof is left to the reader.

2.5.1.2 Special results for Noetherian rings

Next are some excerpts of the second classical period of Noetherian rings. Although they will have no direct impact in parts of the book, the proofs are masterpieces worth recording here.

Theorem 2.5.6 (I. S. Cohen, 1950). *If every prime ideal of the ring A is finitely generated then A is Noetherian.*

Proof. If there is some nonfinitely generated ideal then the family of such ideals is nonempty and is easily seen to be inductive. Let P be a maximal element of this family.

One claims that P is a prime ideal. Indeed, suppose there are $a, b \in A \setminus P$ such that $ab \in P$. In particular, P is properly contained in the ideal (P, a), hence by the maximality of P, the latter ideal is finitely generated. Clearly, one may choose a set of generators of (P, a) of the form $x_1 + b_1 a, \ldots, x_n + b_n a$, with $x_i \in P$, $b_i \in A$. On the other hand, the quotient $P : a$ is also finitely generated since $b \in (P : a) \setminus P$. However, at is easy to see, $P = (x_1, \ldots, x_n, a(P : a))$, so P is finitely generated, which gives a contradiction.

By the main hypothesis of the statement, P is finitely generated and this repeated contradiction shows that there could not be any nonfinitely generated ideal to start with. □

The second result was proved simultaneously, but independently, by P. Eakin ([48]) and M. Nagata ([113]). About 33 years later, Nagata gave a new proof ([114]). Quite recently, a more encompassing result has been given by P. Jothilingam ([89]) The assertion of the theorem involves the notion of a (finitely generated) module, as well as the concept of integral extension, for which one refers to Chapter 3 and to Section 2.2, respectively. The proof below is the first argument given by Nagata, which still looks the clearest, if not the shortest.

Theorem 2.5.7 (Eakin–Nagata). *Let A be a subring of a Noetherian ring R. If R is finitely generated as A-module, then A is Noetherian.*

Proof. The argument is divided in several reduction steps. As a natural start, one wishes to induct on the number of generators of R as an A-module. The problem is that by writing $R = Ab_1 + \cdots + Ab_m$ as a finitely generated A-module, for certain $b_i \in R$, an intermediate submodule such as $Ab_1 + \cdots + Ab_{m-1}$ is Noetherian (as a submodule of a Noetherian ought to be), but has no structure of a ring. To fix it, one

takes the A-subalgebra $A[b_1, \dots, b_{m-1}]$. Clearly, the latter is still finitely generated as an A-module. With this, one is reduced to the following.

Step 1. One may assume that $R = A[b]$.

Step 2. One may assume that $A/I \cap A$ is Noetherian for any nonzero ideal $I \subset R$.

Indeed, let $I \subset R$ be a nonzero ideal. Pick a nonzero element $a \in I$ and pass to $R/(a)$. If the latter ring is Noetherian, $I/(a)$ is a finitely generated ideal thereof, hence so is I by lifting a finite set of generators of $I/(a)$ and adding a.

Step 3. If B is a subring of a Noetherian ring R which is a free B-module, then B is Noetherian.

In fact, for any ideal $I \subset B$, freeness implies that $IR \cap B = I$, hence a finite set of generators of IR gives a finite set of generators of I.

Step 4. There exists $a_0 \in A$ such that $a_0 b$ is integral over A.

Recall the generator b from step 1. Let $a_0 b^n + a_1 b^{n-1} + \cdots + a_{n-1} b + a_n = 0$ be an equation of lowest possible degree satisfied by b over A—such an equation exists due to the finite generation of R over A, which implies that the set of powers of b must be linearly dependent over A. Multiplying through by a_0^n yields an equation of integral dependence for $a_0 b$ over A.

In particular, $A[a_0 b]$ is free as A-module, so it would suffice by step 3 to show that this submodule is Noetherian. In any case, rewriting an equation of integral dependence of $a_0 b$ over A in the form $a_0 b((a_0 b)^{n-1} + \cdots + a_0^{n-1} a_{n-1}) = -a_0^n a_n \in A$ and telescoping in, one may assume that there is an element $a \in A$ such that $a.a_0^n b^n \in A$ for some n. Therefore, consider the saturated quotient $J := A :_A (b)^\infty$, an ideal both of A as of R. Thus, since R is finitely generated over A, if a_0 is not nilpotent, then $J \neq 0$.

Let $P \subset A$ be a prime ideal.

Step 5. Suppose a_0 not nilpotent and $P \cap J = \{0\}$.

Since J is also an R-ideal, one has $JR \cap A = J$. Since $J \neq \{0\}$, then A/J is Noetherian by step 2. In particular, the ideal $(P, J)/J \subset A/J$ is finitely generated. But $(P, J)/J \simeq P/P \cap J = P$. Since P is an arbitrary prime ideal of A, it follows from Theorem 2.5.6 that A is Noetherian.

Step 6. Suppose a_0 not nilpotent and $P \cap J \neq \{0\}$.

Let $Q \in R$ be a prime ideal contracting to P (Proposition 2.2.10). Then $PR \cap A \subset Q \cap A = P$, hence $PR \cap A = P$. Pick $0 \neq a \in P \cap J$. By definition of J, one has $ab^n \in A$ for all n. Since the powers of b generate R over A, the entire R-ideal aR is contained in A, hence is contained in $P = PR \cap A$. Now, one has an induced ring inclusion $A/aR \hookrightarrow R/aR$, with A/aR Noetherian and $aR \neq \{0\}$. By step 2, A/aR is Noetherian, so P/aR is finitely generated and, therefore, P is finitely generated and one concludes likewise above.

Step 7. Suppose that a_0 is nilpotent.

Changing to a suitable power of a_0 and renaming, one may assume that $a_0^2 = 0$. Set $I_0 := a_0 R \cap A$. Then A/I_0 is Noetherian by step 2 and I_0 is nilpotent, hence $I_0 \subset P$. Thus, P/I_0 is a finitely generated ideal. Moreover, $I_0 a_0 \subset a_0^2 R = \{0\}$, hence $a_0 R$ is a module over the ring A/I_0. Clearly, it is finitely generated over A/I_0, hence is a Noetherian module (here one needs Theorem 3.1.2) as an A/I_0-module. Since the canonical

map $A \twoheadrightarrow A/I_0$ makes A/I_0 finitely generated over A, then a_0R is a Noetherian module as an A-module. Therefore, its submodule I_0 is a finitely generated A-module. Since P/I_0 is finitely generated, so is P and one concludes as above. □

The following local–global criterion of Noetherianess was proved in [112, Appendix A.1].

Theorem 2.5.8 (Nagata Noetherian criterion). *Let R be a ring such that $R_{\mathfrak{m}}$ is Noetherian for every maximal ideal $\mathfrak{m}$ and $R/(a)$ is semilocal for every nonzero $a \in R$. Then R is Noetherian.*

Proof. Let $0 \neq I \subset R$ be an ideal. By assumption, the ring R/I is semilocal. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ be the finitely many maximal ideal of R containing I. Since the finitely many localizations $R_{\mathfrak{m}_i}$ are Noetherian by hypothesis, there is a common finite subset $\mathbf{a} = \{a_1, \ldots, a_s\} \subset I$ generating $I_{\mathfrak{m}_i}$ for $1 \leq i \leq r$. On the other hand, since $I_{\mathfrak{m}} = R_{\mathfrak{m}}$ for all $\mathfrak{m} \neq \mathfrak{m}_i$, $1 \leq i \leq r$, there is a finite subset $\mathbf{b} = \{b_1, \ldots, b_t\} \subset I$ such that $\mathbf{b}_{\mathfrak{m}} = R_{\mathfrak{m}}$ for all $\mathfrak{m} \neq \mathfrak{m}_i$, $1 \leq i \leq r$. Then $\{\mathbf{a}, \mathbf{b}\} \subset I$ generates I locally at every maximal ideal of R, hence generates I by an easy local-global principle of localization, namely, an R-module vanishes if and only if it vanishes locally at every maximal ideal of R. □

Nagata used this criterion to give an example of a Noetherian ring with infinite Krull dimension. This happens when the heights of prime ideals increase indefinitely.

Example 2.5.9. Let $S = k[x_1, x_2, \ldots]$ stand for a polynomial ring in countably many variables over a field k. Let $\{m_i \mid i = 1, 2, \ldots\}$ be an infinite sequence of positive natural number satisfying $m_{i+1} - m_i > m_i - m_{i-1}$ for all i. For every i, consider the prime ideal $\wp_i := (x_j | m_i \leq j < m_{i+1})$, which has height $m_{i+1} - m_i$. Set $\mathfrak{S} := \bigcap_i (S \setminus \wp_i)$, a multiplicative set. The desired ring is the ring of fractions $\mathfrak{S}^{-1}S$. It is Noetherian as an application of the above criterion, but the heights of primes increase indefinitely.

2.5.1.3 Artinian rings

Coming back to the last two conditions in Lemma 2.5.1, there is a sort of dual statement.

Lemma 2.5.10. *The following conditions for a ring R are equivalent:*

(i) (Descending chain condition) *Every chain of ideals $I_1 \supset I_2 \supset \cdots$ is stationary, i. e., there exists an index i such that $I_i = I_{i+1} = \cdots$.*

(iii) (Minimum condition) *Every nonempty family of ideals of R has a minimal element (i. e., an ideal belonging to the family not containing properly any other ideal in the family).*

The verification of this equivalence is left to the reader.

Definition 2.5.11. A ring R is called *Artinian* or an *Artin ring* (after Emil Artin) if it satisfies the above equivalent conditions.

The basic theory of Artin rings is a lot more involved than the Noetherian counterpart. Here are some of its "strange" basic properties.

Proposition 2.5.12. *Let R be an Artin ring. Then:*
(1) *If R is a domain, then it must be a field.*
(2) *Every prime ideal of R is maximal.*
(3) *If R is a local ring, then every nonunit is nilpotent.*
(4) *The annihilator of a proper (i. e., nonzero) minimal ideal of R is a prime ideal.*
(5) *Any ideal of R is a (finite) product of prime ideals.*
(6) *The set of maximal (resp., prime) ideals of an Artin ring is finite.*

Proof. (1) Let $0 \neq a \in R$. Then the descending chain $(a) \supset (a^2) \supset \cdots$ stabilizes. Say, $(a^n) \subset (a^{n+1})$. Then $a^n = a^{n+1}b$, for some $b \in B$. Cancelling a^n yields $ab = 1$, hence a is a unit.

(2) For any ideal $I \subset R$, the ring R/I is again Artinian as is easily verified. In particular, if $P \subset R$ is a prime ideal then R/P is a field by (1), hence P is a maximal ideal.

(3) Recall that R has a unique maximal ideal $\mathfrak{m}$. Let $a \in R$ be a nonunit, *i. e.*, $a \in \mathfrak{m}$. Consider again a stable value (a^n) of the descending chain $(a) \supset (a^2) \supset \cdots$. As in the proof of (1), one gets $a^n(ab - 1) = 0$, for some $b \in R$. But $ab - 1 \notin \mathfrak{m}$ since $a \in \mathfrak{m}$, *i. e.*, $ab - 1$ is a unit. It follows that $a^n = 0$.

(4) Let $I \subset R$ be a proper minimal ideal and let $\mathfrak{a} := 0 : I$ denote its annihilator. Let $c, d \in R$ such that $cd \in \mathfrak{a}$. If neither $c \in \mathfrak{a}$ nor $d \in \mathfrak{a}$ then both cI and dI are nonzero deals contained in I. By minimality, one must have $cI = I = dI$. Multiplying through by d, yields $cdI = dI = I \neq 0$. Therefore, $cd \notin \mathfrak{a}$—a contradiction.

(5) If $I \subset R$ is an ideal, then R/I is again Artinian, as one easily sees. Therefore, one can assume that $I = \{0\}$.

While showing that $\{0\}$ is a product of prime ideals in a Noetherian ring derives easily from the maximum condition, a dual argument using the minimum condition is much less obvious. The following argument is due to I. Cohen ([37, Proof of Theorem 1]): consider the family of ideals of R each of which is a product of finitely many prime ideals. By the axiom of choice, R admits at least one maximal ideal, hence this family is nonempty. Let J denote a minimal element in this family. Claim: $J = \{0\}$. Supposing otherwise, then $1 \notin 0 : J$, hence the family of ideals properly containing the annihilator $0 : J$ is nonempty. Let I denote a minimal element in this family. Passing to the residue ring $R/0 : J$ and applying item (3), yields that $P := (0 : J) : I$ is a prime ideal. This gives $(JP)I = PI.J = \{0\}$, hence $0 : JP \supset I$. But I contains $0 : J$ properly by construction, hence so does $0 : JP$. Thus, PJ is properly contained in J, being itself a finite product of prime ideals. This contradicts the minimality of J.

(6) By (2), every prime ideal is maximal, hence it suffices to argue with the latter. By (5), $\{0\}$ is the product of a finite family of maximal ideals. Since any maximal ideal contains this product it contains one of its factors, hence must equal this factor. □

The relevance of the statement in item (5) above is the following result of E. Noether.

Theorem 2.5.13 (Noether Artinian criterion [118, Section 10]). *Let R be any ring such that $\{0\}$ is the product of finitely many maximal ideals. Then R satisfies the ascending chain condition if and only if it satisfies the descending chain condition.*

Proof. Set $\{0\} = \mathfrak{m}_1 \cdots \mathfrak{m}_r$, by assumption,with $\mathfrak{m}_i$ a maximal ideal. Consider the sequence of inclusions

$$R \supset \mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \cdots \supset \mathfrak{m}_1 \cdots \mathfrak{m}_r = \{0\}.$$

Claim. If any of the two chain conditions is satisfied in R then the above sequence can be refined by inserting additional ideals so as to reach a finite sequence admitting no proper refinement—such a sequence is called a *composition series* of R and will be fully treated in Subsection 3.1.2; see also Historic Note 3.5.1.

To prove the claim, note that, for each $i = 1, \ldots, r$, the ideal

$$\mathfrak{m}_1 \cdots \mathfrak{m}_{i-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_i \subset R/\mathfrak{m}_1 \cdots \mathfrak{m}_i$$

vanishes when multiplied by the elements of $\mathfrak{m}_i$, hence it has a natural structure of a vector space over the field $(R/\mathfrak{m}_1 \cdots \mathfrak{m}_i)/(\mathfrak{m}_i/\mathfrak{m}_1 \cdots \mathfrak{m}_i) \simeq R/\mathfrak{m}_i$. Clearly, every such vector space inherits both chain condition assumed on R and there are only finitely many such vector spaces. Therefore, one has reduced the problem to showing that if a k-vector space V satisfies one of the chain conditions for its subspaces then it is finite dimensional, and hence any sequence of inclusions of subspaces can be refined to a finite one such sequence admitting no proper refinements.

Now, it is sufficiently clear that the ascending chain condition in V implies its finite dimensionality. For if V has an infinite basis, then by the axiom of choice one can choose a countably infinite subset of this basis, say, $\{v_1, v_2, \ldots\} \subset V$. Then $kv_1 \subsetneq kv_1 + kv_2 \subsetneq \cdots$ is a nonstabilizing chain of subspaces. Next, the descending chain condition implies the ascending chain condition. Otherwise, by the same token, one can choose countably many independent $\{v_1, v_2, \ldots\} \subset V$ and take for each $i = 1, 2, \ldots$ the subspace V_i spanned by $\{v_i, v_{i+1}, \ldots\}$. Clearly, $V_1 \supsetneq V_2 \supsetneq \cdots$ is a nonstabilizing descending chain.

So much for the claim. To complete the proof the statement, it suffices to show that, since R admits at least one composition series, any sequence of inclusions of ideals of R can be refined to obtain a composition series and that any two such series have the same number of terms. This result is due to C. Jordan ([86]) in the case of groups and will be proved in all its generality in Section 3. In fact, once this is shown, then any ascending (resp., descending) chain will eventually refine to a composition series. □

The deepest basic result about Artinian rings to follow is now a consequence of the preceding theorem. Although Nagata in [112] attributes it to Akizuki, there is quite some history behind this result (History 2.8.5).

Theorem 2.5.14 (The Artinian–Noetherian theorem). *The following conditions are equivalent for a ring R:*
(i) *R is Artinian.*
(ii) *R is Noetherian and has Krull dimension zero.*

Proof. (i) $\Rightarrow$ (ii). Combining Proposition 2.5.12 (4) and Theorem 2.5.13 gives that R is Noetherian. The dimension assertion is the content of Proposition 2.5.12 (2).

(ii) $\Rightarrow$ (i). Since R is Noetherian, $\{0\}$ is a product of prime ideals (Proposition 2.5.3). Since $\dim R = 0$, every prime ideal is maximal. Therefore, the hypothesis of Theorem 2.5.13 is satisfied, and hence R satisfies the descending chain condition. □

Remark 2.5.15. Rings of Krull dimension zero were called *einartig* by van der Waerden (see [98, Section 2.9]) and were largely considered by various authors, Krull included. As Krull points out, for such rings that fail to be Noetherian, one should resort to deal with their *graded hull*. This side of the theory will not be pursued in this book.

Proposition 2.5.16. *An Artinian ring is isomorphic to the direct product of finitely many primary Artinian rings and this decomposition is unique up to ordering and isomorphisms.*

Proof. As a first step, one shows that there are ideals $I_1, \dots, I_r$ of R such that $R = I_1 + \cdots + I_r$, verifying the condition $I_i \cup \sum_{j\neq i} I_j = \{0\}$, for every i. As usual, this implies an R-linear isomorphism $R \simeq I_1 \oplus \cdots \oplus I_r$.

To see this, write $\{0\} = \mathfrak{m}_1^{e_1} \cdots \mathfrak{m}_r^{e_r}$, where $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ are the distinct maximal ideals of R (one has used Proposition 2.5.12 (5) and collected repetitions). Since $\mathfrak{m}_i, \mathfrak{m}_j$ are comaximal for $i \neq j$, it follows that $\{0\} = \mathfrak{m}_1^{e_1} \cap \cdots \cap \mathfrak{m}_r^{e_r}$. Now apply the general form of the Chinese remainder theorem to conclude that

$$R = \sum_{i=1}^{r} \left(\bigcap_{j\neq i} \mathfrak{m}_j^{e_j} \right), \quad \text{with } \left(\bigcap_{j\neq i} \mathfrak{m}_j^{e_j} \right) \cap \sum_{j\neq i} \left(\bigcap_{i\neq j} \mathfrak{m}_i^{e_i} \right) = \{0\}.$$

Explicitly, since for every $i = 1, \dots, r$, the ideals $\bigcap_{j\neq i} \mathfrak{m}_j^{e_j}$ and $\mathfrak{m}_i^{e_i}$ are comaximal, then any element $a \in R$ can be written as $b_i + c_i$, with $b_i \in \bigcap_{j\neq i} \mathfrak{m}_j^{e_j}$ and $c_i \in \mathfrak{m}_i^{e_i}$, for $1 \leq i \leq r$. Then $a - \sum_{i=1}^{r} b_i = (a - b_j) - \sum_{j\neq i} b_i \in \mathfrak{m}_j^{e_j}$, since each b_i for $i \neq j$ belongs to $\bigcap_{j\neq i} \mathfrak{m}_j^{e_j} \subset \mathfrak{m}_j^{e_j}$. Since j runs through $1, \dots, r$, one has $a = \sum_{i=1}^{r} b_i$, thus proving that $R = \sum_{i=1}^{r} (\bigcap_{j\neq i} \mathfrak{m}_j^{e_j})$.

The independence condition follows from the inclusion $\sum_{j\neq i} (\bigcap_{i\neq j} \mathfrak{m}_i^{e_i}) \subset \mathfrak{m}_i^{e_i}$ already observed.

Next, since the decomposition is a direct sum, for fixed i the kernel of the projection $R \twoheadrightarrow \bigcap_{j\neq i} \mathfrak{m}_j^{e_j}$ is precisely the subideal $\sum_{j\neq i} (\bigcap_{i\neq j} \mathfrak{m}_i^{e_i}) \subset \mathfrak{m}_i^{e_i}$. Recall the elementary so-called modular law $I \cap (J_1, J_2) = (J_1, I \cap J_2)$ for three ideals I, J_1, J_2 such that $J_1 \subset I$. Applying with $I = \mathfrak{m}_i^{e_i}$, $J_1 = \sum_{j\neq i} (\bigcap_{i\neq j} \mathfrak{m}_i^{e_i})$ and $J_2 = \bigcap_{j\neq i} \mathfrak{m}_j^{e_j}$, it follows that

$$\mathfrak{m}_i^{e_i} = \mathfrak{m}_i^{e_i} \cap R = \mathfrak{m}_i^{e_i} \cap \left(\sum_{j \neq i} \left(\bigcap_{i \neq j} \mathfrak{m}_i^{e_i} \right), \bigcap_{j \neq i} \mathfrak{m}_j^{e_j} \right)$$
$$= \left(\sum_{j \neq i} \left(\bigcap_{i \neq j} \mathfrak{m}_i^{e_i} \right), \mathfrak{m}_i^{e_i} \cap \left(\bigcap_{j \neq i} \mathfrak{m}_j^{e_j} \right) \right) = \left(\sum_{j \neq i} \left(\bigcap_{i \neq j} \mathfrak{m}_i^{e_i} \right), 0 \right) = \sum_{j \neq i} \left(\bigcap_{i \neq j} \mathfrak{m}_i^{e_i} \right).$$

Thus, one has for each $i = 1, \ldots, r$ an R-linear isomorphism $\varphi_i : R/\mathfrak{m}_i^{e_i} \simeq \bigcap_{j \neq i} \mathfrak{m}_j^{e_j}$. But since each $R/\mathfrak{m}_i^{e_i}$ is a ring, the R-linear isomorphism $R \simeq I_1 \oplus \cdots \oplus I_r$ converts into a ring isomorphism $R \simeq R/\mathfrak{m}_1^{e_1} \times \cdots \times R/\mathfrak{m}_r^{e_r}$ given as the composite of

$$a = b_1 + \cdots + b_r \mapsto (b_1, \ldots, b_r) \in \bigoplus_{i=1}^{r} \bigcap_{j \neq i} \mathfrak{m}_j^{e_j}$$

and

$$(b_1, \ldots, b_r) \mapsto (\varphi_1(b_1), \ldots, \varphi_r(b_r)) \in R/\mathfrak{m}_1^{e_1} \times \cdots \times R/\mathfrak{m}_r^{e_r}.$$

This shows that R is isomorphic to the direct product of finitely many Artinian primary (local) rings.

The uniqueness assertion can be obtained as follows: (1) the direct sum decomposition into ideals is characterized by a decomposition $1 = \mathfrak{i}_1 + \cdots + \mathfrak{i}_r$ of the identity, where each $\mathfrak{i}_i$ is an idempotent satisfying the rules $\mathfrak{i}_i \mathfrak{i}_j = 0$ for $i \neq j$; (2) a local ring admits no idempotents other than $0, 1$. From this, assuming another identity decompositions $1 = \mathfrak{j}_1 + \cdots + \mathfrak{j}_s$, one gets by juggling with the above rules that the corresponding idempotents are the same as before up to reordering. □

As a consequence of the above proposition, an Artinian local ring is the piece par excellence of the theory in dimension zero. It plays a central role in both commutative algebra and algebraic geometry.

2.5.2 Associated primes

Let R be a ring and let $I \subset R$ be an ideal. While the set of ring homomorphisms $R \to R/I$ is quite involved, the set of R-linear maps $R \to R/I$ is much simpler: any such map must be given by multiplication by an element of R/I. This leads naturally to the following concept.

Definition 2.5.17. A prime ideal $P \subset R$ is called an *associated prime* of R/I if P is the kernel of an R-linear map $R \to R/I$.

Quite often, by abuse, an associated prime $P \subset R$ of R/I is referred to as an associated prime of the ideal I. Since $P = 0 :_{R/I} (\overline{x})P = I : (x) = I :_R (x)$, for some nonzero element $\overline{x} \in \overline{R} = R/I$, if only to emphasize the role of I in place of R/I, one says that P is the I-annihilator of some $x \in R \setminus I$.

If R is a Noetherian ring, the family of such ideals is reasonably under control, according to the following

Proposition 2.5.18. *Let R be a Noetherian ring and let $I \subsetneq R$ be a proper ideal. Then:*
(i) *The family of annihilators $I : (x)$, with $x \in R \setminus I$, has maximal elements and any such element is a prime ideal (necessarily associated) to R/I;*
(ii) *The associated primes of R/I obtained by way of* (i) *are finitely many.*

Proof. (i) Clearly, the family of such annihilators is nonempty. Since R is Noetherian, it has maximal elements. Let $I : (x)$ be any such maximal annihilator in the family and suppose that $ab \in I : (x)$, where $a, b \in R$, but, say, $a \notin I : (x)$. Since $I : (x) \subset I : (ax)$ and $ax \notin I$, it must be the case that these ideals coincide. Since $b \in I : (ax)$, then $b \in I : (x)$, as required. Thus, $I : (x)$ as chosen is a prime ideal.

(ii) Let $J \subset R$ be the ideal generated by all $x \in R$ such that $P = I : (x)$ is a maximal element in the above family. Since R is Noetherian, J is finitely generated and, clearly, can be generated by a set $\{x_1, \ldots, x_n\}$ such that $P = I : (x_i)$ is a maximal element for every $i = 1, \ldots, n$. Setting $P_i = I : (x_i)$, $1 \leq i \leq n$, the maximal annihilators are precisely $P_1, \ldots, P_n$. Indeed, for any maximal annihilator $P = I : (x)$, write $x = \sum_i a_i x_i$, with $a_i \in R$. This readily implies $P \supset P_1 \cap \cdots \cap P_n$, hence $P \supset P_i$ for some i. Therefore, $P = P_i$ by maximality. □

Note that, as a consequence, the set $\mathcal{Z}(R/I)$ of the elements of R which are not regular modulo I is the union of a finite family of prime ideals, each of which is the I-annihilator of an element in $R \setminus I$.

As a side consequence, an element $a \in R$ is regular modulo I if and only if it avoids all associated primes of R/I. This provides the following useful fact.

Proposition 2.5.19. *Let R be a Noetherian ring, $I \subset R$ an ideal. If $a \in I$ is regular modulo I, then* $\operatorname{ht}(I, a) \geq \operatorname{ht} I + 1$.

Proof. By definition, one has to show that $\operatorname{ht} Q \geq \operatorname{ht} I + 1$ for every prime $Q \supset (I, a)$. Since $Q \supset I$, there is a minimal prime P of R/I contained in Q. But $a \notin P$ as it is regular modulo I. Therefore, the inclusion $P \subset Q$ is proper, resulting in $\operatorname{ht} Q \geq \operatorname{ht} P + 1 \geq \operatorname{ht} I + 1$. □

Going somewhat in the opposite direction, one has the following.

Proposition 2.5.20. *Let R be a Noetherian ring and let $I \subset R$ be an ideal. Then:*
(i) *Every minimal prime overideal $P \subset R$ of I is an associated prime of R/I.*
(ii) *I admits only finitely many minimal prime overideals.*

Proof. (i) The following reduction strategy is left to the reader's verification: localizing at P, one has that $P_P \subset R_P$ is a minimal prime overideal of I_P; in addition, if P_P is an associated prime of R_P/I_P then P is an associated prime of R/P.

This granted, one can assume that R is a Noetherian local ring, with unique maximal ideal $\mathfrak{m}$ and that $I \subset \mathfrak{m}$ is an ideal over which $\mathfrak{m}$ is minimal. Then, for any $x \in R \setminus I$, one has $I \subset I : x \subset \mathfrak{m}$. Take x such that $I : x$ is maximal possible. Then, by Proposition 2.5.18 (i), $I : x$ is a prime ideal, hence it must coincide with $\mathfrak{m}$ since $\mathfrak{m}$ is minimal over I.

(ii) Consider the family of ideals of R for which the assertion fails and assume it is nonempty. Let $J \subset R$ be a maximal element thereof. In particular, J is not a prime ideal, so there are elements $a, b \in R$ such that $ab \in J$ but neither $a \in J$ nor $b \in J$. By maximality, each of the ideals (J, a) and (J, b) admits only finitely many minimal prime overideals. Therefore, it suffices to show that $J = (J, a) \cap (J, b)$ up to radicals. This is easy: if $x \in \sqrt{(J, a)} \cap \sqrt{(J, b)}$, then $x^n = y_1 + c_1 a$ and $x^m = y_2 + c_2 b$, for some $n, m \geq 1$ and with $y_1, y_2 \in J$. Then $x^{n+m} \in J$, as required. □

With just slightly more work, one can state the following criterion.

Proposition 2.5.21. *Let R be a Noetherian ring and let $I \subset R$ be an ideal.*

(i) *A necessary and sufficient condition that a prime ideal $P \subset R$ be associated to R/I is that $I : (I : P) \subset P$.*

(ii) *Given an ideal $J \subset R$, then the inclusion $I \subset I : J$ is proper if and only if J is contained in some associated prime of R/I.*

Proof. (i) As in the proof of Proposition 2.5.20, the statement localizes, hence one can assume that R is a local ring and $P = \mathfrak{m}$ is the unique maximal ideal of R. In this case, the inclusion $I : (I : \mathfrak{m}) \subset \mathfrak{m}$ is equivalent to having a proper inclusion $I \subsetneq I : \mathfrak{m}$.

But the latter takes place if and only if $\mathfrak{m}$ is an associated prime of R/I. Indeed, if $\mathfrak{m}$ is an associated prime of R/I then $\mathfrak{m} = I : (x)$ for some $x \in \mathfrak{m} \setminus I$, hence every element of $\mathfrak{m}$ is a zero-divisor on R/I. At least one such element is not zero module R/I unless $\mathfrak{m} = I$, in which case the conclusion is obvious as $\mathfrak{m} : \mathfrak{m} = (1) = R$ which contains $\mathfrak{m}$ properly. Conversely, if the inclusion $I \subset I : \mathfrak{m}$ is proper, let $x \in (I : \mathfrak{m}) \setminus I$. Then $x\mathfrak{m} \subset I$, hence $\mathfrak{m} \subset I : (x)$. Since $x \notin I$, this inclusion must be an equality. Thus, $\mathfrak{m}$ is an associated prime of R/I.

(ii) Suppose that $I \subset I : J$ is a proper inclusion and let $x \in (I : J) \setminus I$. Then $J \subset I : (x)$, where $x \notin I$. By the maximum condition J is contained in some maximal annihilator $I : (y)$ and the latter is a prime ideal (see the proof of Proposition 2.5.18), hence is an associated prime of R/I.

The converse is left to the reader. □

The set of all associated primes of R/I is commonly denoted by $\mathrm{Ass}(R/I)$. So far, one has taken care of the minimal and maximal elements of this set, while the other ones are also finitely many, a result to be proved in Theorem 2.6.3. The minimal primes of the family $\mathrm{Ass}(R/I)$ are called *minimal primes* of R/I.

The next result is one of the many forms of the so-called "prime avoidance" lemma.

Lemma 2.5.22 (Prime avoidance). *Let R be a ring and let $J_1, \dots, J_n$ be ideals of which at least $n-2$ are prime. Given an ideal $I \subset R$ such that $I \subset J_1 \cup \cdots \cup J_n$, then one has $I \subset J_i$ for some i.*

Proof. By induction on n, there is nothing to prove if $n = 1$. If $n \geq 2$, by the inductive hypothesis, one may assume that I is not contained in the union of a proper subset of $\{J_1, \dots, J_n\}$ because the assumption to the effect that at least $n-2$ of them are prime only gets stronger. Then, for every i pick

$$x_i \in I \setminus J_1 \cup \cdots \cup J_{i-1} \cup J_{i+1} \cup \cdots \cup J_n.$$

Note that then $x_i \in J_i$ for every i since $x_i \in I \subset J_1 \cup \cdots \cup J_n$ (all of them).

Now, if $n = 2$ one has $x_1 + x_2 \in I \setminus J_i$ for every i, a contradiction.

If $n > 2$, assume as one can that J_1 is prime. Then the element $x_1 + (x_2 \cdots x_n)$ belongs to I but to none of the J_i's. □

Proposition 2.5.23. *Let R be a Noetherian ring and let $P \subset R$ be a prime ideal of height n. Then P is a minimal prime overideal of an ideal generated by n elements.*

Proof. Proceed by induction on n. For $n = 0$, P is a minimal prime of the ring, hence the ideal $\{0\}$ will do it (as it is generated by the empty set).

Thus, let $n \geq 1$. By Proposition 2.5.20 the ring R (*i. e.*, the zero ideal) has only finitely many minimal prime ideals $P_1, \dots, P_m$. Of course, $\operatorname{ht} P_i = 0 \ \forall i$ and since $\operatorname{ht} P = n \geq 1$, then $P \not\subset P_i \ \forall i$. By Lemma 2.5.22, there exists $a \in P \setminus P_i \ \forall i$. Set $\overline{R} = R/(a)$ and $\overline{P} = P/(a)$. It is easy to see that $\operatorname{ht}(\overline{P}) \leq n-1$. Indeed, any prime chain $\overline{P_0} \subsetneq \cdots \subsetneq \overline{P_m} = \overline{P}$ can be lifted to a prime chain $P_0 \subsetneq \cdots \subsetneq P_m = P$ and the latter can be properly augmented with a minimal prime ideal $P_i \subsetneq P_0$ since $\operatorname{ht}(P_0) \geq 1$ as $a \in P_0 \setminus P_i$. The rest is immediate by the inductive hypothesis. □

The previous result is sometimes referred to as the converse to the prime ideal theorem of Krull, but it is by no means of the same depth.

2.5.3 Krull's principal ideal theorem

The next result is one of the cornerstones of Noetherian ring theory, if not of commutative algebra itself. The present account follows pretty much Krull's original argument.

One needs the not less famous preliminary result.

Lemma 2.5.24. *Let R be a ring with Jacobson radical $\mathfrak{N}$ and let $\mathfrak{a} \subset R$ be a finitely generated ideal. If $\mathfrak{a} \subset \mathfrak{N}\mathfrak{a}$, then $\mathfrak{a} = \{0\}$.*

Proof. Assuming $\mathfrak{a} \neq \{0\}$, let $\{a_1, \dots, a_n\}$ be a set of generators of $\mathfrak{a}$ with $n \geq 1$. By assumption, one can write $a_1 = b_1 a_1 + \cdots + b_n a_n$, for suitable $b_i \in \mathfrak{N}$. It follows that $(1 - b_1)a_1 \in (a_2, \dots, a_n)$, hence $a_1 \in (a_2, \dots, a_n)$ as $1 - b_1$ is invertible. Thus one can always reduce any set of generators, and eventually get $\mathfrak{a} = \{0\}$. □

A more general version of this lemma will be given in Section 5.1 that bears the names of three mathematicians.

Theorem 2.5.25 (Principal ideal theorem). *Let R be a Noetherian ring and let $a \in R$ be a noninvertible element. Then any minimal prime overideal of (a) has height at most* 1.

Proof. Let $P \supset (a)$ be a minimal prime overideal. One can assume that $a \neq 0$ as otherwise certainly $\operatorname{ht}(P) = 0$. Now suppose as it might that there exists a prime chain $P_0 \subsetneq P_1 \subsetneq P$. Passing to the ring R/P_0, the ideal $P/P_0 \subset R/P_0$ is a minimal prime overideal of the nonzero principal ideal $(a, P_0)/P_0 \subset R/P_0$ and one has a prime chain $\{0\} \subsetneq P_1/P_0 \subsetneq P/P_0$ in the domain R/P_0. Thus, on can assume at the outset that R is a domain and there is a nonzero prime ideal Q properly contained in P. One now argues that this is impossible.

First, localize R on P to assume that R is local with maximal ideal $\mathfrak{m}$ minimal over (a) and there is a nonzero prime $Q \subsetneq \mathfrak{m}$. Consider the descending sequence

$$\cdots \supset Q^{(m)} \supset Q^{(m+1)} \supset \cdots,$$

where $Q^{(m)}$ is the mth symbolic power of Q introduced in Section 2.1.3. Note that $Q^{(m)}$ is a Q-primary ideal.

Next, pass to the residue ring $R/(a)$. Since $\mathfrak{m}$ is minimal over (a), the height of the maximal ideal $\mathfrak{m}/(a)$ is 0, hence $\dim R/(a) = 0$. Since R is Noetherian, then $R/(a)$ is an Artinian ring by Theorem 2.5.14, hence the induced sequence

$$\cdots \supset (Q^{(m)}, a)/(a) \supset (Q^{(m+1)}, a)/(a) \supset \cdots$$

stabilizes. Say, $(Q^{(m)}, a)/(a) = (Q^{(m+1)}, a)/(a) = \cdots$.

One claims that $Q^{(m)} = Q^{(m+1)} + aQ^{(m)}$. To see the nontrivial inclusion, let $x \in Q^{(m)}$. Since m is a stability value, we can write $x = y + ba$, with $y \in Q^{(m+1)}$ and $b \in R$. Then $ba \in Q^{(m)}$. But $a \notin \sqrt{Q^{(m)}} = Q$ since $Q \subsetneq \mathfrak{m}$ and $\mathfrak{m}$ is minimal over (a). It follows that $a \in Q^{(m)}$ since $Q^{(m)}$ is a primary ideal. This proves the claim.

Finally, one passes to the residue ring $R/Q^{(m+1)}$, which is still local, to get the equality $Q^{(m)}/Q^{(m+1)} = (a)Q^{(m)}/Q^{(m+1)}$. But since $a \in \mathfrak{m}$ and $\mathfrak{m}/Q^{(m+1)}$ is the unique maximal ideal of $R/Q^{(m+1)}$, one deduces from Lemma 2.5.24 that $Q^{(m)} = Q^{(m+1)}$, hence $Q_Q^m = Q_Q^{m+1} = QQ_Q^m$. A second application of Lemma 2.5.24, this time around on R_Q, gives $Q_Q^m = \{0\}$, hence $Q_Q = \{0\}$ since R_Q is a domain. It follows that $Q = \{0\}$ as well; this is a contradiction to the original assumption that Q was nonzero. □

The above theorem has an expected inductive generalization, though in the actual proof the induction is not entirely trivial as it is based upon a preliminary result on prime avoidance along a chain of primes—in the words of Krull: "nicht ganz triviale Bemerkung."

Accordingly, one first deals with this refinement of prime avoidance.

Lemma 2.5.26 (Prime avoidance along a chain of primes). *Suppose that R is a Noetherian ring. Let $Q, P_1, \ldots, P_r \subset R$ be prime ideals such that $Q \not\subset P_i$ $\forall i$. Then for any prime*

chain $Q_0 = Q \supsetneq Q_1 \supsetneq \cdots \supsetneq Q_m$ there exists a prime chain $Q_0' = Q_0 \supsetneq Q_1' \supsetneq \cdots \supsetneq Q_{m-1}' \supsetneq Q_m' = Q_m$ such that $Q_j' \not\subset P_i$ for every i and $j = 1, \ldots, m-1$.

Proof. By iterating (top to bottom), it suffices to prove the case where $m = 2$, with $Q_0 \supsetneq Q_1 \supsetneq Q_2$, in which case one only has to guess the intermediate prime Q_1'. Now, by ordinary prime avoidance (Lemma 2.5.22), $Q_0 \not\subset Q_2 \cup P_1 \cup \cdots \cup P_r$, hence pick $x \in Q_0$ such that $x \notin Q_2$ and $x \notin P_i$ for every $1 \leq i \leq r$. Let Q_1' denote a minimal prime overideal of (Q_2, x) contained in Q_0—to see that such minimal prime is available, pass to the corresponding radicals and use Proposition 2.5.20. Clearly, the containment $Q_1' \supset Q_2$ is proper as $x \notin Q_2$. At the other end, applying Theorem 2.5.25 to the principal ideal $(x, Q_2)/Q_2$ on the ring R/Q_2 and its minimal prime overideal Q_1'/Q_2, one has $\operatorname{ht}(Q_1'/Q_2) \leq 1$ while $\operatorname{ht}(Q_0/Q_2) \geq 2$ as $\{0\} \subsetneq Q_1/Q_2 \subsetneq Q_0/Q_2$ is a prime chain. This shows that the other inclusion $Q_0 \supset Q_1'$ is also strict. □

Theorem 2.5.27 (Prime ideal theorem). *Let R denote a Noetherian ring and let $(a_1, \ldots, a_n) \subsetneq R$, be an n-generated proper ideal. Then any minimal prime overideal P of $(a_1, \ldots, a_n)$ has height at most n.*

Proof. Proceed by induction on n. The result is vacuous for $n = 0$, so assume that $n \geq 1$. Let $Q_0 = P \supsetneq Q_1 \supsetneq \cdots \supsetneq Q_m$ be any prime chain. Set $J = (a_1, \ldots, a_{n-1})$. By the inductive hypothesis, one may assume that P is not any of the minimal prime overideals $\{P_1, \ldots, P_r\}$ of J. Applying Lemma 2.5.26, there is a prime chain $Q_0' = P \supsetneq Q_1' \supsetneq \cdots \supsetneq Q_{m-1}' \supsetneq Q_m' = Q_m$ each prime of which avoids the set $\{P_1, \ldots, P_r\}$.

Now on one hand, $\operatorname{ht}(P/J) \leq 1$ by applying Theorem 2.5.25 to the principal ideal $(a_n, J)/J$ and its minimal prime P/J on the ring R/J. On the other hand, $Q_{m-1}' \not\subset P_i$ implies that $(Q_{m-1}', J)/J \not\subset P_i/J$ for every $i = 1, \ldots, r$. Since $\{P_1/J, \ldots, P_r/J\}$ is the set of minimal primes of the ring R/J, this shows that any minimal prime overideal of $(Q_{m-1}', J)/J \subset R/J$ has height ≥ 1. Since $\operatorname{ht}(P/J) \leq 1$, then P/J is necessarily a minimal prime overideal of $(Q_{m-1}', J)/J$, hence P is a minimal prime overideal of (Q_{m-1}', J).

Passing to the residue ring R/Q_{m-1}', the ideal P/Q_{m-1}' is a minimal prime overideal of $(Q_{m-1}', J)/Q_{m-1}'$ on the ring R/Q_{m-1}', an ideal generated by $n-1$ elements (the residues of $a_1, \ldots, a_{n-1}$). By the inductive hypothesis, $\operatorname{ht} P/Q_{m-1}' \leq n-1$. Because of the prime chain $P/Q_{m-1}' \supsetneq Q_1'/Q_{m-1}' \supsetneq \cdots \supsetneq Q_{m-1}'/Q_{m-1}' = \{0\}$ of length $m-1$ on R/Q_{m-1}', one concludes that $m - 1 \leq n - 1$, *i. e.*, $m \leq n$ as required. □

Corollary 2.5.28. *Any prime ideal in a Noetherian ring has finite height.*

Proof. Apply the foregoing result with $P = (a_1, \ldots, a_n)$, for suitable n. □

2.5.4 Dimension under extensions

Consider a ring extension $R \subset S$. A natural question arises as to whether one can relate the corresponding Krull dimensions other than in integral extensions.

2.5.4.1 Polynomial extensions

In this part, one considers the extension $R \subset R[X]$, where X is an indeterminate over R. The case in sight is when R is a Noetherian ring since otherwise the results are more complicated. The treatment here is taken from [138, Chapitre III, (D)].

It is quite elementary to see that, for an arbitrary ring R, if $P \subset R$ is a prime ideal then its extension $PR[X]$ is also prime and its contraction to R is P. The next simple result for polynomial extensions gives more information.

Lemma 2.5.29. *Let R be an arbitrary ring and let $Q \subsetneq Q' \subset R[X]$ be distinct prime ideals having the same contraction to R. Then the extension to $R[X]$ of the common contraction is Q.*

Proof. Set $P = Q \cap R = Q' \cap R$. Passing to the domain R/P, one may assume that $P = \{0\}$ (why?). Passing to the ring of fractions with respect to $S = R \setminus \{0\}$, may further assume that R is a field (why?). Say, $R = k$. But for the principal ideal domain $k[X]$ the result is clear since $\dim k[X] = 1$. □

As an immediate consequence, one gets the following.

Corollary 2.5.30. *Let R be an arbitrary ring. Then for any ideal $I \subset R$ and any minimal prime ideal P of I, the extended ideal $PR[X]$ is a minimal prime of the extension $IR[X]$.*

Proof. Suppose not. Then $IR[X] \subset Q \subsetneq PR[X]$ for some prime ideal Q of $R[X]$. Since $PR[X]$ contracts to P, Lemma 2.5.29 gives a contradiction. □

Proposition 2.5.31. *Let R be a Noetherian ring.*
(i) $\operatorname{ht}(P) = \operatorname{ht}(PR[X])$ *for any prime ideal P of R.*
(ii) $\dim R[X] = \dim R + 1$.

Proof. (i) Clearly, $\operatorname{ht}(P) \leq \operatorname{ht}(PR[X])$ by taking the extensions of the primes in a prime ideal chain for P. For the reverse inequality, let $\operatorname{ht}(P) = n$. By Proposition 2.5.23, there is an ideal $I \subset R$ generated by n elements such that P is a minimal prime of I. By Lemma 2.5.30, $PR[X]$ is a minimal prime of $IR[X]$. Since the latter is still generated by n elements, Theorem 2.5.27 implies that $\operatorname{ht}(PR[X]) \leq n$, as required.

(ii) By (i), one can assume that $\dim R < \infty$. Then $\dim R = \operatorname{ht}(P)$ for some (maximal) prime. Then $\operatorname{ht}(PR[X]) = \dim R$ by the first part. Since, $PR[X]$ is not a maximal ideal, necessarily $\dim R[X] \geq \dim R + 1$.

For the reverse inequality, take any chain of prime ideals $Q_0 \subsetneq \cdots \subsetneq Q_m$ in $R[X]$. Consider the sequence of contracted primes $Q_i \cap R$. If no collapsing happens along this sequence, $m \leq \dim R$. By the first inequality, the chain of primes of $R[X]$ is not maximal possible. Thus, let $i \geq 0$ denote the first index from the right such that $Q_i \cap R = Q_{i+1} \cap R$. By Lemma 2.5.29 and part (i) of the present statement, $\operatorname{ht}(Q_i \cap R) = \operatorname{ht}(Q_i) \geq i$. But the length of the chain $Q_i \cap R \subsetneq Q_{i+2} \cap R \subsetneq \cdots \subsetneq Q_m \cap R$ added to $\operatorname{ht}(Q_i \cap R)$ certainly gives a lower bound to $\dim R$, *i. e.*, $\dim R \geq m - i - 1 + i = m - 1$, hence $m \leq \dim R + 1$, as required. □

Corollary 2.5.32. *If R is a Noetherian ring and $X_1, \dots, X_n$ are indeterminates over R, then* $\dim R[X_1, \dots, X_n] = \dim R + n$. *In particular, if k is a field then* $\dim k[X_1, \dots, X_n] = n$.

Using the Noether dimension theorem, one deduces the following.

Proposition 2.5.33. *Let $R = k[X_1, \dots, X_n]$ and let $Q \subset R$ denote a prime ideal. Then* $\dim R/Q + \operatorname{ht} Q = n$.

Proof. Induct on n, the result being trivial for $n = 0$

Let $n \geq 1$ and set $S := k[X_1, \dots, X_{n-1}] \subset R$, with $P := Q \cap S$.

Consider the usual two cases:

(1) $PR \neq Q$.

Then $\operatorname{ht} Q \geq \operatorname{ht} P + 1$ by Proposition 2.5.31 (i). Therefore, by the inductive hypothesis

$$\operatorname{ht} Q \geq \operatorname{ht} P + 1 = \dim S - \dim S/P + 1 = \dim R - 1 - \dim S/P + 1 \geq \dim R - \dim R/Q,$$

where one has used that $\dim S/P = \operatorname{trdeg}_k(S/P)$ and $\dim R/Q = \operatorname{trdeg}_k(R/Q)$ by Theorem 2.3.7.

Since $\operatorname{ht} Q \leq \dim R - \dim R/Q$ always holds, one is done in this case.

(2) $PR = Q$.

Here, one has $R/Q = R/PR \simeq (S/P)[X_n]$, hence $\dim R/Q = \dim S/P + 1$ by Proposition 2.5.31 (ii). Therefore, by the inductive hypothesis

$$\operatorname{ht} Q = \operatorname{ht} P = \dim S - \dim S/P = \dim R - 1 - \dim S/P + 1 \geq \dim R - \dim R/Q$$

and one concludes as before. □

Corollary 2.5.34. *Let R be a finitely generated domain over a field k and let $P \subset R$ be a prime ideal. Then* $\dim R/P + \operatorname{ht} P = \dim R$.

Proof. Take a Noether normalization $k[\mathbf{x}] = k[x_1, \dots, x_r] \subset R$, $r = \dim R$, and let $Q := P \cap k[\mathbf{x}]$. By Proposition 2.5.33, one has

$$\dim k[\mathbf{x}]/Q + \operatorname{ht} Q = r = \dim R.$$

Since $k[\mathbf{x}]/Q \hookrightarrow R/P$ is also integral, then $\dim k[\mathbf{x}]/Q = \dim R/P$ and $\operatorname{ht} Q = \operatorname{ht} P$ by Corollary 2.3.3 and its proof, respectively. Therefore, $\dim R/P + \operatorname{ht} P = \dim R$ as required. □

Proposition 2.5.35. *Let S stand for a polynomial ring in finitely many variables over a domain R. Let $P \subset S$ denote a prime ideal and $\wp := P \cap R$ its contraction to R. Then*

$$\operatorname{height} P - \operatorname{height} \wp = \operatorname{trdeg}_R(S) - \operatorname{trdeg}_{k(\wp)}(k(P)), \tag{2.5.35.1}$$

where $k(\wp)$ and $K(P)$ denote the respective fields of fractions of $R/\wp$ and S/P.

The proof is left to the reader, drawing upon the same techniques used in the discussion of Theorem 2.5.31 and Proposition 2.5.33.

2.5.4.2 Arbitrary extensions

In this part, one considers the more encompassing case of an extension $R \subset S$ of domains.

The results are inspired from the following.

Proposition 2.5.36. *Let $R \subset S$ be a finitely generated extension with S a domain. Let $P \subset S$ denote a prime ideal such that $P \cap R = \{0\}$. Then*

$$\operatorname{height} P = \operatorname{trdeg}_R(S) - \operatorname{trdeg}_R(S/P), \tag{2.5.36.1}$$

Proof. Since $P \cap R = \{0\}$, passing to the localization $R_{\{0\}}$ of R at its zero (prime) ideal preserves the primeness of $PS_{\{0\}}$; consequently, $\operatorname{height} P = \operatorname{height} PS_{\{0\}}$. On the other hand, since $R_{\{0\}}$ is a field and $S_{\{0\}}$ is finitely generated over $R_{\{0\}}$, Theorem 2.3.7 yields

$$\operatorname{trdeg}_R(S) = \operatorname{trdeg}_{R_{\{0\}}}(S_{\{0\}}) = \dim S_{\{0\}}$$

and

$$\operatorname{trdeg}_R(S/P) = \operatorname{trdeg}_{R_{\{0\}}}(S_{\{0\}}/PS_{\{0\}}) = \dim S_{\{0\}}/PS_{\{0\}},$$

so the result follows from Proposition 2.5.33 as mentioned in Corollary 2.5.34. □

The first important result is due to I. S. Cohen ([38]). It has been popularized in [108] as the *dimension inequality*.

Theorem 2.5.37 (Cohen defect formula). *Let $R \subset S$ be a finitely generated extension with S a domain. Let $P \subset S$ denote a prime ideal and $\wp := P \cap R$ its contraction to R. Then*

$$\operatorname{height} P - \operatorname{height} \wp \leq \operatorname{trdeg}_R(S) - \operatorname{trdeg}_{k(\wp)}(k(P)), \tag{2.5.37.1}$$

where $k(\wp)$ and $K(P)$ denote the respective fields of fractions of $R/\wp$ and S/P.

Proof. One inducts on the cardinality n of a finite set of generators of S as an R-algebra. There is nothing to prove if $n = 0$ (*i. e.*, $R = S$). Thus, assume that $n \geq 1$. Say, $S = R[x_1, \ldots, x_n]$. Considering the R-subalgebra $R[x_1, \ldots, x_{n-1}]$, for which by the inductive hypothesis the inequality holds, one can reduce the problem to the case where $S = R[x]$, generated over R by one single element.

Let $Q \subset S$ be such that $S \simeq R[X]/Q$, with X a variable over R and Q a prime ideal. If $Q = 0$ the result follows from Proposition 2.5.35, hence assume that $Q \neq 0$. In this case, $\operatorname{height} Q > 0$ since R is a domain, so one gets

$$\begin{aligned} \dim R[X]/Q &\leq \dim R[X] - \operatorname{height} Q = \dim R + 1 - \operatorname{height} Q \\ &\leq \dim R + 1 - 1 = \dim R. \end{aligned}$$

By Theorem 2.3.7, one has $\operatorname{trdeg}_R(S) = 0$, hence one has to prove the inequality $\operatorname{height} P \leq \operatorname{height} \wp - \operatorname{trdeg}_{k(\wp)}(k(P))$.

Now, since $R \subset R[X]/Q$ by the obvious identification, one has $Q \cap R = \{0\}$. Therefore, $QR_{\{0\}}[X]$ is a prime, necessarily of height 1, where $R_{\{0\}}$ denotes the field of fractions of R (localization at the zero ideal of the domain R). Thus, height $Q = 1$ as well. Letting $\tilde{P} \subset R[X]$ denote the prime ideal such that $P = \tilde{P}/Q$, one has $k(\tilde{P}) = k(P)$. Since $\tilde{P} \cap R = \wp$ and $\wp R[X] \subsetneq \tilde{P}$ because $\wp R[X] \subsetneq (\wp, Q) \subset \tilde{P}$, then

$$\text{height } \tilde{P} = \text{height } \wp + 1 - \text{trdeg}_{k(\wp)}(k(\tilde{P})) = \wp + 1 - \text{trdeg}_{k(\wp)}(k(P))$$

by Proposition 2.5.31 (i) and Proposition 2.5.35.

On the other hand, one has

$$\begin{aligned}\text{height } P = \text{height } P_P = \text{height } \tilde{P}_{\tilde{P}}/Q_{\tilde{P}} = \dim S_{\tilde{P}}/Q_{\tilde{P}} \\ \leq \dim S_{\tilde{P}} - \text{height } Q_{\tilde{P}} = \text{height } \tilde{P} - \text{height } Q = \text{height } \tilde{P} - 1.\end{aligned}$$

Collecting the pieces, one gets the stated inequality. □

Corollary 2.5.38. *Let $R \subset S$ be a finitely generated extension, let $P \subset S$ denote a prime ideal and $\wp := P \cap R$ its contraction to R. Then*

$$\begin{aligned}\dim S/P &\leq \dim R/\wp + \text{trdeg}_{R/\wp}(S/P) \\ &\leq \dim R/\wp + \dim S_\wp/\wp S_\wp,\end{aligned}$$

where $S_\wp = \mathfrak{S}^{-1}S$, with $\mathfrak{S} = R \setminus \wp$.

Proof. For the first inequality, one can assume that $R \subset S$ are domains and the inequality to be proved becomes $\dim S \leq \dim R + \text{trdeg}_R(S)$. Now, this follows from Theorem 2.5.37 applied with P such that height $P = \dim S$, noting that height $\wp \leq \dim R$ for any prime $\wp \subset R$.

For the inequality in the second line above, note that since $R_\wp/\wp_\wp$ is a field then

$$\text{trdeg}_{R/\wp}(S/P) = \dim S_\wp/PS_\wp \leq \dim S_\wp/\wp S_\wp.$$

Of a slightly different content is the following more recent result, where the emphasis is switched to the Krull dimension of the rings involved.

Proposition 2.5.39 ([141]). *Let $R \subset S$ be a finitely generated extension with S a domain. Suppose that there exists a prime ideal $P \subset S$ such that $P \cap R = \{0\}$ and $S = R + P$. Then*

$$\dim S = \dim R + \text{height } P = \dim R + \text{trdeg}_R(S).$$

Proof. One has $S/P = R + P/P \simeq R/R \cap P = R$. Therefore, Proposition 2.5.36 gives height $P = \text{trdeg}_R(S)$. Again, since $S/P \simeq R$, one has the trivial inequality $\dim S \geq \dim R + \text{height } P$.

On the other hand, one may clearly assume that $\dim R < \infty$, hence also $\dim S < \infty$. Thus, let $\mathfrak{M} \subset S$ denote a maximal ideal such that $\dim S = \text{height}\, \mathfrak{M}$ and $\mathfrak{m} := \mathfrak{M} \cap R$. By Theorem 2.5.37.1,

$$\begin{aligned}\dim S = \text{height}\, \mathfrak{M} &\leq \text{height}\, \mathfrak{m} + \text{trdeg}_R(S) - \text{trdeg}_{k(\mathfrak{m})}(k(\mathcal{M})) \\ &\leq \text{height}\, \mathfrak{m} + \text{trdeg}_R(S) \leq \dim R + \text{trdeg}_R(S) = \dim R + \text{height}\, P.\end{aligned}$$

This completes the argument. □

Corollary 2.5.40. *Let $S = S_0 \oplus S_1 \oplus \cdots$ denote a Noetherian $\mathbb{N}$-graded domain and let $S_+ \subset S$ denote the ideal generated by the elements of positive degree. Then* $\dim S = \dim S_0 + \text{height}\, S_+$.

More on graded structures in Section 7.

2.6 Primary decomposition

In this section, one confronts the role of the associated primes with the theory of primary decomposition. The latter was a brilliant achievement of Emmy Noether and constitutes a great simplification of prime and primary ideal theory in Noetherian rings.

2.6.1 The nature of the components

The basic insight of E. Noether consisted in starting out with a stronger notion than that of a primary ideal.

Definition 2.6.1. Let R be a ring. An ideal $I \subset R$ is *irreducible* if it is not the proper intersection of two ideals, that is, whenever there are ideals $I_1, I_2 \subset R$ such that $I = I_1 \cap I_2$, then either $I_1 = I$ or $I_2 = I$.

The terminology is inspired from the classical case of an irreducible polynomial. Noether showed the following.

Lemma 2.6.2. *Let R denote a Noetherian ring. Then:*
(1) (Satz II) *Any ideal is the intersection of a finite set of irreducible ideals.*
(2) (Satz VI) *An irreducible ideal is primary.*

Proof. (1) Assume the assertion is false, so the family of ideals of R for which the assertion fails has a maximal element $I \subset R$. Since I is not irreducible, one must have an intersection $I = I_1 \cap I_2$ where both factors contain I properly. By the maximality of I, both I_1 and I_2 must be finite intersections of irreducible ideals, hence so is I—a contradiction.

(2) Let $I \subset R$ be irreducible, but not primary. By definition, there are elements $a, b \in R$ such that $ab \in I$, but neither $a \in I$ nor $b^l \in I$ for every integer $l \geq 1$. Then the ideals (I, a) and (I, b^l) (for all $l \geq 1$) contain I properly.

One claims that there is an integer $r \geq q$ such that $I = (I, a) \cap (I, b^r)$. This will give that I is not irreducible—a contradiction. To get an integer r for which the proposed equality holds, consider the chain of ideals $I : (b) \subset I : (b^2) \subset \cdots$ and take r to be an exponent from which on the chain becomes stationary.

With this choice, let $c \in (I, a) \cap (I, b^r)$. Then $c = x + ua = y + vb^r$ for certain $x, y \in I$ and $u, v \in R$. Multiplying through by b yields $bx + uab = by + vb^{r+1}$, with the left-side member belonging to I (since $ab \in I$). Therefore, $vb^{r+1} \in I$, *i. e.*, $v \in I : (b^{r+1}) = I : (b^r)$, hence $vb^r \in I$. Summing up, it has been shown that $c = y + vb^r \in I$, as required. □

As a consequence of the above result, every ideal in a Noetherian ring is the intersection of a finite set of primary ideals. However, as Noether pretty much understood, one may need to develop two different theories, depending as to whether one takes irreducible or primary ideals as the desired components.

That a primary ideal is quite commonly not irreducible is easily seen by noting the decomposition $(x, y)^2 = (x, y^2) \cap (x^2, y)$ into irreducible components of the primary ideal $(x, y)^2$ in the polynomial ring $k[x, y]$.

Another question has to do with the uniqueness of a primary decomposition. For example, the ideal (x^2, xy) admits the following two primary decompositions

$$(x^2, xy) = (x) \cap (x, y)^2 = (x) \cap (x, y^2) \cap (x^2, y),$$

the first a decomposition into primary ideals not all irreducible, the second a decomposition into irreducible ideals. This tells us that without further restrictions, even the number of primary components is not uniquely defined.

This motivates introducing the following restriction: a primary decomposition is *reduced* or *irredundant* provided (1) none of the components is superfluous, *i. e.*, no component contains intersections of others; (2) the components have distinct prime ideals.

It is an easy exercise—using the fact that the intersection of primary ideals with the same radical is still primary with that radical—to see that any primary decomposition affords a unique reduced primary decomposition.

The set of associated primes of R/I will be denoted by $\mathrm{Ass}(R/I)$. If needed, one denotes the set of minimal primes of R/I by $\mathrm{Min}(R/I)$. Recall that $\mathrm{Min}(R/I) \subset \mathrm{Ass}(R/I)$. The totality of primes $P \subset R$ containing I is the *support* of R/I. It contains $\mathrm{Ass}(R/I)$ as a subset and the minimal primes in the support coincide with the minimal associated primes. The associated primes $P \in \mathrm{Ass}(R/I) \setminus \mathrm{Min}(R/I)$ are called *embedded* associated primes of R/I. Any such associated prime contains properly at least one minimal prime of R/I.

2.6.2 The Lasker–Noether fundamental theorem

Theorem 2.6.3 (Primary decomposition). *Let $I \subset R$ be an ideal of a Noetherian ring R. For any reduced primary decomposition $I = \bigcap_{i=1}^{m} \mathcal{P}_i$, one has:*

(a) $\{\sqrt{\mathcal{P}_1}, \dots, \sqrt{\mathcal{P}_m}\} = \mathrm{Ass}(R/I)$.
(b) *For any other reduced primary decomposition* $I = \bigcap_{i=1}^{m} \mathcal{Q}_i$, *one has*

$$\{\mathcal{P}_i \mid \sqrt{\mathcal{P}_i} \in \mathrm{Min}(R/I)\} = \{\mathcal{Q}_i \mid \sqrt{\mathcal{Q}_i} \in \mathrm{Min}(R/I)\}.$$

Proof. Let $I = \bigcap_l \mathcal{P}_i$ stand for a reduced primary decomposition and set $P_i = \mathcal{P}_i$.

(a) Let $P \in \mathrm{Ass}(R/I)$ be an associated prime of R/I. Say, $P = I : (x)$, for some $x \in R \setminus I$ (*cf.* Definition 2.5.17). Then $P = \bigcap_i (\mathcal{P}_i : (x))$. Note that $\mathcal{P}_i : (x)$ is again P_i-primary if $x \notin \mathcal{P}_i$, else it is $(1) = R$. Thus, passing to radicals, P is the intersection of a (necessarily, nonempty) finite subset of the set $\{P_i\}_i$. Therefore, P must coincide with one of these prime ideals.

Conversely, let P denote the radical of a primary component. In order to show that $P \in \mathrm{Ass}(R/I)$, it suffices to show that $P_P \in \mathrm{Ass}(R_P/I_P)$. Changing notation, one can now assume that R is local, with unique maximal ideal $\mathfrak{m}$, and $I \subset \mathfrak{m}$ admits a reduced primary decomposition with an $\mathfrak{m}$-primary component $\mathcal{M}$. One wishes to show that $\mathfrak{m} \in \mathrm{Ass}(R/I)$.

Now, the radical of any other primary component is a prime ideal contained in $\mathfrak{m}$. Let $x \in \mathfrak{m} \setminus \mathcal{M}$ be an element contained in every other primary component, a choice granted by the reduced nature of the primary decomposition. Then $I : (x) = \mathcal{M} : (x)$, hence $I : (x)$ is $\mathfrak{m}$-primary. By Proposition 2.5.18(i), there is an element $y \in \mathfrak{m}$ such that $I : (y)$ is an associated prime of R/I. But then $I : (y)$ contains a power of $\mathfrak{m}$, so necessarily $I : (y) = \mathfrak{m}$. Therefore, $\mathfrak{m} \in \mathrm{Ass}(R/I)$, as was to be shown.

(b) Given $P \in \mathrm{Min}(R/I)$, localizing at P, clearly $I_P = \mathcal{P}_P$, where $\mathcal{P}$ denotes the corresponding primary component of the given primary decomposition. If $\mathcal{Q}$ is the P-primary component of another reduced primary decomposition, one must have the equality $\mathcal{P}_P = \mathcal{Q}_P$, locally of two P-primary ideals. It follows that they are also equal over R (*cf.* Proposition 2.1.4). □

Remark 2.6.4. It had been realized by Noether, if not earlier by Lasker, that the non-minimal primary components in a reduced primary decomposition of an ideal are not uniquely determined by the ideal. Even worse, to any embedded associated prime of R/I there usually correspond infinitely many distinct primary components. Noether gave the following simple example on a footnote of her paper: $I = (X^2, XY) \subset k[X, Y]$ (k an infinite field). Then $I = (X) \cap (X^2, Y + aX)$ is a reduced primary decomposition for any $a \in k$.

2.7 Hilbert characteristic function

2.7.1 Basics on the underlying graded structures

A more comprehensive treatment of graded structures will be considered in Chapter 7. Here, one focus on the following special setup: $R := k[x_0, \dots, x_n]$ stands for a polyno-

mial ring over a field k. One endows R with a structure of graded ring, by which one means the decomposition

$$R = \bigoplus_{t\geq 0} R_t, \quad R_t = kx_0^t + kx_0^{t-1}x_1 + \cdots + kx_n^t \subset R.$$

The k-vector space R_t, spanned by the homogeneous polynomials of degree t, is called the tth graded part of R. An ideal $I \subset R$ is homogeneous if it can be generated by homogeneous polynomials or, equivalently, if $I = \bigoplus_{t\geq 0} I_t$, where $I_t := I \cap R_t$.

Often a homogeneous polynomial of degree t will be called a t-form. Given a homogeneous ideal I, an important related degree is the initial degree of I, defined to be the least $t \geq 0$ such that $I_t \neq 0$.

Perhaps the first feature of homogeneous ideals is that the property of being prime or primary can be verified solely by using homogeneous test elements.

Lemma 2.7.1. *Let $I \subset R$ denote a homogeneous ideal. Then I is prime (resp., primary) if given homogeneous elements $f, g \in R$ such that $fg \in I$ then either $f \in I$ or else $g \in I$ (resp., $g^\ell \in I$, for some $\ell \geq 1$).*

Proof. One proves the case of a prime ideal, leaving the case of a primary ideal to the reader as being similarly handled. Here, one argues with the initial degree of a polynomial. Let $f, g \in R$ such that $f \in I$ nor $g \in I$. Write $f = f_u + \cdots$, $g = g_v + \cdots$, with $f_u \neq 0$, $g_v \neq 0$. Let f_{u+u_0} and g_{v+v_0} denote the respective first homogeneous constituents not belonging to I. By assumption on homogeneous test elements, one has $f_{u+u_0}g_{v+v_0} \notin I$. By homogeneity of I, it follows that

$$(f - (f_u + \cdots + f_{u+u_0-1}))(g - (g_v + \cdots + g_{v+v_0-1})) \notin I.$$

But since by construction, $f - (f_u + \cdots + f_{u+u_0-1})$ and $g - (g_v + \cdots + g_{v+v_0-1})$ belong to I, necessarily $fg \notin I$, as was to be shown. □

One next collects the main operationwise properties of homogeneous ideals.

Proposition 2.7.2. *Let I, J denote homogeneous ideals of R. Then:*
(i) *(I, J), IJ and $I \cap J$ are homogeneous.*
(ii) *$I : J$ is homogeneous.*
(iii) *$\sqrt{I}$ is homogeneous.*

Proof. (i) The first two are obvious. For the intersection, note that, for any integer $t \geq 0$, one has $(I \cap J)_t = I_t \cap J_t$.

(ii) Take a finite set $\{g_1, \ldots, g_m\}$ of homogeneous generators of J. Given $f \in I : J$, write $f = \sum_i f_j$, with f_i homogeneous of degree i and consider the products $f_i g_j$, for a fixed j. Since these are forms of different degrees and I is homogeneous, then $f_i g_j \in I$ for every i. Since j was arbitrarily fixed, one has $f_i J \subset I$ for every i, thus showing that $f_i \in I : J$ for every i. Therefore, $I : J$ is generated by forms.

(iii) Letting $f \in \sqrt{I}$, write $f = f_u + f_{u+1} + \cdots$, with $f_u \neq 0$. By definition, $f^\ell \in I$ for some integer $\ell \geq 1$. Clearly, $f^\ell = {f_u}^\ell +$ terms of degree $> u\ell$. By a similar token as in (ii), one has ${f_u}^\ell \in I$, hence $f_u \in \sqrt{I}$. But now $f - f_u \in I$ and one can proceed by iteration to prove that all the homogeneous constituents of f belong to $\sqrt{I}$. □

Note that, as a consequence of (iii) above, if $\wp \subset$ is a prime ideal and $\mathfrak{P}$ is a homogeneous $\wp$-primary ideal then $\wp$ is homogeneous as well. By a mix of the arguments in (ii) and (iii) above, the reader will find rewarding to prove, more generally, the following.

Lemma 2.7.3. *Let $I \subset R$ denote a homogeneous ideal. Then any associated prime $\wp$ of R/I is the annihilator of a homogeneous element. In particular* (*by* (ii) *of the above proposition*)*, $\wp$ is homogeneous.*

One is actually interested in a sort of weak converse. To wit, since R is a Noetherian, any homogeneous ideal $I \subset R$ in particular admits a reduced primary decomposition. It is natural to ask whether one can always find a primary decomposition of I whose components are homogeneous ideals as well. Note that a reduced primary decomposition has a rigid (uniquely defined) part, hence this part would have to be a priori homogeneous. This is in fact the case, but it does not follow automatically from the original argument of Noether (Proposition 2.6.2 (1)).

For that, one needs the following notion: for any ideal $J \subset R$, let $J^* \subset J$ denote the ideal generated by all homogeneous elements of J. Clearly, J^* is the largest homogeneous ideal contained in J. This notion and its uses make sense in a more encompassing graded environment.

Lemma 2.7.4. *Let $J \subset R$ denote an ideal. Then:*

(i) *If J is a prime* (*resp., primary*) *ideal then so is J^*.*

(ii) *If J is homogeneous with primary decomposition $J = \cap \mathfrak{P}_i$ then $J = \cap \mathfrak{P}_i^*$, with homogeneous primary components.*

Proof. (i) By Lemma 2.7.1, it suffices to test for forms f, g. If $fg \in J^*$, then either $f \in J$ or $g \in J$ since J is prime. Since f, g are forms, then $f \in J^*$ or $g \in J^*$.

The argument in the case of a primary ideal is similar.

(ii) By (i), each $\mathfrak{P}_i^*$ is a primary ideal. Obviously, $\cap \mathfrak{P}_i^* \subset \cap \mathfrak{P}_i = J$. Conversely, since $J \subset \mathfrak{P}_i$ is homogeneous then $J \subset \mathfrak{P}_i^*$. □

Since the minimal primary components of a homogeneous ideal are uniquely defined then they must be homogeneous. Moreover, the radicals of the primary components are uniquely defined. Finally, if it happens that $\cap \mathfrak{P}_i^*$ fails to be a reduced primary decomposition, then one can always derive a reduced one by disregarding superficial components (necessarily embedded). Thus, in the sequel, one will refer to a *reduced homogeneous primary decomposition* of the homogeneous ideal I in the sense that it is reduced and the primary components are homogeneous.

Remark 2.7.5. It is interesting to note that in his book ([112]) Nagata takes another approach to homogeneous primary decompositions, drawing upon the notion of idealization.

A question arises as to whether there is a natural bridge between arbitrary ideals and homogeneous ideals of the polynomial ring $R = k[x_0, \dots, x_n]$ other than the operation $I^* \subset I$ above. The answer, given by the process of homogenization and dehomogenization, still draws on that operation.

Namely, set $\overline{R} := R/(x_0 - 1) \simeq k[x_1, \dots, x_n]$, a polynomial ring in one less variable. Given any ideal $I \subset R$, let $\overline{I} = (I, x_0 - 1)/(x_0 - 1) \subset \overline{R}$ denote its image by the canonical ring homomorphism $\pi : R \twoheadrightarrow \overline{R}$. It is clear that $\overline{I}$ is obtainable by setting x_0 to 1 in the elements of a set of generators of I. When I is in particular homogeneous, $\overline{I}$ is called its *dehomogenized* ideal.

Conversely, given an ideal $J \subset \overline{R}$, let $\mathfrak{h}(J) := (\pi^{-1}(J))^* \subset \pi^{-1}(J)$. Clearly, $\mathfrak{h}(J)$ is the ideal of all forms $f \in R$ such that $\pi(f) \in J$. This ideal is called the *homogenized* ideal of J. It can be obtained in quite an effective way by means of the usual process of homogenizing an individual polynomial using an extra variable. Recall this procedure: given $f \in k[x_1, \dots, x_n]$ of total degree d, let

$$^h f := x_0^d f(x_1/x_0, \dots, x_n/x_0) \in R,$$

which is clearly a homogeneous polynomial of degree d.

The following operation properties take place.

Lemma 2.7.6. *For any $f_1, f_2 \in k[x_1, \dots, x_n]$, one has:*

(1) $^h(f_1 f_2) = {}^h f_1 \cdot {}^h f_2$

(2) $x_0^{d_1+d_2} .^h (f_1 + f_2) = x_0^d (x_0^{d_2} .^h f_1 + x_0^{d_1} .^h f_2)$, *where d_1, d_2, d are the total degrees of f_1, f_2 and $f_1 + f_2$, respectively.*

Proof. (1) This is straightforward.

(2) One can assume that $d_1 \geq d_2$. If $d_1 > d_2$, then $d = d_1$. Set $\widetilde{X} = \{x_1/x_0, \dots, x_n/x_0\}$ for short. Then

$$^h(f_1 + f_2) = x_0^{d_1}(f_1 + f_2)(\tilde{X}) = x_0^{d_1} f_1(\widetilde{X}) + x_0^{d_1 - d_2} x_0^{d_2} f_2(\widetilde{X}) = {}^h f_1 + x_0^{d_1 - d_2} .^h f_2.$$

Multiplying throughout by $x_0^{d_1+d_2}$ yields the desired expression.

If $d_1 = d_2$, then $d \leq d_1$. Then

$$\begin{aligned} x_0^{d_1+d_2} .^h (f_1 + f_2) &= x_0^{2d_1} .^h (f_1 + f_2) = x_0^{2d_1} x_0^d (f_1 + f_2)(\tilde{X}) \\ &= x_0^{d_1+d} \big(x_0^{d_1} f_1(\widetilde{X}) + x_0^{d_2} f_2(\widetilde{X})\big) = x_0^d (x_0^{d_2 h} f_1 + x_0^{d_1 h} f_2), \end{aligned}$$

which is the required expression for this case. □

Proposition 2.7.7. *Let $J = (f_1, \dots, f_m) \subset k[x_1, \dots, x_n]$ denote an ideal and one of its finite sets of generators. Then $\mathfrak{h}(J) = ({}^h f_1, \dots, {}^h f_m) : (x_0)^\infty$.*

Proof. First, note that $({}^hf_1, \dots, {}^hf_m)$ is a homogeneous ideal of R and is contained in $\mathfrak{h}(J)$. Next, any power of x_0 is homogeneous, hence the saturation $({}^hf_1, \dots, {}^hf_m) : (x_0)^\infty$ is a homogeneous ideal by Proposition 2.7.2; moreover, if f is a homogeneous element in this saturation then clearly $\pi(f) \in \pi(({}^hf_1, \dots, {}^hf_m)) = J$. Therefore, one has an inclusion $({}^hf_1, \dots, {}^hf_m) : (x_0)^\infty \subset \mathfrak{h}(J)$.

Conversely, let $f \in \mathfrak{h}(J)$ be a form and set $f_0 := \pi(f)$ for the result of evaluating f at $x_0 \mapsto 1$. Then $f = (x_0{}^s)^h f_0$ for suitable $s \geq 0$. Now, $f_0 \in J$, hence $f_0 = \sum_{i+1}^m g_i f_i$, for certain $g_i \in k[x_1, \dots, x_n]$. Applying Lemma 2.7.6, a sufficiently high power of x_0 will land f into $({}^hf_1, \dots, {}^hf_m)$. □

Because of this proposition, it makes sense to use the alternative notation ${}^hJ$ for the homogenized of J. This ideal can be recovered from a slightly different construction to be now described.

Start with the localization R_{x_0} and the structural map $R \to R_{x_0}$, which is injective since R has no proper zero-divisors. The natural grading of R induces a fractional grading on R_{x_0} by setting $\deg(f/x_0^r) = \deg(f) + r$ for a homogeneous $f \in R$. The homogeneous elements of degree 0 in this grading constitute the subring $k[x_1/x_0, \dots, x_n/x_0]$, which is a k-polynomial ring since the elements $x_1/x_0, \dots, x_n/x_0$ of the field of fractions of R are algebraically independent over k. Thus, abstractly, $k[x_1/x_0, \dots, x_n/x_0]$ and $\overline{R}$ are isomorphic k-algebras, but one can do a little better by taking some natural identification. Namely, the natural surjection $R \twoheadrightarrow \overline{R}$ induces a homomorphism $R_{x_0} \to \overline{R}$ whose restriction to $k[x_1/x_0, \dots, x_n/x_0]$ is an isomorphism onto $\overline{R}$. The inverse maps x_i to x_i/x_0. Given an ideal $J \subset \overline{R}$, one takes its image in $k[x_1/x_0, \dots, x_n/x_0] \subset R_{x_0}$ and contracts back to R.

The reader will find it rewarding, using the properties of contraction in rings of fractions, to show that the resulting ideal is again the homogenized ideal ${}^hJ$.

The main go-between properties of this procedure are collected next.

Proposition 2.7.8. *Notation as above. The ring homomorphism $\pi : R \twoheadrightarrow \overline{R}$ and the homogenization assignment $\mathfrak{h} : \overline{R} \rightsquigarrow R$ establish a bijection between the family of homogeneous ideals of R modulo which x_0 is regular and the family of all ideals of $\overline{R}$. Moreover, this bijection respects inclusion, intersection, primeness, primariness, radical and reduced primary decompositions.*

Proof. Most properties are easily verified. For example, one gets $\pi(\mathfrak{h}(J)) = J$ for an arbitrary ideal $J \subset \overline{R} = k[x_1, \dots, x_n]$ and $x_0^r \mathfrak{h}(\pi(I)) \subset I \subset \mathfrak{h}(\pi(I))$, for some $r \geq 0$. This establishes the stated bijection.

The preservation of the stated features is also routinely verified and is left to the reader. As to the primary decomposition, coming from a homogeneous ideal $I \subset R$ one assumes that all primary components are homogeneous; then the primary decomposition of $\pi(I)$ is obtained by striking out the image of any primary component of I containing a proper power of x_0. □

2.7.2 First results

Clearly, the residue ring R/I inherits same sort of grading as R, where $(R/I)_t = R_t/I_t$. Therefore, as k-vector spaces,

$$\dim_k(R/I)_t = \dim_k R_t - \dim_k I_t = \binom{t+n}{n} - \dim_k I_t.$$

Thus, the vector dimensions of $(R/I)_t$ and I_t differ by a known number, hence they are theoretically and computationally fairly interchangeable.

Definition 2.7.9. Let $I \subset R$ denote a homogeneous ideal. The *Hilbert function* of R/I is the numerical function

$$H(R/I, \_) : \mathbb{N} \longrightarrow \mathbb{N}, \quad t \mapsto \dim_k(R/I)_t.$$

In particular, $H(R,t) = \binom{n+t}{t}$ for every $t \geq 0$. This notion is attached to a graded ring, but it is customary to extend it to graded modules, which includes homogeneous ideals. For this reason, one frequently defines the Hilbert function of the ideal I:

$$H(I,t) := \dim_k I_t = \binom{t+n}{n} - H(R/I,t).$$

Clearly, as already observed, the two are interchangeable.

Classically, side wise with the Hilbert function one also talks about the *Hilbert series* of R/I as the generating function of $H(R/I, \_)$. It will be denoted $H_{R/I}(t)$. Thus, $H_{R/I}(t) = \sum_{i\geq 0} H(R/I,t)t^i$. It can be shown that it is a rational function in t, whose denominator is $(1-t)^d$, where $d = \dim R/I$. The numerator is a polynomial that can be written down as soon as one knows the minimal free resolution (Proposition 7.4.11) of R/I over R. The Hilbert series will be considered in more detail in the general case of graded modules (Section 7.4.2).

An important feature of combinatorics is the fact that

$$\binom{t+n}{n} = \frac{1}{n!}t^n - \frac{1}{n!}\binom{n+1}{2}t^{n-1} + \text{lower order terms in } t, \tag{2.7.9.1}$$

a polynomial expression in t of order n and with coefficient of the higher order term equal to $1/n!$. The following example throws further light on this matter.

Example 2.7.10. Let $f \in R$ denote a form of degree $d \geq 1$. Then

$$H(R/(f),t) = \begin{cases} \binom{t+n}{n} & \text{if } t < d \\ \binom{t+n}{n} - \binom{t-d+n}{n} & \text{if } t \geq d \end{cases} \tag{2.7.10.1}$$

To prove the above, one may assume that $t \geq d$ as otherwise $I_t = \{0\}$. In this case, multiplication by f gives an injective k-vector space map $R_{t-d} \to R_t$ with cokernel $R_t/fR_{t-d} = (R/(f))_t$.

As a final touch on this example, one notes that, for $t \geq d$,

$$\begin{aligned}\binom{t+n}{n} - \binom{t-d+n}{n} &= \frac{1}{n!}t^n + a_1 t^{n-1} + \cdots \\ &\quad - \left(\frac{1}{n!}(t-d)^n + a_1(t-d)^{n-1} + \cdots\right) \\ &= \frac{1}{n!}\left(t^n - (t-d)^n\right) + a_1\left(t^{n-1} - (t-d)^{n-1}\right) + \cdots \\ &= \frac{d}{(n-1)!}t^{n-1} + \text{lower order terms in } t,\end{aligned}$$

also a polynomial expression in t, this time around of degree $n - 1 = \dim R/(f)$ and leading coefficient $d/(n-1)!$, where $d = \deg f$.

One of the most basic properties of the Hilbert function is the following.

Proposition 2.7.11. *With the above notation, suppose that the ring R/I has a homogeneous nonzero divisor of degree* 1.

(1) $H(R/I, t) \leq H(R/I, t+1)$ *for every* $t \geq 0$.

(2) *If* $H(R/I, r) = H(R/I, r+1)$ *for some* $r \geq 0$, *then this equality holds true for any value* $t \geq r$.

Proof. (1) Let $f \in R$ denote a form of degree 1 which is a nonzero divisor modulo I. Multiplication by f induces a k-vector space map $(R/I)_t \to (R/I)_{t+1}$ which is injective.

(2) Supposing $H(R/I, t) = H(R/I, t+1)$, the map above forces the equality $(R/I)_{t+1} = \overline{f}(R/I)_{t+1}$, where $\overline{f}$ denotes the residue of f modulo I. It suffices to prove the same sort of equality in the next degree. Thus, given $F \in R_{t+2}$, write $F = \sum_{i=1}^{n} x_i F_i$, for certain forms $F_i \in R_{t+1}$. By assumption, $\overline{F_i} = \overline{f}\,\overline{G_i}$ for every $1 \leq i \leq n$ and certain $G_i \in R_t$. Substituting and expanding yields $\overline{F} = \overline{f}(\overline{F_0} + \overline{x_1}\,\overline{G_1} + \cdots + \overline{x_n}\,\overline{G_n})$, as was to be shown. □

Remark 2.7.12. If k is an infinite field, the hypothesis of the proposition means that the maximal ideal $(x_1, \ldots, x_n)$ is not an associated prime of R/I. Equivalently, $I : (x_1, \ldots, x_n) = I$, a condition that allows to transfer the issue to nonhomogeneous ideals in one variable less.

2.7.3 More advanced steps

Two natural questions arise: the first is as to whether there is some sort of inductive construction to express $H(R/I, t)$; the second, as to whether there is an expression of $H(R/I, t)$ as a polynomial whose coefficients are rational numbers, provided $t \gg 0$. It turns out that both were affirmatively answered by Hilbert in [72] and subsequently considered by various authors, culminating with Serre's reformulation of the theory in terms of the general setup of finitely generated graded modules over a standard graded ring over an Artinian ground ring.

The method of Hilbert draws on the finite graded resolution of R/I over R along with an additive property of $H(R/I,t)$ that is piecewise like the elementary kernel-cokernel calculation of vector dimensions (see the notion of a short exact sequence of modules in Chapter 3). It has the advantage of calculating $H(R/I,t)$ in terms of free graded modules only, avoiding the general notion of a graded module; its drawback is that it only proves the existence of an asymptotic polynomial in the case where R/I admits a finite graded resolution over R.

The method of Serre is based on an inductive procedure using associated primes—this is the approach currently in use and is presented in Section 7.4. It excels in generality, but the method of proofs is not automatically suited for computation, requiring rather sophisticated algorithms.

In this part, the approach is historically intermediary between the above two paths, where one follows closely Lasker ([101, Kapitel II]) and van der Waerden ([154], [155, Section 4]), which is a modern update of Hilbert–Lasker work.

Proposition 2.7.13 (Hilbert). *Let $I,J \subset R$ be homogeneous ideals. Then*

$$H\big(R/(I,J),t\big) = H(R/I,t) + H(R/J,t) - H(R/I\cap J,t),$$

for $t \geq 0$.

Proof. Consider the direct sum $I_t \oplus J_t$ of k-vector spaces and the natural k-linear map $I_t \oplus J_t \to (I,J)_t$ defined by $(f,g) \mapsto f+g$. This map is clearly surjective and it is immediate that the image of the k-linear diagonal map $(I\cap J)_t \to I_t \oplus J_t, f \mapsto (f,-f)$, coincides with the kernel of the previous surjective map.

Therefore, one has $H((I,J),t) = H(I,t) + H(J,t) - H(I\cap J,t)$. It easily follows that

$$H\big(R/(I,J),t\big) = H(R/I,t) + H(R/J,t) - H(R/I\cap J,t),$$

as required. □

Remark 2.7.14. One notes that all maps in the above proof actually come from module maps by taking the homogeneous t-parts. In fact, anticipating the terminology of exact sequences, one has the two short exact sequences of R-modules

$$0 \to I\cap J \longrightarrow I\oplus J \longrightarrow (I,J) \to 0$$

and

$$0 \to R/I\cap J \longrightarrow R/I \oplus R/J \longrightarrow R/(I,J) \to 0.$$

These are useful while considering a more general context of Hilbert functions.

The next result is a useful inductive procedure and generalizes Example 2.7.10.

Proposition 2.7.15 (Lasker). *Let $I \subset R$ denote a homogeneous ideal and let $f \in R$ stand for a d-form which is regular on R/I. Then*

$$H\big(R/(I,f),t\big) = H(R/I,t) - H(R/I,t-d).$$

Proof. Since f is regular modulo I, one has $I \cap (f) = If$. It follows that $H(I \cap (f),t) = H(I,t-d)$.

On the other hand, as argued in Example 2.7.10, $H((f),t) = \binom{t-d+n}{n}$. By these two observations and Proposition 2.7.13,

$$\begin{aligned} H\big(R/(I,f),t\big) &= H(R/I,t) + H\big(R/(f),t\big) - H\big(R/I \cap (f),t\big) \\ &= H(R/I,t) + H\big((f),t\big) - H\big(I \cap (f),t\big) \\ &= H(R/I,t) - \binom{t-d+n}{n} + H(I,t-d) \\ &= H(R/I,t) - H(R/I,t-d), \end{aligned}$$

as required. □

Taking $I = \{0\}$ above and expanding, one finds

$$\begin{aligned} H\big(R/(f),t\big) &= \binom{t+n}{n} - \binom{t-d+n}{n} \\ &= \frac{1}{n!}\big((t+n)(t+n-1)\cdots(t+1) - (t-d+n)(t-d+n-1)\cdots(t-d+1)\big) \\ &= \frac{1}{n!}\left(\binom{n+1}{2} - \left(-nd + \binom{n+1}{2}\right)\right)t^{n-1} + \text{lower order terms} \\ &= \frac{d}{(n-1)!}t^{n-1} + \text{lower order terms} \end{aligned}$$

More generally, one has the following.

Proposition 2.7.16. *Let $\{f_1,\dots,f_m\} \subset R$ be forms of respective degrees $d_1,\dots,d_m$ forming a regular sequence. Then*

$$H\big(R/(f_1,\dots,f_m)\big) = \frac{d_1\cdots d_m}{(n-m)!}t^{n-m} + \textit{lower order terms.}$$

Proof. One inducts on m.

The case where $m = 1$ is provided by the above calculation. Assume $m > 1$. Applying Proposition 2.7.15 with $I = (f_1,\dots,f_{m-1})$ and the inductive hypothesis yields

$$\begin{aligned} H\big(R/(f_1,\dots,f_m),t\big) &= H\big(R/(I,f_m),t\big) = H(R/I,t) - H(R/I,t-d_m) \\ &= \frac{d_1\cdots d_{m-1}}{(n-m+1)!}\big(t^{n-m+1} - (t-d_m)^{n-m+1}\big) + \text{LOT} \end{aligned}$$

$$= \frac{d_1 \cdots d_{m-1}}{(n-m+1)!}(n-m+1)d_m t^{n-m} + \text{LOT}$$
$$= \frac{d_1 \cdots d_m}{(n-m)!} t^{n-m} + \text{LOT},$$

where LOT denotes "lower order terms." □

One observes that in the examples so far, for $t \gg 0$ one has

$$H(R/I, t) = \frac{e_0}{r!} t^r + \text{lower order terms},$$

where $r = \dim R/I - 1$ and e_0 is a nonnegative integer. This raises the question as to whether there is a general pattern here. In fact, we have the following.

Theorem 2.7.17 (Hilbert–Lasker). *Let $I \subset R$ denote a homogeneous ideal. Then*

$$H(R/I, t) = e_0 \binom{t}{r} + e_1 \binom{t}{r-1} + \cdots + e_r, \tag{2.7.17.1}$$

for $t \gg 0$, where $r := \dim R/I - 1$, the e_i's are integers and $e_0 \geq 0$.

Proof. One doubly inducts on $r \geq -1$ and the number $s \geq 1$ of primary components in a reduced homogeneous primary decomposition of I.

For $r = -1$, $\dim R/I = 0$, hence I is an $\mathfrak{m}$-primary ideal, where $\mathfrak{m} = (x_0, \ldots, x_n)$. Let $\ell \geq 1$ be an integer for which $\mathfrak{m}^\ell \subset I$. This gives a surjection of k-vector spaces $R_t/\mathfrak{m}_t \twoheadrightarrow R_t/I_t$ for all $t \geq \ell$, thus implying that $H(R/I, t) = 0$ for $t \geq \ell$. By convention, $\binom{t}{-s} = 0$ for $t \geq 0$ and $s \leq -1$. For a later reason, one sets $e_0 = \lambda(R/I) := \dim_k(R_{\leq t}/I_{\leq t})$, for $t \gg 0$ (where λ denotes length to be introduced in Section 3.1.2).

For $s = 1$ and $r \geq 0$, the ideal I is $\wp$-primary, for some prime ideal $\wp$. By the previous argument, $\wp \subsetneq \mathfrak{m}$. Pick a linear form $l \in \mathfrak{m} \setminus \wp$. Clearly, l is regular on R/I, so applying Proposition 2.7.15 yields

$$H(R/(I, l), t) = H(R/I, t) - H(R/I, t-1). \tag{2.7.17.2}$$

Since $\dim R/(I, l) = \dim R/I - 1$, by the inductive hypothesis one has

$$H(R/(I, l), t) = e_0 \binom{t}{r-1} + e_1 \binom{t}{r-2} + \cdots + e_{r-1},$$

for, say, $t \geq t_0$, where $e_0 \geq 0$. Applying (2.7.17.2) recursively, one has

$$H(R/I, t) - H(R/I, t_0) = a_0 \left[\binom{t+1}{r} - \binom{t_0+1}{r} \right] + a_1 \left[\binom{t+1}{r-1} - \binom{t_0+1}{r-1} \right] + \cdots + a_{r-1}(t - t_0)$$

Collecting coefficients, using the known formula $\binom{t+1}{h} = \binom{t}{h} + \binom{t}{h-1}$, and passing the fixed term $H(R/I, t_0)$ to the right-hand side, yields the required expression.

Assume now that $r \geq 0$ and $s \geq 2$, *i. e.*, $\dim R/I \geq 1$ and I has at least two distinct primary components. Say, $I = \mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_s$. By Proposition 2.7.13, one has

$$H(R/I,t) = H(R/\mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_{s-1},t) + H(R/\mathfrak{P}_s,t) - H\big(R/(\mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_{s-1},\mathfrak{P}_s),t\big)$$

By the double inductive hypothesis, the first two summands on the right-hand side have the required form with nonnegative respective leading coefficients.

As to the last summand, one has $\dim R/\mathfrak{P}_j \leq \dim R/I$ for every j. On the other hand, $\mathfrak{P}_s$ is not contained in any associated prime of $R/(\mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_{s-1})$. By prime avoidance (Lemma 2.5.22), one can pick an element $a \in \mathfrak{P}_s$ which is regular modulo $\mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_{s-1}$. By Proposition 2.5.19 and Proposition 2.5.33, it then follows that

$$\dim R/(\mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_{s-1},\mathfrak{P}_s) \leq \dim R/(\mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_{s-1},a) \leq \dim R/I - 1.$$

Therefore, by the inductive hypothesis, $H(R/(\mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_{s-1},\mathfrak{P}_s),t)$ has the required form, in particular its rth term has null coefficient. Thus, $H(R/I,t)$ has the required form with nonnegative leading exponent. □

Definition 2.7.18. The polynomial obtained in (2.7.17) is called the *Hilbert polynomial* of R/I.

Note that this polynomial is an invariant of R/I since it coincides with its Hilbert function for any sufficiently high value of the latter. Yet, the polynomial itself can be represented in other combinatorial forms with rational coefficients. However, of course, its leading coefficient as such is well determined, justifying the following.

Definition 2.7.19. The leading coefficient e_0 of the Hilbert polynomial of R/I is called its *degree* (or *multiplicity*) of R/I.

By abuse, if no confusion arises, one often refers to e_0 as the multiplicity of the ideal I. The other coefficients may depend on the specific combinatorial shape, and as the latter is a property common to any polynomial over the rationals taking integer values, one cannot expect a strong uniqueness of the other coefficients in terms of the invariants of R/I. Often they are called the *Hilbert coefficients* of R/I, but this has a certain amount of looseness. For example, the Hilbert polynomial can also be written in the form

$$a_0\binom{t+r}{r} - a_1\binom{t+r-1}{r-1} + \cdots + (-1)^r a_r,$$

with $a_0 = e_0$, in which case the coefficients are often called the normalized Hilbert coefficients of R/I.

Example 2.7.20. The case of a regular sequence is one of a few large classes of ideals where one can express the Hilbert coefficients in terms of the degrees of the given forms. Namely, let $d_1,\ldots,d_m$ de the degrees of m forms in regular sequence. Then

$$
\begin{aligned}
e_0 &= d_1 \cdots d_m \text{ as was seen in Proposition 2.7.16} \\
e_1 &= -\frac{1}{2}\prod_{i=1}^{m} d_i\left(\sum_{i=1}^{m} d_i - 2n + m\right) \\
&\vdots \\
e_l &= \binom{n}{r+m} - \sum_{i=1}^{m}\binom{n-d_i}{r+m} + \mathfrak{T},
\end{aligned}
$$

where $\mathfrak{T}$ denotes a sum of other similar numbers involving sums of d_i's. The proof of the general formula can be obtained by induction on m. Note that the actual sign of e_l may depend on the given data. It is not totally obvious how the values of e_0, e_1 derive from the general formula. In fact, it is not clear how useful such a formula might turn out to be.

One can further exploit the bearing of a primary decomposition.

Lemma 2.7.21. *Let $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_s\}$ denote the primary components of maximal dimension of a homogeneous ideal $I \subset R$. Then*

$$e_0(R/I) = \sum_{i=1}^{s} e_0(R/\mathfrak{P}_i).$$

Proof. The assumption is that $\dim R/\mathfrak{P}_i = \dim R/I$ for every $1 \le i \le s$, but $\dim R/\mathfrak{Q}_j < \dim R/I$ for any other component of I in a reduced primary homogeneous decomposition of I. Set $\mathfrak{P} = \bigcap_{i=1}^{s} \mathfrak{P}_i$ and let $I = \mathfrak{P} \cap \mathfrak{Q}$ stand for a reduced homogeneous primary decomposition of I, where $\mathfrak{Q}$ denotes the intersection of all primary components of smaller dimension than R/I. Then

$$H(R/I, t) = H(R/\mathfrak{P}, t) + H(R/\mathfrak{Q}, t) - H\big(R/(\mathfrak{P}, \mathfrak{Q})\big)$$

by Proposition 2.7.13.

Note that $\dim R/\mathfrak{Q} < \dim R/I$ and $\dim R/(\mathfrak{P}, \mathfrak{Q}) < \dim R/I$ by the same token as the proof of Theorem 2.7.17. Therefore, for $t \gg 0$ making all terms above coincide with the respective Hilbert polynomials, then the degree and leading term of the left-hand side polynomial is given by the degree and leading term of the left-most summand on the right-hand side. Thus, $e_0(R/I) = e_0(R/\mathfrak{P})$, hence one can assume that I has only primary components of maximal dimension.

Repeating the procedure,

$$H(R/I, t) = H\left(R/\bigcap_{i=1}^{s-1}\mathfrak{P}_i, t\right) + H(R/\mathfrak{P}_s, t) - H\left(R/\left(\bigcap_{i=1}^{s-1}\mathfrak{P}_i, \mathfrak{P}_s\right), t\right)$$

and again $\dim R/(\bigcap_{i=1}^{s-1}\mathfrak{P}_i, \mathfrak{P}_s) < \dim R/I$. Thus, one is done by induction on s. □

Remark 2.7.22. The ideal $\bigcap_{i=1}^{s} \mathfrak{P}_i$ is called the *unmixed part* of I. The above result says that the degree of I is insensitive to components of smaller dimension in a homogeneous primary decomposition of I.

2.7.4 The formula of van der Waerden

In this part, one derives the formula established by van der Waerden, based on earlier ideas of Lasker. Although the method will be superseded by the later developments of Part II in this book, the tools allow for diving in certain aspects of polynomial theory that seems worth for the newcomer's familiarization.

Note that if $P \subset R$ is a minimal prime ideal of R/I then the localization R_P/I_P is an Artinian ring (Theorem 2.5.14). Therefore, it admits a composition series by Section 3.1.2, and hence has finite length $\lambda(R_P/I_P) < \infty$.

Take a composition series of R_P/I_P and lift to a chain of P-primary ideals

$$I = I_1 \subset I_2 \subset \cdots \subset I_\lambda = P,$$

where $\lambda = \lambda(R_P/I_P)$.

If all I_i's were homogeneous, one could show that $e_0(I_i) = e_0(I_{i+1}) + e_0(P)$, for $i = 1, \ldots, \lambda - 1$. Unfortunately, it is not clear how to guarantee the existence of such a particular chain of P-primary ideals series coming from a composition series of R_P/I_P. Thus, one needs a subtler procedure drawing upon the previous notion of homogenization (Section 2.7.1).

Using the notation in *loc. cit.*, set $\overline{R} = k[x_1, \ldots, x_n] \simeq R/(x_0 - 1)$. Let $\wp \in \overline{R}$ denote a prime ideal such that $\dim \overline{R}/\wp > 0$. Up to a change of variables, one can assume that the image of $x_1 \bmod \wp$ is transcendental over k or, in other words, that $\wp \cap k[x_1] = \{0\}$. Now, consider an additional variable y over $\overline{R}$ and the ideal $(\wp, x_1 - y) \subset k[x_1, \ldots, x_n][y]$. Clearly, this is a prime ideal since

$$k[x_1, \ldots, x_n][y]/(\wp, x_1 - y) \simeq k[x_1, \ldots, x_n]/\wp.$$

Then the extended ideal $(\wp, x_1 - y)k(y)[x_1, \ldots, x_n]$ is also prime. By a similar token, if $\mathfrak{Q} \subset \overline{R}$ is a $\wp$-primary ideal then $(\mathfrak{Q}, x_1 - y)k(y)[x_1, \ldots, x_n]$ is $(\wp, x_1 - y)k(y)[x_1, \ldots, x_n]$-primary.

In what follows, whenever one writes $(\wp, x_1 - y)$ (resp., $(\mathfrak{Q}, x_1 - y)$) is to be meant the ideal generated in the extended polynomial ring $\overline{R}(y) := k(y)[x_1, \ldots, x_n]$ over the purely transcendental extension $k(y)$.

More is true.

Lemma 2.7.23. *Fixing a $\mathfrak{p}$-primary ideal $\mathfrak{Q}$ in $\overline{R}$, the assignment $\mathfrak{Q}' \rightsquigarrow (\mathfrak{Q}', x_1 - y)$ establishes an inclusion preserving bijection between the family of $\wp$-primary ideals of $\overline{R}$ containing $\mathfrak{Q}$ and the family of $(\wp, x_1 - y)$-primary ideals of $\overline{R}(y)$ containing $(\mathfrak{Q}, x_1 - y)$. In particular, $k[x_1, \ldots, x_n]_\wp/\mathfrak{Q}_\wp$ and $k(y)[x_1, \ldots, x_n]_{(\wp, x_1 - y)}/(\mathfrak{Q}, x_1 - y)_{(\wp, x_1 - y)}$ have the same length.*

Proof. The proof is quite straightforward, with a word about the inverse map to the stated assignment. To wit, given a $(\wp, x_1 - y)$-primary ideal $\mathfrak{Q}''$ of $k(y)[x_1, \ldots, x_n]$ containing $(\mathfrak{Q}, x_1 - y)$, one takes $\mathfrak{Q}' := \mathfrak{Q}'' \cap k[x_1, \ldots, x_n]$, which is a $\wp$-primary ideal. Then $(\mathfrak{Q}', x_1 - y) \subset \mathfrak{Q}''$ and equality must hold since $\mathfrak{Q}'$ is the set of all polynomials of $\mathfrak{Q}''$ whose coefficients do not involve y. □

Set by analogy $R(y) := k(y)[x_0, \dots, x_n]$ and

$$\pi(y) : R(y) \twoheadrightarrow R(y)/(x_0 - 1) = \overline{R}(y) = k(y)[x_1, \dots, x_n]$$

for the natural surjective ring homomorphism. Since y is not changed by $\pi(y)$, one may denote $\overline{R(y)} := \overline{R}(y)$.

Lemma 2.7.24. *Let $P \subset R$ denote a homogeneous prime ideal of dimension ≥ 2 and let $\mathfrak{P} \subset R = k[x_0, \dots, x_n]$ a P-primary ideal, where one assumes that $x_1 \bmod P$ is transcendental over k. Let y denote a new variable as above and set $P' := (P, x_1 - yx_0) \subset R(y)$ and $\mathfrak{P}' := (\mathfrak{P}, x_1 - yx_0) \subset R(y)$, and let $\overline{P'} = \pi(y)(P') = (\pi(P), x_1 - y) \subset \overline{R(y)}$ and $\overline{\mathfrak{P}'} = \pi(y)(\mathfrak{P}') = (\pi(\mathfrak{P}), x_1 - y) \subset \overline{R(y)}$. Then $R_P/\mathfrak{P}_P$ and $R(y)_{\mathfrak{h}(\overline{P'})}/\mathfrak{h}(\overline{\mathfrak{P}'})_{\mathfrak{h}(\overline{P'})}$ have the same length.*

Proof. Note that one does not lose generality by assuming that $x_1 \bmod P$ is transcendental over k: since $\operatorname{trdeg}_k(R/P) = \dim R/P \geq 2$, up to change of variables one can actually assume that $\{x_0, x_1\}$ is part of a transcendence basis of R/P over k. The assertion follows from Lemma 2.7.23, but one has to be careful with the choices. By the choice made, in particular $x_0 \notin P$. Thus, x_0 is regular on R/P and also on $R/\mathfrak{P}$. By Proposition 2.7.8, the ideal $\pi(P) \subset \overline{R}$ is prime and $\pi(\mathfrak{P})$ is $\pi(P)$-primary. Moreover, $\dim \overline{R}/\overline{P} = \dim R/(P, x_0 - 1) \geq 1$, where $\overline{P} := \pi(P)$. Therefore, the discussion just before Lemma 2.7.23 shows that $\overline{P'} = (\overline{P}, x_1 - y)$ is a prime ideal of $\overline{R(y)}$ and $\overline{\mathfrak{P}'} = (\overline{\mathfrak{P}}, x_1 - y)$ is $\overline{P'}$-primary.

Using Proposition 2.7.8 in the reverse direction, $\mathfrak{h}(\overline{P'})$ is a prime ideal of $R(y) = k(y)[x_0, \dots, x_n]$ and $\mathfrak{h}(\overline{\mathfrak{P}'})$ is an $\mathfrak{h}(\overline{P'})$-primary ideal thereof. Thus, the contention makes sense and follows from Lemma 2.7.23. □

One is now ready for the main result of this part, often designated as the *associativity formula* or the *additivity formula* of multiplicities.

Theorem 2.7.25 (Lasker–Noether–van der Waerden). *Let $\{\mathfrak{P}_1, \dots, \mathfrak{P}_s\}$ denote the primary components of maximal dimension of a homogeneous ideal $I \subset R = k[x_0, \dots, x_n]$. Then*

$$e_0(R/I) = \sum_{i=1}^{s} \lambda(R_{P_i}/\mathfrak{P}_{i P_i}) e_0(R/P_i),$$

where $P_i = \sqrt{\mathfrak{P}_i}$ and $\lambda(\_)$ denotes length.

Proof. By Lemma 2.7.21, one can assume that I is P-primary for some homogeneous prime ideal $P \subset R$. As observed above, $\lambda(R_P/I_P) < \infty$. For mnemonic purpose, set $\mathfrak{P} := I$.

One argues by induction on the Krull dimension $\dim R/\mathfrak{P}$.

If $\dim R/\mathfrak{P} = 0$, then $\mathfrak{P}$ is $\mathfrak{m}$-primary, where $\mathfrak{m} = (x_0, \dots, x_n)$. In this case, the result is an immediate consequence of the conventionalized definition (see the proof of Theorem 2.7.17).

Since the zero-dimensional case is invisible in the inductive process, as well as in the geometric background, one proves the case where $\dim R/\mathfrak{P} = 1$ which is both algebraically and geometrically the first relevant (sic) situation.

As has been often employed before, up to a projective change of variables, one can assume that $x_0 \notin P$. Therefore, x_0 is regular on $R/\mathfrak{P}$, hence $\mathfrak{P} = \mathfrak{h}(\overline{\mathfrak{P}})$ by Proposition 2.7.8, where $\overline{\mathfrak{P}} = \pi(\mathfrak{P}) \subset \overline{R} = k[x_1, \dots, x_n]$ in the notation introduced above.

Now, one has $\overline{R}/\overline{\mathfrak{P}} \simeq R/(\mathfrak{P}, x_0 - 1)$ and since $\mathfrak{P}$ is homogeneous, $\dim \overline{R}/\overline{\mathfrak{P}} = 0$. That is, $\dim_k(\overline{R}/\overline{\mathfrak{P}}) < \infty$. Moreover, as fragments of Proposition 2.7.8 one has

$$H(R/\mathfrak{P}, t) = \dim_k(R_t/\mathfrak{P}_t) = \dim_k(\overline{R}_{\leq t}/\overline{\mathfrak{P}}_{\leq t}), \tag{2.7.25.1}$$

for all $t \geq 0$. But $H(R/\mathfrak{P}, t)$ coincides with the Hilbert polynomial of $R/\mathfrak{P}$ and $\dim_k(\overline{R}/\overline{\mathfrak{P}}) = \dim_k(\overline{R}_{\leq t}/\overline{\mathfrak{P}}_{\leq t})$, for all $t \gg 0$. In addition, since $\dim R/\mathfrak{P} = 1$ the Hilbert polynomial of $R/\mathfrak{P}$ coincides with the degree $e_0(R/\mathfrak{P})$. Thus, one concludes that $e_0(R/\mathfrak{P}) = \dim_k(\overline{R}/\overline{\mathfrak{P}})$. By the same token, one also has $e_0(R/P) = \dim_k(\overline{R}/\overline{P})$.

It remains to prove that $\dim_k(\overline{R}/\overline{\mathfrak{P}}) = \lambda(\overline{R}_{\overline{P}}/\overline{\mathfrak{P}}_{\overline{P}}) \dim_k(\overline{R}/\overline{P})$. One has the following.

Claim 1. Let $\mathfrak{Q} \subset \overline{R} = k[x_1, \dots, x_n]$ denote a $\mathfrak{n}$-primary ideal, $\mathfrak{n}$ a maximal ideal, and let $\mathfrak{Q}_1 = \mathfrak{Q} \subset \mathfrak{Q}_2 \subset \cdots \subset \mathfrak{Q}_\lambda = \mathfrak{n}$ denote a chain of primary ideals lifted from a composition series of $\overline{R}_{\mathfrak{n}}/\mathfrak{Q}_{\mathfrak{n}}$. Then $\mathfrak{Q}_{i+1}/\mathfrak{Q}_i \simeq \overline{R}/\mathfrak{n}$ for $1 \leq i \leq \lambda$.

One applies this claim to the above landscape, with $\mathfrak{n} = \overline{P}$ and $\mathfrak{Q} = \overline{\mathfrak{P}}$—for this observe that $\overline{P}$ is prime and $\overline{\mathfrak{P}}$ is $\overline{P}$-primary by Proposition 2.7.8.

To prove the claim, note that $\mathfrak{Q}_{i+1} = (\mathfrak{Q}_i, a_i)$, for some $a_i \in \mathfrak{Q}_{i+1} \setminus \mathfrak{Q}_i$—this is an immediate consequence of the hypothesis that no further ideal can be properly inserted between $\mathfrak{Q}_i$ and $\mathfrak{Q}_{i+1}$ because this comes from a composition series (see Subsection 3.1.2). Since $(\mathfrak{Q}_i, a_i)/\mathfrak{Q}_i \simeq (a_i)/(a_i) \cap \mathfrak{Q}_i$, the surjective ring homomorphism $R \twoheadrightarrow (\mathfrak{Q}_i, a_i)/\mathfrak{Q}_i$ such that $1 \mapsto a_i \bmod ((a_i) \cap \mathfrak{Q}_i)$ has kernel $\mathfrak{Q}_i : (a_i)$. Since $a_i \notin \mathfrak{Q}_i$ then $\mathfrak{Q}_i : (a_i) \subset \mathfrak{n}$. Conversely, $\mathfrak{n} a_i \subset \mathfrak{n}\mathfrak{Q}_{i+1} \subset \mathfrak{Q}_i$—to see the latter inclusion, *i. e.*, that $\mathfrak{n}$ annihilates every such quotient $\mathfrak{Q}_{i+1}/\mathfrak{Q}_i$, one localizes at $\mathfrak{n}$ and uses the exponent of the Artinian local ring $\overline{R}_{\mathfrak{n}}/(\mathfrak{Q}_i)_{\mathfrak{n}}$.

Being through with the one-dimensional case, now assume that $\dim R/\mathfrak{P} \geq 2$ and that the stated formula is true in smaller dimension.

Claim 2. If y is a transcendental element over k and $I \subset k[x_0, \dots, x_n]$ is an arbitrary homogeneous ideal, then $\dim_k I_t = \dim_{k(y)} \tilde{I}_t$, for every $t \geq 0$, where $\tilde{I} \subset k(y)[x_0, \dots, x_n]$ denotes the extended ideal of I.

In other words, the claim is that the Hilbert function is unchanged by thus enlarging the ground field. To see this, let $\{f_1, \dots, f_m\}$ be a k-basis of I_t. It suffices to show that this set is still $k(y)$-linearly independent. Suppose one had a relation $\sum_{i=1}^m b_i f_i = 0$, with $b_i \in k(y)$. By eliminating denominators, one may assume that $b_i \in k[y]$, say, $b_i = \sum_{i,j} a_{i,j} y^j$, $a_{i,j} \in k$. Substituting, the above relation yields

$$\sum_j \Big(\sum_i a_{i,j} f_i \Big) y^j = \sum_i \Big(\sum_j a_{i,j} y^j \Big) f_i = 0,$$

from which $\sum_i a_{i,j} f_i = 0$ for all i, hence $a_{i,j} = 0$ for all i, j by the assumption, thus showing that $b_i = 0$ for all i.

As a consequence of this claim, one has in particular $e_0(R/\mathfrak{P}) = e_0(R(y)/\mathfrak{P}R(y))$. Since $x_1 - yx_0$ is regular on $R(y)/\mathfrak{P}R(y)$, one gets

$$\begin{aligned} e_0(R/\mathfrak{P}) &= e_0\big(R(y)/(\mathfrak{P}, x_1 - yx_0)\big), \quad \text{by Proposition 2.7.15} \\ &= e_0\big(R(y)/\mathfrak{h}(\overline{\mathfrak{P}}, x_1 - y)\big), \quad \text{by Proposition 2.7.8, since } x_0 \notin (\mathfrak{P}, x_1 - yx_0) \\ &= \lambda\big(R(y)_{\mathfrak{h}(\overline{P}, x_1 - y)}/\mathfrak{h}(\overline{\mathfrak{P}}, x_1 - y)_{\mathfrak{h}(\overline{P}, x_1 - y)}\big) e_0\big(R(y)/\mathfrak{h}(\overline{P}, x_1 - y)\big), \end{aligned}$$

by the inductive hypothesis, as $\dim R(y)/\mathfrak{h}(\overline{P}, x_1 - y) = \dim R(y)/(\mathfrak{P}, x_1 - yx_0) \leq \dim R/\mathfrak{P} - 1$. Therefore,

$$\begin{aligned} e_0(R/\mathfrak{P}) &= \lambda\big(R(y)_{(P, x_1 - yx_0)}/(\mathfrak{P}, x_1 - y)_{(P, x_1 - yx_0)}\big) e_0\big(R(y)/\mathfrak{h}(P, x_1 - yx_0)\big) \\ &= \lambda(R_P/\mathfrak{P}_P) e_0(R/P), \end{aligned}$$

by Lemma 2.7.24. □

2.7.5 Multiplicities galore

After such a long discussion on the preliminaries of the multiplicity, one now turns to its relation to ideal theory proper.

2.7.5.1 Intersection multiplicity

The next lemma is fundamental to grasp the subsequent material.

Lemma 2.7.26. *Let $I \subset R$ stand for homogeneous ideal and let $f \in R$ denote a form which is regular modulo I. Then* $\dim R/(I, f) = \dim R/I - 1$.

Proof. The fastest argument is by localizing at the maximal ideal $\mathfrak{m} := (x_0, \ldots, x_n)$, and applying the later Proposition 5.1.12 to the local ring $R_{\mathfrak{m}}$, with $M = R_{\mathfrak{m}}$ and the image of f as an element of a system of parameters. Having the required equality on the local level, one can lift up back to R by homogeneity (this may not work if the data are not homogeneous). □

Remark 2.7.27. The above equality fails miserably if I is not homogeneous. For example, take $I = ((x_0 - 1)(x_1, \ldots, x_n))$, an ideal of dimension n, and $f = x_0$. Then $(I, f) = \mathfrak{m}$. On the bright side, if R is a Cohen–Macaulay (see Section 5.3) Noetherian ring and $I \subset R$ is a perfect ideal (see Definition 6.2.27) then the equality holds ([5, Proposition 1.1(iii)]). The inequality $\dim R/(I, f) \leq \dim R/I - 1$ always holds in any finitely generated domain R over a field due to Proposition 2.5.19 and the fact that dimension and height are complementary in such a ring (Proposition 2.5.33). However, it is the reverse inequality that plays an important role, as will shortly be seen below.

The multiplicity $e_0(R/I)$ has many interesting properties, where $R = k[x_0, \dots, x_n]$. Perhaps the easiest is the following.

Proposition 2.7.28. *Let $I \subset R$ stand for homogeneous ideal and let $f \in R$ denote a form which is regular modulo I. Then $e_0(R/(I,f)) = e_0(R/I)\deg(f)$.*

Proof. By the previous lemma, one has $\dim R/(I,f) = \dim R/I - 1$. Therefore, the result follows from Proposition 2.7.15 by taking the coefficients of t-degree $\dim R/I - 1$ on both sides of the equality there. □

Corollary 2.7.29. *Same assumption as in the previous* proposition. *Then*

$$\sum_{\wp} \lambda(R_{\wp}/(I,f)_{\wp}) e_0(R/\wp) = e_0(R/I)\deg(f), \tag{2.7.29.1}$$

where $\wp$ runs through the minimal primes of maximal dimension of $R/(I,f)$.

Proof. It follows immediately from Theorem 2.7.25. □

Looking at (2.7.29.1), one has a déja-vu feeling: is it a version of Bézout theorem in this case? The answer is affirmative if I is moreover a prime ideal, or more generally, an equidimensional ideal. In this case, the length $\lambda(R_{\wp}/(I,f)_{\wp})$ is a faithful substitute to the local intersection number—this is a result of [155, Section 12], where it is also pointed out for the first time that the length is not anymore the correct local intersection number if none of the two ideals is principal.

Examples 2.7.30.

(1) (Counterexample by van der Waerden ([155, Section 11]))
- $R = k[x_0, x_1, x_2, x_3, x_4]$
- $I = (x_1x_2 - x_0x_3, x_2^3 - x_1x_3^2, x_1^3 - x_0^2x_2x_0x_2^2 - x_1^2x_3)$, the homogeneous defining ideal of the cone in $\mathbb{P}^4$ over a nonnormal quartic curve in $\mathbb{P}^3$;
- $J = (x_0, x_3)$, the homogeneous defining ideal of the cone in $\mathbb{P}^4$ over the coordinate line $x_0 = x_3 = 0$ in $\mathbb{P}^3$.

Then the two cones intersect at their common vertex, the single point $(0 : 0 : 0 : 0 : 1) \in \mathbb{P}^4$; more precisely, $(I,J) = (x_0, x_3, x_1x_2, x_1^3, x_2^3)$, which is easily seen to be an (x_0, x_1, x_2, x_4)-primary ideal of length 5 locally at (x_0, x_1, x_2, x_4).

On the other hand, by the classical method of van der Waerden and others, the true local intersection should count the number of virtual points by taking a sufficiently general deformation of the ideal (x_0, x_3). Actually, in this simple case, it suffices to take $\tilde{J} := (x_0 - x_4, x_3 - x_4)$. A calculation yields $(I,\tilde{J}) = (x_0 - x_4, x_3 - x_4, x_1x_2 - x_4^2, (x_1^2 - x_2^2)x_4, x_1^3 - x_2x_4^2, x_2^3 - x_1x_4^2)$. From this, one easily sees that $(x_1x_2 - x_4^2, (x_1^2 - x_2^2)x_4, x_1^3 - x_2x_4^2, x_2^3 - x_1x_4^2)$, as an ideal in $k[x_1, x_2, x_4]$, has the form $\wp_1 \cap \wp_2 \cap \wp_3 \cap \wp_4 \cap \mathfrak{M}$, where $\wp_1 = (x_1 - x_2, x_2 - x_4)$, $\wp_2 = (x_1 - x_2, x_2 + x_4)$, $\wp_3 = (x_1 + x_2, x_2 + \iota x_4)$, $\wp_4 = (x_1 + x_2, x_2 - \iota x_4)$ (over an algebraic closure of k), while $\mathfrak{M}$ denotes an embedded primary component associated to the 'maximal ideal' (x_1, x_2, x_4).

Therefore, the intersection multiplicity is 4.

(2) (Counterexample by Hartshorne [68, Appendix A, (1.1.1)])
- $R = k[x_0, x_1, x_2, x_3, x_4]$
- $I = (x_0, x_1) \cap (x_2, x_3)$, the homogeneous defining ideal of the cone in $\mathbb{P}^4$ over the intersection of two nonintersecting lines in $\mathbb{P}^3$
- $J = (x_0 - x_2, x_1 - x_3)$, the homogeneous defining ideal of the cone in $\mathbb{P}^4$ over a transverse line in $\mathbb{P}^3$.

Once more, the two cones intersect at their common vertex, the single point $(0 : 0 : 0 : 0 : 1) \in \mathbb{P}^4$. Here, even more simply, $(I, J) = (x_0 - x_2, x_1 - x_3, (x_2, x_3)^2)$, which has length 3.

However, the true local intersection is 2—each minimal prime of I contributes 1 since the intersection is transverse (rigorously, one would have to do as above, deforming the ideal J in $\mathbb{P}^4$ to look for explicit virtual primes).

Remark 2.7.31. Hartshorne's example is by far simpler, but perhaps less intuitive since it resorts to a disconnected union of varieties. Had the latter historically preceded van der Waerden's, one might then justifiably ask whether in a more "normal" situation the length would still work fine. Of course, van der Waerden's example dashes all hopes as it is about a smooth curve in $\mathbb{P}^3$, a perfectly 'normal' situation—alas, neither *perfect* nor *normal* in the technical meaning. Indeed, the failure here could be explained in terms of the fact that the curve is not projectively normal (*i. e.*, not arithmetically Cohen–Macaulay).

A question arises as to whether the result of Lemma 2.7.26 extends to more general situations. In this regard, let $I, J \subset R$ denote homogeneous ideals. In general, one has the inequality $\operatorname{ht}(I, J) \leq \operatorname{ht} I + \operatorname{ht} J$, but this is not a trivial result. Over the polynomial ring R, it can also be written in the form $\dim R/(I, J) \geq \dim R/I - \operatorname{ht} J$. Note that it extends the inequality part $\dim R/(I, f) \geq \dim R/I - 1$ of the lemma, where $J = (f)$. The known modern proofs are by means of the so-called "reduction to the diagonal" (see [169, Theorem 27], but the precedence seems to be van der Waerden's [156]). Both the result and the method underwent a deep history, culminating with some fundamental facts of homology theory and intersection theory (see [138] for a glimpse of the main questions).

Next is a small piece of reduction to a more palatable situation, which was possibly often assumed classically: it suffices to prove van der Waerden's inequality for homogeneous prime ideals. To see this, let P be a minimal prime of R/I of maximal dimension and let Q be any homogeneous prime containing J (*e. g.*, one of its minimal primes). Note that P is automatically homogeneous. Then one has

$$\begin{aligned}\dim R/(I, J) &\geq \dim R/(P, Q) \geq \dim R/P - \operatorname{ht} Q = \dim R/I - \operatorname{ht} Q \\ &\geq \dim R/I - \operatorname{ht} J.\end{aligned}$$

One says that I and J are in *proper mutual position* if $\operatorname{ht}(I,J) = \operatorname{ht} I + \operatorname{ht} J$, *i. e.*, if $\dim R/(I,J) = \dim R/I - \operatorname{ht} J = \dim R/I + \dim R/J - \dim R$. As remarked above, if R/I and R/J are equidimensional (*i. e.*, the respective minimal primes have the same dimension) then it can be shown that also $R/(I,J)$ is equidimensional.

Then Bézout theorem has a form close to that of (2.7.29.1).

Theorem 2.7.32 (Bézout [20]). *Let $I, J \subset R$ equidimensional homogeneous ideals in proper mutual position. Then*

$$e_0(R/I)e_0(R/J) = \sum_{\wp} \iota_{\wp}(I,J)e_0(R/\wp),$$

where $\wp$ runs through the minimal primes of $R/(I,J)$ and $\iota_{\wp}(I,J)$ is the intersection multiplicity *of R/I and R/J along $\wp$.*

The definition of $\iota_{\wp}(I,J)$ is quite involved and the proof has many different approaches. Both have evolved from deep discussions in both commutative algebra and algebraic geometry.

2.7.5.2 Minimal degree

The above discussion had to do with the behavior of the degree in the interaction of two homogeneous ideals. Next, one examines the impact of the degree on the structure of one single ideal.

Proposition 2.7.33. *Let R denote a standard polynomial ring over a field and let $I \subset R$ stand for a homogeneous ideal generated in degrees ≥ 2. Then the numerator $P \in \mathbb{Z}[t]$ in the rational form of the Hilbert series of R/I has the shape*

$$P = 1 + \operatorname{ht}(I)t + \sum_{i\geq 2} a_i t^i,$$

for certain integers $a_i \in \mathbb{Z}$. In particular, $e(R/I) = 1 + \operatorname{ht}(I) + \sum_{i\geq 2} a_i$.

Proof. Let $P = a_0 + a_1 t + \cdots$. One computes a_0 and a_1 from the Hilbert series. Namely, reading coefficients off the equality $P = (1-t)^{d+1} \sum_{n\geq 0} H(R/I,n)t^n$ one derives $a_0 = H(R/I,0) = 1$, while

$$\begin{aligned} a_1 &= H(R/I,1) - (d+1)H(R/I,0) = H(R/I,1) - (d+1) \\ &= \dim_k R_1 - (d+1), \quad \text{since } I \text{ is generated in degrees} \geq 2 \\ &= \dim R - (d+1) = \operatorname{ht} I, \end{aligned}$$

as was to be shown. □

Note that $e(R/I) \geq 1 + \operatorname{ht}(I)$ if and only if $\sum_{i\geq 2} a_i \geq 0$.

The basic result in this regard is the following.

Proposition 2.7.34. *Let R stand for a polynomial ring over an algebraically closed field and let $P \subset R$ denote a homogeneous prime ideal generated in degrees ≥ 2. Then $e(R/P) \geq 1 + \mathrm{ht}(P)$.*

Proof. Say, $R = k[x_0, \ldots, x_n]$. One inducts on $\dim R/P$. Let $\ell \in R$ denote any 1-form. Then $\ell \notin P$, hence $e_0(R/(P,\ell)) = e_0(R/P)$ by Proposition 2.7.28. One can harmless assume that ℓ involves effectively the variable x_n, say, $\ell = \sum_{i=0}^{n} a_i x_i$, with $a_n \neq 0$. Then

$$R/(P,\ell) \simeq k[x_0, \ldots, x_{n-1}]/P',$$

where $x_i \mapsto x_i$ for $0 \leq i \leq n-1$ and $x_n \mapsto -\sum_{i=0}^{n-1}(a_i/a_n)x_i$. Clearly, P' is a homogeneous ideal minimally generated by a set of minimal generators of P after evaluating accordingly. In particular, P' is also generated in degrees ≥ 2.

Distinguishing the ground ring over which one computes degrees and setting $R' := k[x_0, \ldots, x_{n-1}]$, one has $e_{0R'}(R'/(P')) = e_0(R/(P,\ell)) - 1$.

The crucial assertion is now the following.

Claim 1. If ℓ is a general 1-form (*i. e.*, general coefficients) and $\dim R/P \geq 3$, then P' is a prime ideal.

This follows from the following general theorem.

Theorem 2.7.35 ([134, Theorem 12]). *Let $R = k[x_0, \ldots, x_n]$ denote a polynomial ring over an infinite field. If $P \subset R$ is a prime ideal such that $\dim R/P \geq 2$ and $\ell \in R$ is a general affine linear form, then (P,ℓ) is a prime ideal.*

The proof of this result is beyond the present objectives, as it depends on a more elaborate theory of transcendental field extensions plus the notion of *ground-form* as introduced by E. Noether—more on this in the history account of Subsection 2.8.7.

By the above claim, inducting on $\dim R/P$, it follows that

$$e_0(R/P) = e_0\big(R/(P,\ell)\big) = e_{0R'}\big(R'/(P')\big) + 1 \geq \mathrm{ht}_{R'} P' + 2 = \mathrm{ht}\, P + 1,$$

provided $\dim R/P \geq 3$.

The final blow depends on the following initial step of the induction.

Claim 2 (k algebraically closed). If C denotes a reduced and irreducible curve in projective nth space, then its general linear section is a reduced set with of least n points.

For a geometric-minded proof, based on Bézout theorem, see [67, Proposition 18.9]. It is a nice challenge to give an entirely algebraic proof of this fact.

Assuming this and since k is algebraically closed, the minimal primes of (P,ℓ) are each generated by 1-forms, hence Proposition 2.7.21 gives that $e_0(R/P) = e_0(R/(P,\ell))$ counts the number of these primes, hence $e_0(R/P) \geq n = \mathrm{ht}\, P + 1$. □

The above suggests the following.

Definition 2.7.36. Let k denote an algebraically closed field. For a homogeneous prime ideal $P \subset R = k[x_0, \dots, x_n]$ generated in degrees ≥ 2, one says that R/P has *minimal degree* if $e_0(R/P) = 1 + \operatorname{ht} P$.

In support of the characterization of such ideals, the following easy piece seems relevant.

Proposition 2.7.37. *Let R/P as above of minimal degree and* $\dim R/P = d + 1$. *Then* $\dim_k [P]_2 = \binom{n-d+1}{2}$.

Proof. The proof is straightforward: with the notation and argument of Proposition 2.7.33, one finds that $a_2 = 0$ if and only if

$$H(R/P, 2) = (d+1)H(R/P, 1) - \binom{d+1}{2} H(R/P, 0).$$

Substituting for these first few values of the Hilbert function, one arrives at the formula

$$\dim_k [P]_2 = \binom{n+2}{2} + \binom{d+1}{2} - (d+1)(n+1).$$

Induction on $d \geq 0$ will easily show the stated value. □

The typical example of the situation in the corollary is that of the ideal P of 2-minors of the piecewise catalecticant (Hankel) $2 \times (n - d + 1)$ matrix

$$\left(\begin{array}{cccc|cccc|c|cccc} x_0 & x_1 & \dots & x_{a_0-1} & y_0 & y_1 & \dots & y_{a_1-1} & \dots & z_0 & z_1 & \dots & z_{a_{r-1}} \\ x_1 & x_2 & \dots & x_{a_0} & y_1 & y_2 & \dots & y_{a_1} & \dots & z_1 & z_2 & \dots & z_{a_r} \end{array} \right),$$

where $a_0 + \cdots + a_r = n + 1 - d$. It can be shown that the ideal P is prime and has the expected codimension, namely, $n - d + 1 - 2 + 1 = n - d$, hence $\dim R/P$ is one plus the number ($= d$) of Hankel blocks. The corresponding geometric object is the celebrated *rational normal scroll*. As a matter of fact, it can be shown that this is essentially the only example of minimal degree in any given dimension. However, the proof is not trivial. This result was obtained in [42] and, since then, often revisited in more recent times (see, *e. g.*, [52]).

2.8 Historic note

2.8.1 Fractions

If one is asked to choose one single most elementary aspect of commutative algebra not straightforwardly available in the noncommutative theory, certainly the notion of rings of fractions stands up first. Special cases of this theory are so well entrenched in both commutative algebra and algebraic geometry—such as localization at a prime ideal—that it became a trade mark of commutative theory. This author's feeling is that

the topic ought to be introduced as soon as possible. Here, the emphasis is on the relation between the ideals of a ring and its ring of fractions with respect to an arbitrary multiplicatively closed set. The inception of saturation and symbolic powers stand up as essential tools for the entire theory.

Rings of fractions were extensively studied by W. Krull, who attributes the idea to H. Grell ([63, Section 6]). By and large both assumed that the elements of the multiplicatively closed set $\mathfrak{S}$ were nonzero-divisors ("regular" in the terminology of Grell, largely disseminated nowadays). Grell's paper deals with extension and contraction of ideals under ring extensions and the case of rings of fractions was granted full treatment in the paper. Krull would mainly consider the case where $\mathfrak{S}$ is the complementary set to a prime ideal in the case the ring itself was a domain. Thus, for the definition of a "symbolic power" of a prime ideal $\wp \subset R$ in an arbitrary Noetherian ring he would take directly the $\wp$-primary component instead of the inverse image of the extended ideal in the ring of fractions. The general case of a ring of fractions seems to be a later habit.

Symbolic powers have a great significance in algebraic geometry because, given an algebraic (affine or projective) variety W defined by a prime ideal P, the elements of the symbolic power $P^{(s)}$ translate as the rational functions vanishing generically on W to order $\geq s$. It is not clear whether Krull had any knowledge of such an interpretation. In any case, this interpretation has been given by Zariski a little later ([166]), as an application of his *lemme célèbre* proving that, for an irreducible subvariety W of an irreducible algebraic variety V, a rational function of V vanishing at the closed points of a dense subset of W to order at least a given nonnegative integer s already vanishes to that order at the generic point of W. This lemma was intended by Zariski to apply to his theory of holomorphic functions on an algebraic variety, in particular, to prove that the proposed notion was the same whether one considered all closed points or just the closed points with algebraic coordinates over the ground field. The application to the above geometric interpretation of symbolic powers is shortly given at the end of the paper. The proof of the main lemma itself is technically involved; for a more conceptual proof in modern style see [53].

2.8.2 Prüfer and the determinantal trick

The proof of Proposition 2.2.1 is traditionally known as the "determinantal trick." It would seem likely that it first appeared in this context in the seminal paper of H. Prüfer ([125, p. 14]). And yet, no notion of arbitrary modules was then available; so, how did the author get away with it? The explanation is that he was only considering the case where R is a domain and S its field of fractions, hence the finitely generated R-module considered in the above proof was really a *fractional ideal* (as one calls today) treated by Prüfer as modeled on the notion introduced earlier by Dedekind in the case of $R = \mathbb{Z}$ and $S = \mathbb{Q}$. He used the same sort of ideas to prove that the integral closure of an ideal

$I \subset R$ (R a domain) in the field of fractions K of R was a notion equivalent to another one he had introduced earlier in a more involved way. The subtlety is that he took the integral closure as a fractional ideal in K and nowadays one takes it as an ideal of R itself. A virtual difference if R is integrally closed in K—which he might be assuming among the long list of *Eigenshafte* established. Note that Proposition 2.2.13 is also proved by Prüfer ([125, p. 16]) within his standing setup. The so-called determinantal trick does not yield in general an equation of integral dependence of least possible degree. Possibly having in mind a more efficient method, Prüfer gives another proof of the result proposing a different matrix, perhaps more intrinsic to the given data. It may be a good occasion, specially for students, to look at this other matrix envisaging a more computationally efficient algorithm.

2.8.3 Noether and Krull

It is not altogether clear who first introduced the numerical invariants related to prime ideals and their chains. Some of the ideas were underpinned by E. Noether ([117, Section 4]). By and large it seems that both Noether and Krull dealt with chains of primes in the case of integral domains of finite type over a field, while in the additions to the second edition of his book, Krull introduced the notion of dimension and height ("Dimensionsdefekt") for local rings.

The normalization lemma has some cloudy history behind it. The usual reference for it in the literature is the paper of E. Noether *Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p*, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, (1926) 28–35. In his book, Krull does not firmly attribute the result to Noether, but says that it is in the above paper that she makes its most important application. It seems like Noether herself never claimed any original priority, rather saying in a passage that Hilbert was aware of the result.

Here are some additions for the sake of further accuracy.

The usual statement of the normalization lemma—in this book as well as in most texts—solely concerns the existence of a polynomial ring over which a finitely generated k-algebra R is integral. This is fine, however, Noether's main worry was about a sort of converse to this statement, namely: *let $K|k$ be a finitely generated field extension and let $S \subset K$ be an arbitrary k-subalgebra. If S is integral over a finitely generated k-subalgebra $R \subset S$, then S is itself finitely generated over k.*

That this converse is actually true is a consequence of the theory of Noetherian rings and the integral closure, by proceeding along the following steps: S is contained in the integral closure $\widetilde{R}$ of R in the field of fractions L of S, which one may assume that up to an isomorphism is contained in K; now $\widetilde{R}$ is a finitely generated R-module, hence so is S because R is a Noetherian ring (*cf.* Theorem 2.5.4 and its consequences) and, for even more reason, S is a finitely generated R-algebra. Therefore, S is a finitely generated k-algebra as a composite of $S|R$ and $R|k$.

The essential result in the above argument, that the integral closure of a finitely generated k-domain R is a finitely generated R-module, was also proved by Noether in characteristic zero, but was spread among her previous papers and based on the principle of the existence of a *finite rational basis*.

In the 'Der Endlichkeitssatz' paper by Noether that is usually quoted in the literature, her main worry was to prove the converse result as stated above in case of prime characteristic. The popular version of the normalization lemma as in Theorem 2.3.5—quite important as it is—was apparently regarded by Noether as less important in the paper, since the proof for infinite fields could easily be adapted to finite fields as well. She actually makes a point about this by quoting her previous paper *Algebraische und Differentialinvarianten*, Jahresber. Deutsch. Math.-Verein. 3**8** (1923), 177–184. Incidentally, in a footnote she mentions Hilbert's seminal paper on invariant theory, where he apparently was aware of parts of the *finiteness theorem*.

In a different vein, a generalization of the result itself has been sought by assuming that the ground field k is replaced by an arbitrary ring. Unfortunately, this turns out to be unattainable as one can easily see by taking a polynomial ring over the integers. This remark is usually attributed to S. Abhyankhar, but it seems to have long been known to M. Nagata, who tried to develop some theory along this line in his book [112]. Strangely enough, this virtual generalization is quoted in [168] as a general theorem. As a means of correcting this mistake, one can easily prove that the generalization is true over the localization of the ground ring at the powers of a convenient element.

2.8.4 Primary decomposition

The characterization of a primary submodule in terms of condition (iv) of Proposition 5.2.13 seems to have slipped E. Noether's mind, who wrote in this regard: "As well the definition of primary and prime ideal cannot be transported to modules since the product of two quantities (elements) is not defined." ([116, Section 9, p. 56]) In spite of the fact that the notion of the quotient was sufficiently known and largely used by Noether, the idea of a zero-divisor on a module does not seem to be fully undertaken at the time. In this book, as well as in most books on the subject, the argument in the proof of Theorem 5.2.17 is elegantly abstract. The original argument of Lasker and Noether, in the case of ideals, went through the consideration of an *irreducible* decomposition rather than a primary one. Actually, Noether dedicated quite some space for such a consideration, with many examples throughout. Perhaps the reason irreducible decomposition essentially faded out in modern exposés is the lack of uniqueness or of a stable number of components. Thus, from a decomposition into irreducible components one passes to a primary normally nonirreducible decomposition by clipping together primary submodules with same radical—the main step in reaching a reduced primary decomposition.

2.8.5 Hilbert and Artin

Theorem 2.5.4 was proved by David Hilbert in *Über die Theorie der algebraischen Formen*, Mathematische Annalen, **36** (1890) 473–534. The proof given here is reminiscent of the original argument given by Hilbert with the enormous time gap making Hilbert unaware of the theory of Noetherian rings (only much later fully entrenched by E. Noether). In its original form, he took R to be a polynomial ring over a field in finitely many variables and proceeded by induction on the number of variables, showing that any homogeneous ideal is finitely generated. The proof given in Theorem 2.5.4 stays close to Hilbert's own argument by choosing an infinitely countable set of elements in the given ideal. Hilbert himself was quite aware that this hypothesis was not quite in the generality he wished. In fact, he proceeded in the same paper to explain how one switches from such a countable set to the case of an arbitrary ideal (then called *module* in the language of Kronecker). For that, he assumed without further ado the axiom of choice as a self-granted hypothesis.

Also, Hilbert's original theorem restricted himself to the case of homogeneous polynomials (the German *Formen*). Nonetheless, his argument remains essentially valid for any polynomials. The reason behind this restriction is that he was really interested in the applications to the theory of invariants, a much deeper work he took over in the sequel.

The proof of Theorem 2.5.14 came after a long period of preliminary work both in the commutative as in the noncommutative situation. The idea of the length of a module crystallized slowly from the corresponding notion for finite groups—a clear statement of the main facts was given by E. Noether in 1926 ([118, Section 10]) for the purpose of establishing a version of Theorem 2.5.13.

Now, the implication that an Artin ring is Noetherian had to somehow be firmly grounded on properties of rings alien to modules for the simple fact that there exist nonfinitely generated *Artinian modules* (similar definition)—in fact, the usual local cohomology modules are of this nature. Thus, if one takes for granted the theory of Jordan–Hölder warranting that any two composition series have the same length and this length is by definition the length of R (more generally, this is defined for a module), an alternative argument goes as follows: let $I_1 \subset I_2 \subset \cdots$ be an ascending chain of ideals in R. Then one has a sequence of surjective ring homomorphisms $R/I_1 \twoheadrightarrow R/I_2 \twoheadrightarrow \cdots$. As noted, for any ideal $I \subset R$, R/I is Artinian as well. By the additivity property (here one needs the notion of length for a module as well) the length of R/I_i is strictly larger than the one of R/I_{i+1}. Since R/I_1 has finite length, then $R/I_i = R/I_{i+1}$ for sufficiently large i. This makes the original chain of ideals stationary.

As for the chronology proper, in 1935 (10 years after Noether' above paper) Y. Akizuki ([1]) proved a slightly stronger result, often confused with the "Artin ⇒ Noether" theorem. What he showed is that a commutative ring R such that R/I is Artinian for every ideal $I \neq \{0\}$ is Noetherian. Since an Artinian domain is a field, this result is really

about a condition as to when a ring of Krull dimension ≤ 1 is Noetherian. This question was very much around in the period, Krull having dubbed such rings "einartige Integritätsbereiche" in the domain case. The question as a whole, in the noncommutative setup, drove lots of attention in the late 1930s ([78], [102]). In the commutative setup, the problem was completely clarified by I. Cohen in 1950 ([37]), who dubbed the above condition RM (for *restricted minimum* condition), an alternative terminology for "weakened" ('abgeschwächter') used by E. Noether. He proved that a (commutative) ring satisfies RM if and only if it is a Noetherian ring of Krull dimension ≤ 1 (and, moreover, it is a domain if the Krull dimension is 1). Besides its admirable simple style, Cohen explains the relation among the various results known so far by many authors, giving a complete picture of the theory in the period 1935–1950. A couple of similar results in the noncommutative case were later proved by A. Ornstein ([124]). For a very recent survey-like account, see [62].

2.8.6 The Lasker–Noether binary

The history of this celebrated result is quite rich and amusing by taking a hindsight perspective. No insight into its significance is possible without full consideration of the early efforts of the German mathematicians of nineteenth century toward encompassing formulation of both number theory and early algebraic geometry.

Here, one finds the first attempts at shaping up the notions of ideal and module. The basic instinct came form the early work of Gauss on number theory. Inasmuch as it looks so natural to us, the extension of his ideas to rings and ideals, it took nearly half a century or so to crystallize the notions. It would seem like Kronecker was the first to make systematic use of the term "Modul" (German), while a bit later Dedekind introduced the notion of "Ideale," inspired by the work and early terminology of Kummer and encouraged by Dirichlet.

One overall difficulty in guessing the exact state of things while browsing through the corresponding literature lies on the various, sometimes imprecise, meanings the same word acquires from author to author. Terms such as "Bereich," "Formen" and alike appear throughout often without definition and possibly with varying meaning. A more stable terminology would only shape up in the second and third decades of the twentieth century, in the steps of the success attained by the work of E. Noether, B. van der Waerden, W. Krull and a few others.

Alas, E. Lasker stands out as an isolate happening. For one thing, he belonged to the "old" school of the previous century, while his one work in commutative algebra/algebraic geometry singles out as a true benchmark over all the preceding endeavor. On one hand, Kapitel I of his paper deals with elimination theory (resultants, etc.) and the reading is quite difficult due to a mix of notions from classical invariant theory and early algebraic geometry. Then Kapitel II is like a nonanticipated trip to heavens, where the algebraic treatment is very clean, with notions introduced in a

clear manner (*i. e.*, fairly followed by a twenty-first century trained algebraist). It is in this part that he introduces the notion of prime and primary ideals—the first already guessed by Kronecker and Dedekind, while the second seems to be his invention at least in the generality the definition is stated, pretty much the same one uses today. This point is ever more strange when one reads what E. Noether had to say about it 15 years circa later:"*Auch das primare Ideal ist bei Lasker* (*und Macaulay*) *unter Zugrundlegung von Begriffen aus der Eliminationstheorie definiert*." This statement that Lasker's definition was essentially based on concepts from elimination theory is with flagrant discrepancy vis-a-vis what one reads in the second paragraph of page 51 in Lasker's paper.

Lasker work is a bona-fide pioneering result in pure commutative algebra, even though his mentality was completely taken up by an old, not universally accepted terminology in algebraic geometry. At some point, one gets slightly confused as to whether he is using some of Hilbert's main theorems of the years 1890–1893 or reproving parts of them as a consequence of his results. A comment about this state of affairs is given in Section 10 of Noether's paper ("Special case of a polynomial ring"), but I am afraid the interested reader will have to look also at a long footnote in that section.

At the other end, the E. Noether 1921 paper is clearly the last word on primary decomposition and is followed until these days, with very little improvement (including the proofs in this book). She was first to understand the impact of Hilbert's results of the previous century into a general frame of abstraction. Her paper is seminal in various directions, including in establishing a more stable terminology. As an overture, *e. g.*, she gives the definition of an abstract ring for the first time—except that she attributes the terminology "Ringe" to her young associate A. Fraenkel in his Habilitationsschrift (Leipzig, 1916, published 1920). Even then, Noether was still addicted to the old terminology and notation from the Dedekind school. Thus, *e. g.*, given an element $a \in R$ and an ideal $I \subset R$, the terminology for saying that f belongs to I was "f is divisible by I," and instead of our modern notation $f \in I$ the congruence notation $f \equiv 0(I)$ was used. Also, intersection and sum of ideals were "least common multiple" and "greatest common divisor," respectively. The notation for the intersection was $[I, J]$ instead of $I \cap J$, and so on.

Curiously, Lasker and Noether had some sort of parallel life. Both were of Jewish birth and were forced to emigrate at about the same time due to the growing Nazism in Germany during the 1930s. Both died in the USA of contracted physical failure a few years after having left Germany for good. Lasker called his result on primary decomposition of polynomial ideals the *Noether–Dedekindschen theorem*, referring to Max Noether instead (E. Noether's father), of course totally unaware that he would be largely superseded by the daughter 15 years later. Lasker wrote his PhD thesis under D. Hilbert, while Noether managed to get a job as a mathematician in Götingen thanks to Hilbert's efforts. Thus, both were somewhat very much connected to Hilbert's ideas. Lasker's published mathematical work took up only about 4 years (his seminal paper dating 1905, while he had a teaching position in the USA). Noether, on the other hand,

was a tireless working mathematician starting up with an important result in physics (still much cited in circles of theoretical science) and introducing various fundamental ideas in commutative algebra and algebraic representation theory.

2.8.7 Hilbert function

Very often there is some residual notational confusion between the Hilbert function of a homogeneous ideal $I \subset R = k[x_0, \ldots, x_n]$ and the one of R/I. If one introduces the notion only for ideals, then one has to define it anew for both R ($R = (1)$ is not homogeneous as an ideal!) and R/I. Also, it is R/I that comes naturally for the geometric statements. Probably it is more natural to define the notion for graded rings and graded modules over such rings, as is done in modern theory (see Section 7.4), so as to encapsulate all cases under one single definition with the advantage of some additional elbow-room.

Alas, in 1890 general ideal theory had yet to be established, although there was a great deal of mastery about forms and Hilbert certainly excelled on those. By a master's coup, he took the approach of transforming the problem into a linear one. This is what he does in [72, Section IV], in quite an enjoyable reading if one accepts the language of the period. Much less known or quoted is the nearly hundred pages account of E. Lasker ([101]), wrapping up work by E. Noether, M. Noether, Hilbert and many others. Often referred in the literature as a chess player, Lasker was in fact a competent mathematician, very much connected with Hilbert himself. Many of the modern features of commutative algebra appear in perhaps crude form in Lasker's account. The subsequent work of van der Waerden was in fact inspired on that of Lasker. His clean modern approach became essentially what is usually taught nowadays about the Hilbert function of a homogeneous ideal—unfortunately, only too rarely giving proper credit to the improvement of Hilbert's ideas by so many fine mathematicians of the subsequent period.

What has slightly gone missing in recent accounts of the subject is precisely the fact that Hilbert thought about the characteristic function as counting, for a given homogeneous ideal $I \subset R$ and a given degree d in R, the number of linearly independent conditions imposed upon a d-form in R to belong to I.

In modern language, one considers the family of all d-forms with base parameters the affine algebraic variety k^{N_t}, where $N_t = \binom{n+t}{n}$, and takes a k-vector basis of $[I]_t$. The condition that a t-form f belongs to I is equivalent to having it written as a k-linear combination of the t-forms in the basis of $[I]_t$. This in turn is expressed by a finite number of linear equations in the coordinates of k^{N_t}, defining a linear subspace of the latter. Hilbert's characteristic function was, by definition, the dimension of this linear subspace.

This is not to imply that Hilbert had any hope to use his definition as a means of efficient computation. He would not be dragged into the fashion of the period in

which lengthy computations would take dozens of written pages. Instead, he applied his fresh result on the existence of a graded minimal resolution of a homogeneous ideal in R. Nowadays this is still a valuable theoretical and computational result.

The fact that this "linear" dimension devised by Hilbert coincides with $H(R/I, t)$ is not a majestic result but still requires some proof. Apparently, the first author to give it proper attention was F. S. Macaulay in [105], introducing the terminology *Hilbert numbers* (only to fall in oblivion in favor of the corresponding function with those values). A definite rigorous proof was later established by W. Gröbner in [64], using first principles of what now is known as the theory of Gröbner bases.

The formula (2.7.25) has a historic connection to the Bézout theorem; for the details of this celebrated theorem see, *e. g.*, [67, Lecture 18]. The latter has to do with the intersection of two projective subvarieties in appropriate relative position. This relative position is such that one expects a finite set of points, so that the theorem counts the cardinality of this set and concludes that it equals the product of the degrees of the two varieties. An early expectation was that taking the degree of the intersection of the two varieties would carry out the job.

2.9 Exercises

Exercise 2.9.1. Let R denote a ring and let $\mathfrak{S} \subset R$ stand for a multiplicatively closed set. Prove: given a ring structure on the set $\mathfrak{S}^{-1}R = (R \times \mathfrak{S})/(\text{equiv.})$ in such a way that the map $\sigma : R \to \mathfrak{S}^{-1}R$, defined by $a \mapsto a/1$, be a ring homomorphism, then the structural operations are necessarily the ones defined above.

(Hint: show that if $a/s, b/t \in \mathfrak{S}^{-1}R$ belong to the image $\sigma(R) \subset \mathfrak{S}^{-1}R$, then it necessarily holds that $a/s + b/t = (at + bs)/st$ and $a/s \cdot b/t = ab/st$. To see this, write $a/s = a_1/1$ and $b/t = b_1/1$, express these equalities in terms of the definition and add up the resulting relations conveniently multiplied by elements of $\mathfrak{S}$.)

Exercise 2.9.2. Let R be a ring and let $\mathfrak{S} \subset R$ denote a multiplicatively closed subset.

(1) For a prime ideal $P \subset R$ and an integer $n \geq 1$, express the inverse image $\iota^{-1}\mathfrak{S}^{-1}P^n = \iota^{-1}P_P^n$ in terms of annihilators.
(2) Give an example where the equality $P^n = \iota^{-1}P_P^n$ fails.
(3) Let $\mathfrak{S}$ be the set of nonnegative powers of a single element $s \in R$, in which case one denotes $\mathfrak{S}^{-1}R = R_s$. Prove: if $I \subset R$ is an ideal such that s is regular on R/I and I_s is a prime ideal of R_s, then I is a prime ideal.

Exercise 2.9.3. Let R be a ring, let $\mathfrak{S} \subset \mathfrak{T} \subset R$ denote multiplicatively closed sets and let $I \subset R$ stand for an ideal.

(i) Show that $\iota_{\mathfrak{S}}(\mathfrak{T}) \subset \mathfrak{S}^{-1}R$ is a multiplicatively closed set, where $\iota_{\mathfrak{S}} : R \to \mathfrak{S}^{-1}R$ is the canonical homomorphism
(ii) Show that $\iota_{\mathfrak{S}}(\mathfrak{T})^{-1}(\mathfrak{S}^{-1}I) \simeq \mathfrak{T}^{-1}I$ in a natural manner

(iii) Deduce from (ii) that if $P' \subset P$ are prime ideals of R, then $(I_P)_{P'R_P} \simeq R_{P'}$ in a natural way.

Exercise 2.9.4. Let P_1, P_2 be prime ideals in a Noetherian ring.
(1) Prove: $\operatorname{ht}(P_1P_2) = \operatorname{ht}(P_1 \cap P_2) = \min\{\operatorname{ht} P_1, \operatorname{ht} P_2\}$.
(2) Give an example showing that, in general, $P_1 + P_2$ is not a prime ideal.
(3) Suppose that neither $P_1 \subset P_2$ nor $P_2 \subset P_1$. Give an example showing that, in general, $\operatorname{ht}(P_1 + P_2) < \operatorname{ht} P_1 + \operatorname{ht} P_2$.

Exercise 2.9.5. Let $P_0 \subset P$ be prime ideals of a Noetherian ring.
(1) Prove: if there is at least one prime ideal P_1 such that $P_0 \subsetneq P_1 \subsetneq P$, then there is an infinite family $\{P_i\}_i$ of prime ideals such that $P_0 \subsetneq P_i \subsetneq P$, for every i.
(Hint: apply prime avoidance when assuming that the family of such ideals is finite.)
(2) Illustrate the behavior in (1) with $P_0 = \{0\}$, $P_1 = (X, Y)$ in $\mathbb{Q}[X, Y]$.
(3) Give an example of a non-Noetherian ring where the assertion in (1) fails.

Exercise 2.9.6 (Refinement of prime avoidance (Lemma 2.5.22)). Let A denote a ring containing an infinite field k and let $I, J_1, \ldots, J_m \subset A$ be ideals with $I = (a_1, \ldots, a_n)$. Prove: if $I \not\subset J_j$ for every $j = 1, \ldots, m$, then there exist $\lambda_2, \ldots, \lambda_n \in k$ such that

$$a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n \notin \bigcup_{j=1}^{m} J_j.$$

(Hint: Consider the k-vector subspace $V \subset I$ spanned by $a_1, \ldots, a_n$.)

Exercise 2.9.7. Let $I = (X^2 + YZ, Y^2 + XZ, Z^2 + XY) \subset k[X, Y, Z]$, where k is a field.
(1) If $\operatorname{char}(k) \neq 2$, prove that $\operatorname{ht} I = 3$ by showing that $\sqrt{I} = (X, Y, Z)$
(Hint: show that $X^4, Y^4, Z^4 \in I$.)
(2) What is the height of I if $\operatorname{char}(k) = 2$?
(3) Prove that upon replacing $Z^2 + XY$ by $Z^2 - XY$ the resulting ideal has height 2 in any characteristic; in this case, show that the generators of I are the 2×2 minors of a 3×2 matrix

Exercise 2.9.8. Consider the ideal $P \subset R = \mathbb{Q}[X, Y, Z]$ generated by the 2×2 subdeterminants of the 2×3 matrix

$$\begin{pmatrix} X & Y & Z^2 \\ Y & Z & Z \end{pmatrix}.$$

(1) Prove that P is a prime ideal
(Hint: show by direct calculation that Z is not a zero-divisor modulo P and that $R_Z/P_Z \simeq \mathbb{Q}[Y, Z, 1/Z]/(Y^3 - Z^4)$.)

(2) Consider the polynomial $f = Z^5 + Y^3Z - 3XYZ^2 + X^3$. Show that $f \in P^2 : z$, hence $P^{(2)} \supset (P^2, f)$. Does the equality hold?
(3) How does the maximal ideal (X, Y, Z) of R relate to P^2?

Exercise 2.9.9. Compute a Noether normalization for each of the following domains of finite type over a field k:
(1) $k[X_1, \dots, X_n]/(f)$, where f is an irreducible polynomial over k
(2) $k[T^2, T^3] \subset k[T]$
(3) $k[X, Y, Z, W]/(XW - YZ, Y^2 - XZ, Z^2 - YW)$
(4) $k[T^3, T^4, T^5] \subset k[T]$
(5) $k[T^2, TU, TV, U^2, UV, V^2] \subset k[T, U, V]$.
(6) $k[TU, TV, TW, UV, UW, VW] \subset k[T, U, V, W]$

(Hint: follow the method of the proof, by determining the corresponding presentation ideal over k or at least some of its generators.)

Exercise 2.9.10. Let R denote a principal ideal domain and let $P \subset R$ denote a nonzero prime ideal. Prove that the polynomial ring $R_P[X]$ has a maximal ideal $\mathfrak{m}$ such that $\mathfrak{m} \cap R_P$ is not a maximal ideal (*cf.* Goldman Nullstellensatz (Theorem 2.4.2)).

Exercise 2.9.11. Compute the integral closure of $\mathbb{Z}$ in the following field extensions $K|\mathbb{Q}$:
(1) $K = \mathbb{Q}(i)$, where $i^2 + 1 = 0$
(2) $K = \mathbb{Q}(\sqrt{2})$
(3) $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$
(4) $K = \mathbb{Q}(X)$, where X is an indeterminate over $\mathbb{Q}$
(5) $K = \mathbb{Q}(\zeta_n)$, where $\zeta_n \in \mathbb{C}$ is a primitive root of unity of order n
(Hint: look up some book in algebraic number theory.)

Exercise 2.9.12. Show that each of the following domains is integrally closed in its respective field of fractions:
(1) A unique factorization domain (UFD)
(2) $k[X, Y]/(XY - 1)$ (k a field)
(3) $\mathbb{C}[X, Y]/(X^2 + Y^2 - 1)$
(Hint: apply a suitable change of coordinates and use (2).)
(4) $\mathbb{C}[X, Y, Z]/(Y^2Z - X(X^2 - Z^2))$
(5) $\mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$
(Hint: $\mathbb{R}[X, Y]/(X^2+Y^2-1) = \mathbb{C}[X, Y]/(X^2+Y^2-1) \cap K$, where K is the field of fractions of $\mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$ viewed inside the field of fractions of $\mathbb{C}[X, Y]/(X^2 + Y^2 - 1)$.)

Exercise 2.9.13. Let $A = k[x, y]$ (k a field) and let $A_d \subset A$ denote the dth graded part of A. Set $R := k[A_d]$ and $K = k(A_d)$ for its field of fractions. Show that R is integrally closed in K.

(Hint: prove that $K = k(x^d, y/x)$, yielding $k[A_d] \subset k[x^d, y/x] \subset K$; thus, by the case of a polynomial ring, reduce the problem to showing that $k[A_d]$ is integrally closed in $k[x^d, y/x]$, where a direct calculation comparing negative exponents and nonnegative degrees gives the result.)

Exercise 2.9.14. In the notation of the previous exercise, let $R = k[x^4, x^3y, xy^3, y^4] \subset k[A_4]$. Prove that R is not integrally closed in its field of fractions.

Exercise 2.9.15. Compute the integral closure of the following ideals:
(i) $I = (x^d, y^d) \subset k[x, y]$, for $d \geq 1$.
(ii) $I = (x^d, x^{d-1}y, y^d) \subset k[x, y]$, for $d \geq 2$. Give a generalization.
(iii) $I = (x^3, y^5) \subset k[x, y]$.
(Hint: x^2y^3, xy^4 are integral over I—is this "enough"?)
(iv) $I = (x^3, x^2y^8, xy^{15}, y^{21}) \subset k[x, y]$.
(Hint: test x^2y^7 and xy^{14}—do these suffice?)

Exercise 2.9.16 (Huneke–Swanson). Let $I, J \subset R$ be ideals such that there is an element $a \in \widetilde{(J, I)} \setminus (\tilde{J}, \tilde{I})$. Let T be an indeterminate over R and set $J' := (\tilde{J}, T)$, $I' := (\tilde{I}, T) \subset R[T]$. Prove that $aT \in \widetilde{J'I'} \setminus I'J'$.

Exercise 2.9.17. Compute the integral closure of the following domains in their respective fields of fractions:
(1) $k[X, Y]/(Y^2 - X^3)$ (k a field)
(Hint: if x, y denote the residue classes of X, Y, respectively, then $(y/x)^2 = x \in \mathbb{Q}[x, y]$.)
(2) $k[T^2 - 1, T(T^2 - 1)] \subset k[T]$ (k a field)

Exercise 2.9.18. Let R denote a Noetherian local ring, with unique maximal ideal $\mathfrak{m} \subset R$, and let $I \subset \mathfrak{m}$ denote an ideal.
(1) Show that the minimal number of generators of I coincides with the dimension of the $R/\mathfrak{m}$-vector space $I/\mathfrak{m}I$.
(Hint: apply Lemma 2.5.24.)
(2) Suppose that $J \subset I$ is a subideal of I. Prove that the following conditions are equivalent:
(i) Any finite set of generators of J can be extended to one of I.
(ii) $\mathfrak{m}I \cap J = \mathfrak{m}J$.
(Hint: reduce the inclusion $J \subset I$ modulo $\mathfrak{m}$, compute the resulting kernel and apply (1).)

Exercise 2.9.19. For each of the ideals $I \subset R$ below:
- Compute $\operatorname{ht} I$ and exhibit a chain of primes with length $\operatorname{ht} I$.
- Determine the minimal prime ideals of R over I.
- Compute the radical $\sqrt{I}$.

(1) $I = (X^2 - YZ, Y^2 - XZ, Z^2 - XY)$, $R = k[X, Y, Z]$ ($\mathrm{char}(k) \neq 2$)
(2) $I = (X_0X_1X_2, X_0X_1X_3, X_0X_2X_3, X_1X_2X_3)$, $R = k[X_0, X_1, X_2, X_3]$
(3) $I = (X^3 - YZ, Y^2 - XZ)$, $R = k[X, Y, Z]$
(4) ($k = \mathbb{C}$) I the ideal of $R = k[X, Y, Z, W]$ generated by the 2×2 minors of the matrix

$$\begin{pmatrix} X & Y & Z & W \\ Y & Z & W & X \end{pmatrix}$$

(Hint: it may be useful to show that $X^2 - Z^2, Y^2 - W^2 \in I$.)
What changes if $k = \mathbb{R}$?

Exercise 2.9.20. Let $\mu(\_)$ denote the smallest cardinality of set of generators of an ideal in a Noetherian ring.
(1) Give an example of an ideal I such that $\operatorname{ht} P < \mu(I)$ for every minimal prime ideal P of I.
(2) Give an example of an ideal I, not a prime, such that $\operatorname{ht} P = \mu(I)$ for every minimal prime ideal P of I.
(3) Given arbitrary integers $0 \leq m \leq n$, give an example of an ideal I admitting a unique minimal prime P and such that $\operatorname{ht} P = m$, $\mu(I) = n$.

Exercise 2.9.21. Let there be given a prime ideal $P \subset R$ and an element $a \in R \setminus P$.
(1) Prove that $\operatorname{ht}(P, a) \geq \operatorname{ht} P + 1$.
(2) Discuss the possibility that the inequality in the previous item be strict.
(3) Give an example where $\sqrt{(P, a)}$ is a prime ideal, and yet (P, a) is not prime.

Exercise 2.9.22. Let $R = k[X_1, \ldots, X_n]$, where k is a field. Consider the k-subalgebra $S = R[X_2/X_1, \ldots, X_n/X_1]$ of the field of fractions of R (often called an *affine monoidal transform*).
– Show that $\dim S = n$ and that the extended ideal in S of the maximal ideal $(X_1, \ldots, X_n)$ of R is principal (often called the *exceptional locus*)
– Consider the surjective R-homomorphism $\varphi : R[T_2, \ldots, T_n] \twoheadrightarrow S$ such that $\varphi(T_i) = X_i/X_1$. Show: $\ker \varphi$ contains the ideal $\mathfrak{P} := (X_1T_i - X_i \mid 2 \leq i \leq n)$.
– Discuss about the height and the primeness of $\mathfrak{P}$.
(Hint: discussion will become clearer upon reading Chapter 5.)

Exercise 2.9.23. * Let R denote a Noetherian domain of dimension ≤ 1. Let K stand for the field of fractions of R and let $R \subset S \subset K$ denote an intermediary subring. Prove: S is Noetherian of dimension ≤ 1.

Exercise 2.9.24. Let R denote a finitely generated algebra over a field k. Prove that the following conditions are equivalent:
(1) R is finite-dimensional as a k-vector space
(2) $\dim R = 0$
(3) The set of prime ideals of R is finite

Deduce: if $R \subset S$ is a ring extension such that S is finitely generated as R-module then, for any prime ideal $P \subset R$, the set of prime ideals of S contracting to P is finite.

Exercise 2.9.25. Let $R[[X]]$ stand for the set of formal power series over a ring R.

(i) Prove that $R[[X]]$ is a ring under the usual Cauchy-like sum and product operations

(ii) Endowing $R[[X]]$ with the ring structure as in (i), show that the map $\varphi : R[[X]] \to R$ such that $\varphi(a) = a$, for $a \in R$, and $\varphi(X) = 0$, is a (surjective) ring homomorphism

(iii) Prove: if $P \subset R[[X]]$ is a prime ideal and $\varphi(P)$ is finitely generated, then so is P. (Hint: if $X \in P$ the result is trivial; if $X \notin P$ and $\varphi(P) = (a_1, \ldots, a_r)$ take for each i a power series f_i with constant term a_i. Then apply a similar degree lowering procedure as in the proof employed in the Hilbert basis theorem in order to show that $P = (f_1, \ldots, f_r)$.)

(iv) Prove: R Noetherian $\Rightarrow R[[X]]$ Noetherian.

Exercise 2.9.26 (David Speyer). Give another proof of the Hilbert basis theorem along the following lines. Let $I \subset R[X]$ be an ideal. For a fixed integer $d \geq 0$, let $I(d) \subset R$ denote the set of elements that are leading coefficients of some polynomial in I of degree d.

(a) Show that $I(d)$ is an ideal of R.

(b) Show that $I(0) \subset I(1) \subset I(2) \subset \cdots$, and let $I_\infty \subset R$ denote a stable value of this chain at index r.

(c) Say, $I_\infty = (g_1, \ldots, g_m)$. For each g_i, choose some $f_i \in I$ of the form $g_i\,\mathrm{tr} + \text{lower order terms}$.

(d) Show that $R \cap (R.1 + RX + \cdots + RX^{r-1})$ is finitely generated as an R-module. (Hint: Use the fact that every submodule of the free R-module R^r is finitely generated—see last Section.) Let $\{h_1, \ldots, h_n\}$ stand for a finite set of generators of this R-module.

(e) Show that the set union $\{f_1, \ldots, f_m\} \cup \{h_1, \ldots, h_n\}$ generates the ideal I.

Exercise 2.9.27. As regards the prime avoidance lemma (Lemma 2.5.22):

(1) Deduce that the union of a finite set of prime ideals is not an ideal unless these ideals are all contained in one of them.

(2) Give an example where the union of a finite set of ideals is an ideal. (Hint: let k denote a finite field and let $R = k[x, y] = k[X, Y]/(X, Y)^2$. Consider the set of principal ideals $(ax + by)$, for varying $a, b \in k$.)

Exercise 2.9.28 ($\mathrm{char}(k) \neq 2$). Let $\varphi : R = k[X, Y, Z] \to k[T]$ be the k-homomorphism such that $\varphi(X) = T^3$, $\varphi(Y) = T^4$, $\varphi(Z) = T^5$.

(1) Verify that $P := (X^3 - YZ, Y^2 - XZ, Z^2 - X^2Y) \subset \ker\varphi$ and that $\mathrm{ht}\, P = 2$.

(2) Deduce that $P = \ker\varphi$ (in particular, P is a prime ideal) and show that P is the ideal of maximal subdeterminants of a suitable matrix.

(3) Show that P^2 is not P-primary.
(4) Give the associated primes of R/P^2.

Exercise 2.9.29. Let $I \subset R$ denote a monomial ideal and let $P \subset R$ be an associated prime of R/I. Prove the following assertions:
(1) If $\sqrt{I} = (X_1, \dots, X_n)$, then $P = (X_1, \dots, X_n)$
(2) If $\sqrt{I} \neq (X_1, \dots, X_n)$, say, $X_1 \notin \sqrt{I}$, consider the chain of ideals

$$I_0 = I \subset I_1 = I : X_1 \subset I_2 = I_1 : X_1 \subset \cdots$$

and show that $I_k = I_k : X_1$, for $k \gg 0$
(3) If $P \in \operatorname{Ass}(R/(I_m, X_1))$ for some m, then $(I_m, X_1) = (J, X_1)$, for a suitable monomial ideal J with a set of generators having support in $\{X_2, \dots, X_n\}$
(4) If $P \notin \operatorname{Ass}(R/(I_m, X_1))$ for every m, consider the exact sequence

$$0 \to R/(I_m : X_1) \longrightarrow R/I_m \longrightarrow R/(I_m, X_1) \to 0.$$

Argue that $\operatorname{Ass}(R/I_m) \subset \operatorname{Ass}(R/I_m : X_1) \cup \operatorname{Ass}(R/I_m, X_1)$ and conclude recursively that $P \in \operatorname{Ass}(R/I_m), \forall m$
(5) In particular, $P \in \operatorname{Ass}(R/I_k)$ for a stabilizing value of k as in (2); but as X_1 is regular on R/I_k, conclude that I_k involves only the variables $\{X_2, \dots, X_n\}$.
(6) Conclude, by induction, that P is generated by a set of variables.

Exercise 2.9.30. A monomial ideal is primary if and only if, up to permutation of variables, it has the form

$$I = (X_1^{a_1}, \dots, X_r^{a_r}; \mathbf{X}^{\mathbf{b}_1}, \dots, \mathbf{X}^{\mathbf{b}_s}),$$

for some r, s, where $a_i > 0 \, \forall i$ and the support of $\mathbf{X}^{\mathbf{b}_j}$ is contained in $\{X_1, \dots, X_r\}$ for every $j = 1, \dots, s$.

(Hint: apply the previous exercise.)

Exercise 2.9.31. Every monomial ideal $I \subset A$ admits an irredundant primary decomposition into primary monomial ideals. Prove this assertion by inducting on the number of variables involved in the union of the supports of a set of minimal monomial generators of I, along the following steps:
(1) If I is not primary, then say, $(X_n)^i \notin I$, $\forall i \geq 0$
(2) Up to permutation of a set of monomial generators $\{u_1, \dots, u_r\}$ of I, there are integers $0 \leq a_1 \leq \cdots \leq a_r$, with $a_r > 0$, such that u_j is divisible by $X_n^{a_i}$ but not by $X_n^{a_i+1}$
(3) $I = (I, X_n^{a_r}) \cap (I : X_n^{a_r})$.

Exercise 2.9.32. Apply the procedure of the previous exercise to the ideal $I = (X^2Z, YZ^2, X^3Y^2)$.

Exercise 2.9.33. If a monomial ideal $I \subset R$ admits a set of generators supported on the first $r \leq n$ variables of R, then the primary components in any irredundant primary decomposition of I involve only these many variables.

Exercise 2.9.34. Recall the notion of an irreducible ideal (Definition 2.6.1).
(1) Prove: an irreducible monomial ideal is generated by pure powers of the variables
(2) Any monomial ideal admits a unique irredundant primary decomposition into irreducible primary components.

Exercise 2.9.35. Let $R = k[x_0, x_1, x_2, x_3]$, with k a field, and let $I = (x_0, x_1) \cap (x_2, x_3)$.
(i) Show that $H_{R/(I,x_0)}(2) = H_{R/(I,x_0)}(3) = 4$, while $H_{R/(I,x_0)}(4) = 3$ and conclude that (I, x_0) has an embedded primary component.
(ii) Consider the previous item as a warm-up (since it is easy to very directly the embedded component). Now let $P \subset R$ be the prime ideal such that $R/P \simeq k[t^4, t^3u, tu^3, u^4] \subset k[t, u]$. Show that $H_{R/(P,x_0)}(2) > H_{R/(P,x_0)}(3)$ and conclude, again, that (x_0, x_1, x_2, x_3) is an embedded prime of $R/(P, x_0)$. (For later assessment, this proves that R/P has depth 1, hence it is not a Cohen–Macaulay ring.)

Exercise 2.9.36. Let $R = k[x, y, z]$, with k an infinite field, and $\mathfrak{m} = (x, y, z)$. Let $I \subset R$ be an $\mathfrak{m}$-primary ideal generated by three quadrics. Show:
(i)

$$H_{R/I}(t) = \begin{cases} 1 & \text{if } t = 0 \\ 3 & \text{if } t = 1 \\ 3 & \text{if } 2 = 0 \\ 1 & \text{if } t = 3 \\ 0 & \text{if } t \geq 4 \end{cases}$$

(One sets for short: $H_{R/I}(t) = (1, 3, 3, 1)$)
(ii) Prove that the ideal $(I :_R \mathfrak{m})/I$ is a principal ideal of R/I generated by a form of degree 3.
(iii) Prove the respective analogues of (i) and (ii) for an $\mathfrak{m}$-primary ideal generated by three cubics. What is the possible generalization for any degree $d \geq 2$?

Exercise 2.9.37. Let $R = k[x, y, z]$, with k an infinite field, and $\mathfrak{m} = (x, y, z)$. Let $I \subset R$ be an $\mathfrak{m}$-primary ideal minimally generated by 4 quadrics. Show:
(i) $H_{R/I}(t) = (1, 3, 2, \ldots)$.
(ii) Show that the length $\lambda(R/I)$ is at most 6.
(Hint: show that there exists an $\mathfrak{m}$-primary subideal $J \subset I$ generated by 3 quadrics and apply the result of the previous exercise to J; then look at the exact sequence $0 \to I/J \to R/J \to R/I \to 0$.)
(iii) Conclude that $H_{R/I}(t) = (1, 3, 2)$.

Exercise 2.9.38. Repeat the results of the previous exercise for an ideal $I \subset R$ minimally generated by 5 quadrics. In addition:

(i) $\mathfrak{m}^3 = \mathfrak{m}I$.
(Hint: use the expression of $H_{R/I}$ and the fact that $\mathfrak{m} = (I, q)$ for some (any) monomial q of degree 2 not contained in I.)

(ii) Suppose that I^2 is minimally generated by the maximal possible number $\binom{4+2}{2} = 15$ of elements. Deduce that $\mathfrak{m}^6 = I^3$.

(iii) Prove that $\mathfrak{m}^2$ and I have the same Hilbert polynomial.
(Hint: extend the equality of (ii) to any $n \geq 2$ to obtain $\mathfrak{m}^{2n} = I^n$.)

Exercise 2.9.39. Let $I \subset R = k[x, y, z]$ be an ideal minimally generated by 5 quadrics. Assume that $(I :_R \mathfrak{m})/I$ is not a principal ideal (by a later terminology, this means that R/I is not a *Gorenstein* ring).

(i) Show that $I :_R \mathfrak{m}$ contains a k-linear form and deduce, via k-linear transformation, that $I = (x\mathfrak{m}, q_1, q_2)$, for some quadrics q_1, q_2.

(ii) (k algebraically closed) Show, once more by k-linear transformations, that either $I = (x^2, xy, xz, y^2, z^2)$ or else $I = (x^2, xy, xz, yz, y^2 + \alpha z^2)$, for some $0 \neq \alpha \in k$.

3 Overview of module theory

This chapter assumes a prior knowledge of the basics of general module theory, mainly the definition and the notion of sets of generators. Most elementary properties are envisaged by mimicking the case of an ideal or of a vector space. The notable distinction from ideals, just like a vector space, is that a module is not a priori embedded in a simpler structure (such as a free module), thus making the theory a bit more involved. With Noether and even before, the notion spread out into a vast territory, strongly shared by the noncommutative theory. Sticking to commutative rings makes the general theory a lot more pliable, though not at all trivial. Some of these basics which are useful for the treatment in the book will be covered in the exercises at the end of the chapter. One of the hot topics for homology is the notion of a projective module—some of it will be discussed in Section 6.2.2.

3.1 Noetherian modules

In spite of their major role, the various ideas about finite structures in module theory did not take too long to stabilize, as compared to the idea of a module itself. The word "Modul" had been used by Dedekind and Kronecker, but only a bit later, with Noether and others, the general meaning became stable.

3.1.1 Chain conditions

Let R denote a commutative ring. In full resemblance to Lemma 2.5.1, one defines an R-module to be *Noetherian* provided it satisfies any of the conditions in the following lemma.

Lemma 3.1.1. *The following conditions are equivalent for an R-module M:*
(a) *Every submodule of M is finitely generated*;
(b) *Every chain of submodules $M_1 \subset M_2 \subset \cdots \subset M$ is stationary, i. e., there exists an index m such that $M_m = M_{m+1} = \cdots$*;
(c) *Any nonempty family of submodules of M has a maximal element.*

The proof is left to the reader as an encore of the ring case.

Proposition 3.1.2 (The Hilbert–Noether theorem). *Let R be a Noetherian ring and M an R-module. Then M is Noetherian if* (*and only if*) *M is finitely generated.*

Proof. One reduces to the case where M is a submodule of a free R-module of finite rank. To see this, take a surjective R-module homomorphism $R^n \twoheadrightarrow M$ induced by a choice of a set of generators of M with n elements, with kernel Z. Let $M' \subset M$ denote

https://doi.org/10.1515/9783110616989-003

a submodule. Since $M \simeq R^n/Z$, then $M' \simeq Z'/Z$ for some submodule $Z' \subset R^n$ containing Z. Clearly, if Z' is finitely generated then so is M'.

Thus, let $M \subset R^m$, for some m and proceed by induction on m. For $m = 1$ it boils down to the hypothesis that R is Noetherian. Thus, assume that $m \geq 2$. Taking the canonical basis of R^m one can think about the elements of M as m-tuples. Write $R^m = R \oplus R^{m-1}$ and consider the set $I_1 \subset R$ of first coordinates of all m-tuples in M. Clearly, I_1 is an ideal. Since R is assumed to be Noetherian, one has, say, $I_1 = (a_{1,1}, \ldots, a_{1,r})$. Let u_i denote a vector of M having first coordinate $a_{1,i}$, for $i = 1, \ldots, r$. By the inductive hypothesis, $M' := M \cap R^{m-1} \subset R^{m-1}$ is finitely generated, say, $M' = \sum_{j=1}^{s} Rv_j$.

Then it is clear that M is generated by the set union $\{u_1, \ldots, u_r\} \cup \{v_1, \ldots, v_s\}$. Indeed, given $u \in M$ with first coordinate c, write $c = \sum_i \alpha_i u_i$, or some $\alpha_i \in R$. Then $u - \sum_i \alpha_i u_i$ has zero as first coordinate, hence belongs to M' and, therefore, is of the form $\sum_j \beta_j v_j$. □

Condition (b) of the above lemma is called the *ascending chain condition* for modules. Reversing the sense of the inclusions, one gets the notion of an *descending chain condition*. In addition, trading "maximal" by "minimal' in condition (c) yields a condition equivalent to the latter. A module satisfying any of these conditions is named *Artinian* in honor of Emil Artin. The theory of Artinian modules has a rough parallel to the one of Artinian rings (Definition 2.5.10). In particular, if R is Artinian and M is a finitely generated R-module, then the above proposition implies that M is Noetherian. However, there are some marked differences. For example, many important Artinian modules are not finitely generated.

3.1.2 Composition series

Given an R-module, one looks for finite sequences of submodules

$$M = M_0 \supset M_1 \supset \cdots \supset M_r = \{0\}. \tag{3.1.2.1}$$

Note that one can always discard repeated submodules in the sequence, so one assume once for all the condition that M_i contains M_{i+1} properly, for every index i.

One calls a *proper refinement* of such a sequence the new sequence obtained by proper insertion of another submodule $M_i \supsetneq N \supsetneq M_{i+1}$ between some adjacent terms.

Definition 3.1.3. A sequence as in (3.1.2.1) is called a (finite) *composition series* if it admits no proper refinements. The number of terms of the series is called its *length*.

The following easily establishes a class of modules having a composition series.

Proposition 3.1.4. *Let R denote an arbitrary commutative ring. Then any R-module M which is both Noetherian and Artinian admits a composition series.*

Proof. One can assume that $M \neq \{0\}$. Since M is Noetherian, the family of proper submodules of $M_0 = M$ admits a maximal element, say, $M_1 \subset M_0$. If $M_1 = \{0\}$, one is

done since $M \supsetneq \{0\}$ is a composition series. Otherwise, choose a maximal element $M_2 \subsetneq M_1$ in the family of proper submodules of M_1. Continuing this way, one finds a strictly descending chain of submodules $M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots$ admitting no proper refinements. Since M is Artinian, this chain stabilizes, thus yielding a composition series. □

Any two terms of a composition series are tight together: since $M_i \supsetneq M_{i+1}$ admits no proper refinement, then there is some $u_i \in M_i \setminus M_{i+1}$ such that $M_i = M_{i+1} + Ru_i$ as R-modules. This implies that

$$M_i/M_{i+1} \simeq Ru_i/Ru_i \cap M_{i+1} = Ru_i/(M_{i+1} :_R u_i)u_i,$$

a cyclic module of a special type. Thus, M looks like a bunch of finitely many such cyclic modules put tightly together.

The notion itself, however, admits some stability. This was first proved by C. Jordan in the environment of finite groups.

Theorem 3.1.5 (C. Jordan [86]). *Let R denote an arbitrary commutative ring and M an R-module.*

(a) *All composition series of M have the same length.*

(b) *Suppose that M admits a composition series. Then:*

  (i) *Any finite sequence as* (3.1.2.1) *with no term repetition can be refined to a composition series.*

  (ii) *M is Noetherian and Artinian.*

Proof. (a) and (b)(i). Both assertions are vacuously true if M admits no composition series. Thus, assume M has one of length, say, $r \geq 1$:

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_r = \{0\}.$$

Induct on $r = 1$. For $r = 1$, M has no proper submodules other than $\{0\}$, hence any composition series must be the trivial one $M \supsetneq \{0\}$. In particular, every sequence as (3.1.2.1) with no repetition must be $M \supsetneq \{0\}$.

Assume that $r \geq 2$. By the inductive hypothesis, any composition series must have $s \geq r$ terms, otherwise one gets a contradiction. Let

$$M = N_0 \supsetneq N_1 \supsetneq \cdots \supsetneq N_s = \{0\}$$

stand for any sequence without repetitions.

Next, compare M_1 and N_1. If $N_1 \subset M_1$, one gets a sequence

$$M_1 \supset N_1 \supsetneq \cdots \supsetneq N_s = \{0\}.$$

Then the inductive hypothesis forces

$$r - 1 = \begin{cases} s & \text{if } N_1 \neq M_1 \\ s - 1 & \text{if } N_1 = M_1 \end{cases}$$

In any case, $s \leq r$, hence $s = r$.

Thus, assume that $N_1 \not\subset M_1$. Since M_1 is proper maximal in M, it follows that $M = M_1 + N_1$, hence $M/M_1 = M_1 + N_1/M_1 \simeq N_1/M_1 \cap N_1$, so $M_1 \cap N_1$ is a proper maximal submodule of N_1.

One claims that $M_1 \cap N_1$ admits a composition series of length at most $r-2$. This is because M_1 has a composition series and $M_1 \supsetneq M_1 \cap N_1$, hence by the inductive hypothesis of the assertion (b)(i) any sequence of $M_1 \cap N_1$ refines into a composition series of length at most one less than the length of a composition series of M_1, which is $r-1$.

Letting $P_0 = M_1 \cap N_1 \supsetneq P_1 \supsetneq \cdots \supsetneq P_t = \{0\}$ stand for a composition series of length $t \leq r-2$, one gets two composition series

$$(M = M_1 + N_1 \supsetneq) N_1 \supsetneq P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_t = \{0\} \tag{3.1.5.1}$$

Therefore, N_1 has a composition series of length $t+1 \leq r-1$. By the inductive hypothesis of assertion (b)(i) as applied to the original sequence $N_1 \supsetneq \cdots \supsetneq N_s = \{0\}$, one has $s-1 \leq r-1$, hence $s \leq r$, thus achieving both (a) and (b)(i).

(b)(ii) This is clear by (a) and (b)(i). □

Definition 3.1.6. If M is a Noetherian and Artinian module, its *length* $\lambda(M)$ is the common length of its composition series.

If M fails to be either Noetherian or Artinian, one still talks about its length as being infinite, often writing in this case $\lambda(M) = \infty$.

Proposition 3.1.7. *Let $N \subset M$ be R-modules. Then $\lambda(M) = \lambda(N) + \lambda(M/N)$, with the understanding that if one side in infinite, so is the other side.*

Proof. It is left to the reader to show that M is Noetherian (resp., Artinian) if and only if both N and M/N are Noetherian (respe., Artinian). Thus, assume that M is both Noetherian and Artinian, so $\lambda(M) < \infty$ and also $\lambda(N) = r < \infty$, $\lambda(M/N) = s < \infty$. Let $M/N \supsetneq M_1/N \supsetneq \cdots \supsetneq M_s/N = N/N = \{0\}$ be a composition series of M/N and let $N \supsetneq N_1 \supsetneq \cdots \supsetneq N_r = \{0\}$ be one of N. Then

$$M \supsetneq M_1 \supsetneq \cdots \supsetneq M_s = N \supsetneq N_1 \supsetneq \cdots \supsetneq N_r = \{0\}$$

is a composition series of M. □

3.2 External operations

So far, one has dealt mainly with certain internal behavior of a module. In this regard, just a few of the usual operations with ideals of a ring can be mimicked by submodules M, N of a given module, such as the sum $M + N$ (not a great gain since the outcome is just the smallest submodule containing M and N).

Other important operations whose results do not leave the ambient module $\mathcal{M}$ requires the intervention of an ideal $I \subset R$, such as the quotient $M :_{\mathcal{M}} I$ or, in the event of a local ring $(R, \mathfrak{m})$, the *socle* $0 :_M \mathfrak{m}$ of a finitely generated R-module M.

Therefore, it looks pretty urgent to try out some external operations involving two modules. The main ones are the tensor product and the homomorphisms. Thus, given R-modules M and N, one defines their tensor product $M \otimes_R N$ and the set of homomorphisms $\mathrm{Hom}_R(M, N)$. Both turn out to be R-modules, with a big difference: the first is insensitive to the order in which the modules were taken, while the second one gives different results except in the case where $M = N$.

However, nature is often capricious as the module of homomorphisms requires no new definition, while the tensor product does.

One does it by means of a universal property, stressing generators and relations.

Definition 3.2.1. Let $\mathfrak{F}^{M\times N}$ denote the free R-module having the cartesian product $M \times N$ as basis, and let $\mathfrak{T}$ be the R-submodule generated by the following elements:

$$\begin{cases} (u+u',v)-(u,v)-(u',v) & \text{for } u,u\in M', v\in N \\ (u,v+v')-(u,v)-(u,v') & \text{for } u\in M, v, v'\in N \\ a(u,v)-(au,v),\ a(u,v)-(u,av) & \text{for } u\in M, v\in N, a\in R. \end{cases}$$

Set $M \otimes_R N := \mathfrak{F}^{M\times N}/\mathfrak{T}$.

Setting $u \otimes v$ for the residue of the basis element (u, v) yields all tensor relations one needs for the theory.

Let $\mathfrak{t}$ denotes the restriction to $M \times N$ of the residue map above. The underlying universal property of this construction is as follows.

Proposition 3.2.2. *For any R-module L and any R-bilinear map $\mathfrak{b} : M \times N \to L$, there exists a unique R-homomorphism $\varphi : M \otimes_R N \to L$ such that $\varphi \circ \mathfrak{t} = \mathfrak{b}$.*

Proof. Since the elements of $M \times N$ form a free basis of $\mathfrak{F}^{M\times N}$, then $\mathfrak{b}$ induces an R-homomorphism $\mathfrak{F}^{M\times N} \to L$ such that $\sum_i a_i(u_i, v_i) \mapsto \sum_i a_i \mathfrak{b}(u_i, v_i)$. By this map, clearly $\mathfrak{T}$ maps to zero due to bilinearity of $\mathfrak{b}$. Therefore, one has an induced R-homomorphism from $M \otimes_R N$ to L satisfying the composition assertion. Uniqueness is left to the reader. □

This is the so-called "linearization" of a bilinear map. Conversely, one can show that the associated universal problem has a unique solution up to R-isomorphisms and is described as in the above definition.

The tensor product has the following elementary properties:

- The definition can be extended to the tensor product of finitely many modules.
- As such, it is an associative operation and, moreover, for an integer $t \geq 0$, the tensor power $M^{\otimes t}$ is defined (with the convention that $M^{\otimes 0} = R$ and $M^{\otimes 1} = M$).
- For any two R-modules M and N, one has $M \otimes_R N \simeq N \otimes_R M$ in a natural way.
- The operations is "distributive" relative to the direct sum of finitely many modules.

The verification of these properties is left to the reader, as they are consequences of the universal property. For a complete account on the properties and full functionality of the tensor product, the reader is referred to the excellent expository notes by K. Konrad ([96]).

A third and fourth operations are very useful, except that they are exclusively unary. One cannot universally define the ordinary power of a module—if as to mimic the case of an ideal. For that to work, one needs in principle to have the module embedded in a free module and even then one needs a higher level of technology (Rees algebras of modules). Luckily, there are two sorts of "power raising" that work quite well and are very useful. They are the notion of an exterior power and a symmetric power, emanating from the idea of skew-symmetric and symmetric maps $M^t \to N$, where $M^t = M \times \cdots \times M$ (t times).

Exterior power is an important tool in the theory of Koszul complexes and their modifications, to be studied in Section 6.3.

One establishes the basics of this concept once more by means of introducing an object by generators and relations, then arguing that it solves a certain universal problem.

Definition 3.2.3. Let M be an R-module and $t \geq 0$. Let $\mathfrak{W} \subset M^{\otimes t}$ denote the submodule generated by the elements of the form $u_1 \otimes \cdots \otimes u_t$, where $u_i = u_j$ for at least two indices $i \neq j$ (for $t = 0, 1$, one sets $\mathfrak{W} = \{0\}$). The tth *exterior power* of M is $\bigwedge^t M := M^{\otimes t}/\mathfrak{W}$.

Let $\mathfrak{w}$ denote the composite map of $\mathfrak{t} : M^t \to M^{\otimes t}$ and the residue map $M^{\otimes t} \twoheadrightarrow \bigwedge^t M$. Note that $\mathfrak{w}$ is an R-multilinear map.

The corresponding universal property is the following.

Proposition 3.2.4. *For any R-module N and any alternating R-multilinear map $\mathfrak{a} : M^t \to N$, there exists a unique R-homomorphism $\psi : \bigwedge^t M \to N$ satisfying $\psi \circ \mathfrak{w} = \mathfrak{a}$.*

The proof is now entirely left to the reader.

As in the case of the tensor product, the residue of a tensor $u_1 \otimes \cdots \otimes u_t$ is denoted $u_1 \wedge \cdots \wedge u_t$ and called a *wedge product*.

Among the useful properties of exterior powers, the following ones stand out:

- If M has a finite set of generators over R of cardinality r, then $\bigwedge^t M = \{0\}$ for $t > r$.
- If $\{u_1, \ldots, u_r\}$ generates M over R, then $\bigwedge^t M$ is generated by the wedge products $u_{i_1} \wedge \cdots \wedge u_{i_t}$, for all choices $1 \leq i_1 < \cdots < i_t \leq r$.
- In particular, if M is free with the generating set above being a free basis, then $\bigwedge^t M$ is free on the above set of wedge products.
- An R-homomorphism $M \to N$ induces natural R-homomorphisms $\bigwedge^t M \to \bigwedge^t N$ for all $t \geq 1$.
- For given integers $s, t \geq 0$, there is a natural "glue-together multiplication" R-bilinear map $\bigwedge^s M \times \bigwedge^t M \to \bigwedge^{s+t} M$.
- If M' is a direct summand of a module M, then for every $t \geq 1$, $\bigwedge^t M'$ is a direct summand of $\bigwedge^t M$.

The third listed property above has a surprising converse. It will require the concept of the torsion submodule $\tau(M)$ of a module M to be given at the end of the entire chapter.

Proposition 3.2.5. *Let R be a Noetherian local ring, let M be a finitely generated R-module, and let $t \geq 1$ be an integer. If $\bigwedge^t M$ (resp., $\bigwedge^t M/\tau(\bigwedge^t M)$) is free and nonzero then M (resp., $M/\tau(M)$) is free.*

Proof (*According to Vasconcelos*). One argues by induction on t. Since the assertion is obvious for $t = 1$, assume that $t \geq 2$. Using the universal properties, there is a composite surjective R-homomorphism $M \otimes_R \bigwedge^{t-1} M \twoheadrightarrow \bigwedge^t M/\tau(\bigwedge^t M)$. Since $\bigwedge^t M/\tau(\bigwedge^t M)$ is free and nonzero, one has plenty of surjective R-homomorphisms $M \otimes \bigwedge^{t-1} M \to R$. But there also maps $M \to M \otimes \bigwedge^{t-1} M$ obtained by tensoring with any element of $\bigwedge^{t-1} M$. Therefore, the composition of any two such homomorphisms gives an R-homomorphism $M \to R$. But since R is local, one of these R-homomorphisms has to be surjective. Thus, one has a splitting $M = R \oplus M'$. Applying the result of the last bulleted property above yields that $\bigwedge^{t-1} M'$ is a direct summand of $\bigwedge^t M$. Therefore, $\bigwedge^{t-1} M'$ (resp., $\bigwedge^{t-1} M'/\tau(\bigwedge^{t-1} M')$) is free.

One now claims that $\bigwedge^{t-1} M'/\tau(\bigwedge^{t-1} M') \neq 0$ or, equivalently, $K \otimes_R \bigwedge^{t-1} M' \neq 0$, where K is the total ring of quotients of R. Since $M = R \oplus M'$, one obtains $K \otimes_R \bigwedge^t M \simeq (K \otimes_R \bigwedge^{t-1} M') \oplus (K \otimes_R \bigwedge^t M')$. However, $K \otimes_R \bigwedge^t M \neq 0$ by our assumption, hence $K \otimes_R \bigwedge^{t-1} M'$ or $K \otimes_R \bigwedge^t M'$ is not zero, which indeed gives $K \otimes_R \bigwedge^{t-1} M' \neq 0$. Now apply the inductive hypothesis. □

An important construction is the exterior algebra of a module. In contrast to the more popular symmetric algebra (see below), which is a commutative R-algebra, the exterior algebra is skew-commutative. The multiplication of this algebra is induced by the map in the last bullet above. As mentioned before, the main use of it in this book is related to the Koszul complex (Section 6.3).

The reader is referred to the expository paper [97] for further basic properties of exterior powers.

One now briefly revises the idea of the symmetric power of a module.

Definition 3.2.6. Let M be an R-module and $t \geq 0$. Let $\mathfrak{S} \subset M^{\otimes t}$ denote the submodule generated by the elements of the form

$$u_1 \otimes \cdots \otimes u_i \otimes \cdots \otimes u_j \otimes \cdots \otimes u_t - u_1 \otimes \cdots \otimes u_j \otimes \cdots \otimes u_i \otimes \cdots \otimes u_t,$$

for any two indices i, j (for $t = 0, 1$, one sets $\mathfrak{S} = \{0\}$). The tth *symmetric power* of M is $S^t(M) := M^{\otimes t}/\mathfrak{S}$.

And once more, the corresponding universal property is the following.

Proposition 3.2.7. *For any R-module N and any symmetric R-multilinear map $\mathfrak{c} : M^t \to N$, there exists a unique R-homomorphism $\kappa : S^t M \to N$ satisfying $\kappa \circ \mathfrak{s} = \mathfrak{c}$, where $\mathfrak{s}$ is the composite of $\mathfrak{t}$ and the residue map to $S^t M$.*

The residue of a tensor $u_1 \otimes \cdots \otimes u_t$ is denoted $u_1 \bullet \cdots \bullet u_t$, if for lack of a better notation.

Alas, this is not the most useful property of the symmetric powers. Instead, one takes the *symmetric algebra* of the R-module to be the direct sum

$$S(M) = S_R(M) := \bigoplus_{t \geq 0} S^t M,$$

endowed with the multiplication induced by the map $S^s M \times S^t M \to S^{s+t} M$ given by $(u_1 \bullet \cdots \bullet u_s, u_1 \bullet \cdots \bullet u_t) \to u_1 \bullet \cdots \bullet u_s \bullet u_1 \bullet \cdots \bullet u_t$.

It turns out that $S(M)$ is a commutative R-algebra and, as such it comes along with the following universal property: for every commutative R-algebra A and every R-homomorphism $M \to A$ (A being thought of as an R-module), there exists a unique map of R-algebras $S(M) \to A$ satisfying the obvious composition of maps.

Recall the similarity of this property to that of a polynomial ring over R, and, in fact, that is the case when M is a free R-module.

The reader will easily fill in all the required details of this discussion. More on the symmetric algebra in Section 7.2.

3.3 Free presentation and Fitting ideals

Let R denote a commutative ring.

Definition 3.3.1. A sequence of R-module homomorphisms indexed by $\mathbb{Z}$

$$\cdots \to N_{i-1} \xrightarrow{\varphi_{i-1}} N_i \xrightarrow{\varphi_i} N_{i+1} \to \cdots \tag{3.3.1.1}$$

is called an *exact sequence* if $\ker \varphi_i = \mathrm{Im} \varphi_{i-1}$ for all i.

If 0 is one of the modules in an exact sequence, then one can split the latter into two other ones, called respectively, *right exact* and *left exact*. The appearance of two zeros in distinct positions yields a finite exact sequence. A special case of this has the form $0 \to Z \longrightarrow N \longrightarrow M \to 0$, called a *short exact sequence*. Often one is interested in the left exact or right exact versions of such a short exact sequence.

As a particular, but extremely important, situation, one finds a *free presentation* of a module M, which is a short right exact sequence of the shape

$$F_1 \xrightarrow{\varphi} F_0 \longrightarrow M \longrightarrow 0, \tag{3.3.1.2}$$

where F_0 and F_1 are free modules.

Throughout one assumes that R is a Noetherian ring and M a finitely generated R-module. Then F_0 can be taken to be of finite rank, say, $\operatorname{rank} F_0 = n$, and F_1 is necessarily of finite rank as well. Let $0 \leq r \leq n$ denote an integer. The *Fitting invariant of M of order r* is the determinantal ideal $I_{n-r}(\varphi)$ of a matrix associated to φ. Fitting ([58]) showed that the definition depends only on M and not on the selected presentation.

Theorem 3.3.2 (Fitting). *Let* $F_1 \xrightarrow{\varphi} F_0 \xrightarrow{\pi} M \to 0$ *and* $F_1' \xrightarrow{\varphi'} F_0' \xrightarrow{\pi'} M \to 0$ *be free presentations, where* $\operatorname{rank} F_0 = n$, $\operatorname{rank} F_0' = n'$. *Then* $I_{n-s}(\varphi) = I_{n'-s}(\varphi')$ *for every* $s \geq 0$.

Proof. Here is a typical argument that the reader will have no difficulty in establishing rigorously. By a well-known "inflation" tactic, one can reduce the problem to the simplest case where, say, $F_0' = F_0 \oplus R$ (*i. e.*, $n' = n+1$). In this case, fixing a basis $\{e_1, \ldots, e_n\}$ of F_0, extend it to a basis $\{e_1, \ldots, e_n, e\}$ of F_0'. There follows the obvious exact commutative diagram of R-modules and module homomorphisms,

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & Z & \to & F_0 & \xrightarrow{\pi} & M & \to & 0 \\
 & & \downarrow & & \downarrow & & \| & & \\
0 & \to & Z' & \to & F_0 & \xrightarrow{\pi'} & M & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & Z/Z' & \to & R & \to & 0 & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

where π denotes the restriction of π' to F_0. Therefore, $Z/Z' \simeq R$, so the leftmost vertical arrow is split. Bringing back F_1 and F_1' into scene, one sees that up to a change of bases in these two modules:

$$\varphi' = \begin{pmatrix} \varphi & 0 \\ 0 & 1 \end{pmatrix},$$

from which the equalities $I_{n-s}(\varphi) = I_{n'-s}(\varphi')$ for every $s \geq 0$ follow. □

The two most important Fitting ideals are $\mathcal{F}_0(M)$ and provided M has rank r (to be appropriately defined in the sequel), $\mathcal{F}_r(M)$.

One treats $\mathcal{F}_0(M)$ first. Denote by $0 :_R M$ (or simply $0 : M$) the *annihilator* of the module M. By definition, $0 :_R M = \{a \in R \mid ax = 0 \ \forall x \in M\}$.

Proposition 3.3.3. *For a finitely generated* R*-module* M, $\sqrt{0 :_R M} = \sqrt{\mathcal{F}_0(M)}$.

Proof. One first shows that $\mathcal{F}_0(M) \subset 0 :_R M$. In the notation of (3.3.1.2), let $\{e_1, \ldots, e_n\}$ be a basis of F_0. Then $M \simeq F_0/\varphi(F_1)$, so by expanding an $n \times n$ minor Δ of φ by the Laplace rule will, after a calculation, yield $\Delta \cdot e_i \equiv 0 \pmod{\varphi(F_1)}$, for every i. This proves the required inclusion.

For the reverse radical wise inclusion, let $P \subset R$ be a prime ideal containing $\mathcal{F}_0(M)$. The claim is that $M_P \neq 0$, hence it will follow that $0 :_R M \subset P$, as required. Indeed, if $M_P = 0$, then by the usual elementary transformation method, one can find bases of

F_0 and F_1 such that locally at P:

$$\varphi_P = \left(\begin{array}{cccc|c} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \end{array}\right),$$

where the unspecified entries are all zero. Thus, $I_n(\varphi)_P = I_n(\varphi_P) = R_P$, contradicting the assumption that $I_n(\varphi) \subset P$. □

Remark 3.3.4. The above argument can be turned in the assertion that $(0 :_R M)^n \subset \mathcal{F}_0(M)$.

To deal with the other Fitting ideals, one needs to introduce a notion of rank of a module. For a general Noetherian ring R, not all modules will have a rank. Switching to finite free presentations, accordingly not every free map will have a rank since ranks are expected to add up in an exact sequence. On the other hand, the ordinary notion of rank of a matrix inherited from linear algebra over a field (hence, over a domain as well) is largely satisfactory. To have both notions on the same foot, one reinstates the following concept.

Definition 3.3.5. A free R-map (or matrix) φ has *rank* $s \geq 0$ if $I_t(\varphi) = 0$ for every $t > s$ and grade $I_s(\varphi) \geq 1$.

Here, the *grade* of an ideal is the length of a regular sequence of maximal length inside the ideal; in other words, for an ideal $I \subset R$ in a Noetherian ring, one has $\operatorname{grade} I = \operatorname{depth}_I(R) \leq \operatorname{ht} I$ (Proposition 5.3.11).

The old definition (over a field or a domain) would merely require that $I_s(\varphi) \neq 0$, so every matrix φ would automatically have a rank. By the present definition, this is not automatically ensured and it is trivial to write a matrix with no rank over a ring with proper zero-divisors.

Definition 3.3.6. A finitely generated R-module M *has rank* $r \geq 0$ if M_P is R_P-free of rank r for every $P \in \operatorname{Ass} R$.

It can be shown that a finitely generated R-module M has rank r if and only if the $\mathfrak{S}^{-1}R$-module $\mathfrak{S}^{-1}M$ is free of rank r, where $\mathfrak{S} = R \setminus \bigcup_{P \in \operatorname{Ass} R} P$.

Next is the impact of this notion on modules. In practice, it is more convenient to work from a fixed presentation and with the corresponding determinantal ideals. Let $\mu(M)$ denote the minimal cardinality of a set of generators of a finitely generated module over a Noetherian local ring (it will be shown in Section 5.1.2 that this is a bonafide invariant of M).

Proposition 3.3.7. *Let* $F_1 \xrightarrow{\varphi} F_0 \to M \to 0$ ($\operatorname{rank} F_0 = n$) *be a free presentation. The following conditions are equivalent for an integer* $s \geq 0$*:*

(i) $\operatorname{rank}\varphi = s$
(ii) *M_P is R_P-free of rank $n - s$ for every $P \in \operatorname{Ass} R$.*

Proof. (ii) $\Rightarrow$ (i) One can assume that R is local and its maximal ideal $\mathfrak{m}$ is an associated prime, and that M is free of rank $n - s$. One intends to show that $I_s(\varphi) = R$ (which is the only possible meaning for $\operatorname{grade} I_s(\varphi) > 0$ when $\mathfrak{m} \in \operatorname{Ass} R$) and that $I_t(\varphi) = 0$ for every $t > s$. Now, since M is free, after possibly changing bases, there is a splitting of the form $F_1 = R^s \oplus F_1' \xrightarrow{\varphi} F_0 \simeq R^s \oplus M$, where the restriction of φ to R^s is the identity and to F_1' is the zero map. Therefore, one is done by Theorem 3.3.2.

The reverse implication will be a consequence of the general result to follow. □

Lemma 3.3.8. *Let $F_1 \xrightarrow{\varphi} F_0 \to M \to 0$ ($\operatorname{rank} F_0 = n$) be a free presentation. The following conditions are equivalent for an integer $s \geq 0$ and a prime ideal $P \subset R$:*
(i) $I_s(\varphi) \not\subset P$
(ii) $\mu(M_P) \leq n - s$.

Proof. Localizing at P and possibly changing the bases of the free modules in (3.3.1.2), one arrives to a presentation of M_P of the form

$$R_P^k \oplus R_P^r \xrightarrow{\mathrm{id}\oplus\varphi} R_P^k \oplus R_P^\mu \longrightarrow M_P \longrightarrow 0,$$

where $k = \operatorname{rank} F_0 - \mu$ and $\mu = \mu(M_P)$. Then the matrix of φ has entries in P_P, and from this, one clearly sees that $I_t(\varphi) \subseteq P$ if and only if $t \geq t + 1$, which shows the main assertion. The proof of the supplementary assertion is left to the reader. □

By Proposition 3.3.7, M has rank r if and only if φ has rank $n - r$ for any free presentation $F_1 \xrightarrow{\varphi} F_0 \to M \to 0$ ($\operatorname{rank} F_0 = n$). Alternatively, one can state the following.

Corollary 3.3.9. *If M is finitely generated with rank r, then $\mathcal{F}_r(M)$ is the nonfree locus of M, i. e., M_P is R_P-free of rank r for a prime ideal $P \subset R$ if and only if $\mathcal{F}_r(M) \not\subset P$.*

The above results admit a uniform version for all relevant values of t taken at once.

Proposition 3.3.10. *Let M be a finitely generated R-module having a rank. The following conditions are equivalent for an integer $k \geq 0$:*
(i) *For every $P \in \operatorname{Spec} R$, the inequality*

$$\mu(M_P) \leq \operatorname{ht} P + \operatorname{rank} M + k$$

holds (*resp., and for some $P \in \operatorname{Spec} R$ the equality is attained*).
(ii) *For* any *presentation as* (2.2.6.1) *and any $1 \leq t \leq \operatorname{rank}(\varphi)$, the inequality*

$$\operatorname{ht} I_t(\varphi) \geq \operatorname{rank}\varphi - t + 1 - k$$

holds (*resp., and for some $1 \leq t \leq \operatorname{rank}\varphi$ the equality is attained*).

(iii) *For* some *presentation as* (2.2.6.1) *and any* $1 \le t \le \operatorname{rank}(\varphi)$, *the inequality*

$$\operatorname{ht} I_t(\varphi) \ge \operatorname{rank} \varphi - t + 1 - k$$

holds (*resp., and for some* $1 \le t \le \operatorname{rank} \varphi$ *the equality is attained*).

Proof. First, argue for the inequalities.

(i) $\Rightarrow$ (ii) Given t in the required interval, pick a prime $P \supset I_t(\varphi)$ such that $\operatorname{ht} I_t(\varphi) = \operatorname{ht} P$. Then

$$\operatorname{ht} I_t(\varphi) \ge \mu(M_P) - \operatorname{rank} M - k = \operatorname{rank} \varphi - s_P - k,$$

where $s_P := \operatorname{rank} F - \mu(M_P)$. By Lemma 3.3.8, one has $s_P \le t - 1$, as required.

(ii) $\Rightarrow$ (iii) Trivial.

(iii) $\Rightarrow$ (i) Let $P \in \operatorname{Spec} R$ and s_P as above. Then $I_{s_P} \subseteq P$ by Lemma 3.3.8. On the other hand,

$$\begin{aligned} s_P &= \operatorname{rank} F - \mu(M_P) \\ &\le \operatorname{rank} F - \operatorname{rank} M = \operatorname{rank} \varphi. \end{aligned}$$

Then, by the assumption, $\operatorname{ht} P \ge \operatorname{rank} \varphi - s_P - k = \mu(M_P) - \operatorname{rank} M - k$, as needed to be shown.

Finally, the supplementary assertions as to when the equalities are attained follow from the corresponding ones in Proposition 3.3.7. □

Proposition 3.3.10 motivates the following notion.

Definition 3.3.11. The least $k \ge 0$ such that M satisfies (any of) the conditions of Proposition 3.3.10 is called the *Fitting defect* of M, denoted $\operatorname{fd} M$; M is said to satisfy $(\mathfrak{F}_{-k})$ if $k \ge \operatorname{fd} M$.

The Fitting defect is actually a dimension defect for the symmetric algebra $S_R(M)$. Namely, one has the following result, here stated without proof:

Theorem 3.3.12 ([141, Theorem 1.1.3]). *Let R denote a Noetherian catenary domain and let M stand for a finitely generated R-module. Then*

$$\dim S_R(M) = \dim R + \operatorname{rank} M + \operatorname{fd} M.$$

The number $\dim R + \operatorname{rank} M$ is the dimension of the so-called *Rees algebra* $\mathcal{R}_R(M)$ of M, to be discussed in Section 7.3. Since under the present hypothesis there is a natural surjection $S_R(M) \twoheadrightarrow \mathcal{R}_R(M)$, the introduced terminology is justified.

On the other hand, a version of the property $(\mathfrak{F}_{-k})$ is available for negative values of k, as was extensively treated in the survey work [70]. It is customary in this case, to turn around the notation, by assuming that $k \ge 0$ and asking that the inequality

$$(F_k): \quad \mu(M_P) \le \operatorname{ht} P + \operatorname{rank} M - k \tag{3.3.12.1}$$

holds for every $P \in \operatorname{Spec} R$ not lying in the free locus of M.

Note that $(\mathfrak{F}_0)$ and (F_0) are one and the same condition. The latter property for $k > 0$ has no impact on the dimension. Its main bearing is to the finer properties of M. In the case of an ideal $I \subset R$ having a regular element, (F_1) reads as $\mu(I_P) \leq \dim R_P$ for every prime ideal $P \subset R$ containing I. This condition was originally introduced in [6] under the notation (G_∞), without requiring that I contain a regular element, in which case necessarily $I_P = 0$ for every minimal prime ideal of R containing I.

3.4 Torsion and torsion-free modules

Let M be an R-module, where R is a commutative ring.

An element of M is a *torsion element* if $ax = 0$ for some regular element $a \in R$. The subset of such elements is a submodule of M, denoted $\tau_R(M)$, and called the *torsion submodule* of M.

More exactly, one has the following straightforward.

Lemma 3.4.1. *Let $K := \mathfrak{S}^{-1}R$ denote the total ring of fractions of R, where $\mathfrak{S}$ is the set of regular elements of R. Then $\tau_R(M) = \ker(M \to \mathfrak{S}^{-1}M)$.*

M is called *torsion-free* (resp., *torsion*) if $\tau_R(M) = 0$ (resp., $\tau_R(M) = M$).

It follows easily from the definition that a free module is torsion-free. Clearly, ideals are torsion-free modules.

For the next result, see the notion of *depth* in Section 5.3.1.

Lemma 3.4.2. *A finitely generated R-module M is torsion if and only if*

$$\operatorname{depth}_{(0:M)}(R) \geq 1.$$

Proof. If $\operatorname{depth}_{(0:M)}(R) \geq 1$, let $a \in (0 : M) \setminus \mathcal{Z}(R)$. Then $aM = 0$, so M is torsion.

Conversely, write $M = \sum_{i=1}^{m} Rx_i$. If M is torsion, let $a_i \notin \mathcal{Z}(R)$ such that $a_i x_i = 0$. Then $a := \prod_i a_i \in (0 : M) \setminus \mathcal{Z}(R)$. □

In other words, a finitely generated R-module M is torsion if and only if the annihilator of M has a well-defined rank (necessarily 1).

A submodule of a torsion-free module is torsion-free. In particular, a submodule of a free module is torsion-free—such modules have sometimes been referred as *torsionless* (*cf.* [27]). There is a weak converse as follows.

Proposition 3.4.3. *Let M be a finitely generated R-module. The following are equivalent:*

(i) *M is torsion-free and has a rank.*

(ii) *M is torsionless and $\operatorname{grade}(M : F) \geq 1$ for some embedding $M \hookrightarrow F$ into a free module F of finite rank.*

Proof. (i) ⇒ (ii) By definition of rank and by Lemma 3.4.1, the assumptions mean that $\mathfrak{S}^{-1}M$ is $\mathfrak{S}^{-1}R$-free of finite rank and the natural map $M \to \mathfrak{S}^{-1}M$ is injective, where $\mathfrak{S} = R \setminus \bigcup_{P\in \operatorname{Ass} R} P$. Let $\{e_1/s, \dots, e_r/s\}$ be a K-basis of $= \mathfrak{S}^{-1}M$ for an appropriate $s \in \mathfrak{S}$. Then this set is still linearly independent over R since $R \hookrightarrow K$. Therefore, they generate a free R-module F of rank r and, clearly, $M \hookrightarrow \mathfrak{S}^{-1}M$ factors through $M \hookrightarrow F$. Let us show that $\operatorname{grade}(M : F) \geq 1$, as required. Thus, let $P \in \operatorname{Ass} R$. Then $M_P = \mathfrak{S}^{-1}M_{\mathfrak{S}^{-1}P}$, hence also $M_P = F_P$, therefore, $(M : F)_P = (M_P : F_P) = R_P$. This means that $(M : F) \not\subset P$, as intended.

(ii) ⇒ (i) As previously observed, M is torsion-free. To see that M has a rank, note that the hypothesis to the effect that $\operatorname{grade}(M : F) \geq 1$ implies, conversely, $(M : F) \not\subset P$ for every $P \in \operatorname{Ass} R$, hence by the same token $M_P = F_P$ for every $P \in \operatorname{Ass} R$. □

A convenient notion in the theory of free resolutions is that of a module of syzygies. In a more precise way, one has the following.

Definition 3.4.4. Let $n \geq 1$ be an integer. An nth *syzygy module* is a finitely generated R-module M that fits in an exact sequence $0 \to M = F_n \to \cdots \to F_1 \to F_0$ with F_i free of finite rank.

Thus, a first syzygy module is exactly a torsionless module. Second syzygies are very important. To see this, one says that a module M is *reflexive* if the natural map $M \to M^{**}$ to its double R-dual is an isomorphism.

There is a kind of (dual) analogue to Proposition 3.4.3 for reflexive modules.

Proposition 3.4.5. *Let M be a finitely generated R-module. The following are equivalent:*
(i) *M is reflexive and has a rank.*
(ii) *There is a free map $F_2 \xrightarrow{\psi} F_1$ with rank such that $M = \ker(\psi)$.*

Proof. (i) ⇒ (ii) Since M has a rank, so does its first R-dual M^*. Let $F_1 \xrightarrow{\varphi} F_0 \to M^* \to 0$ be a free presentation. Then φ has a rank and $M^{**} = \ker(\psi)$ where ψ is the dual map to φ. Obviously, ψ has the same rank as φ and since $M = M^{**}$ one is through.

(ii) ⇒ (i) Since M is the kernel of a free map having a rank then by a previous exercise, M has a rank. Therefore, M^{**} has the same rank. On the other hand, there is a natural exact commutative diagram of R-maps

$$\begin{array}{ccccccc} 0 & \to & M & \to & F_2 & \xrightarrow{\psi} & F_1 \\ & & \downarrow & & \| & & \| \\ & & M^{**} & \to & F_2^{**} & \xrightarrow{\psi^{**}} & F_1^{**}. \end{array}$$

By the ker-coker sequence ("snake diagram"), the leftmost vertical map has to be an isomorphism. □

Next are other special results on torsion-free modules.

Proposition 3.4.6. *Let R be an integral domain and let $M \subset N \subset R^m$ be finitely generated submodules of a free module, having the same rank g. Let $I \subset R$ denote the Fitting ideal of order $m - g$ of the cokernel R^m/M. Then $I \subset M : N$.*

Proof. By definition, I can be taken to be the ideal generated by the $g \times g$ minors of the matrix whose columns are the generators of M expressed as linear combinations of the canonical basis of R^m. Thus, let $\Delta \in I$ denote a nonzero determinant thereof. One may assume for simplicity that it is the determinant of the $g \times g$ submatrix on the upper left corner. Given any $i = g+1, \ldots, m$, consider the following $(g+1)\times g$ submatrix of the columns generating M:

$$\begin{pmatrix} u_{1,1} & u_{1,2} & \cdots & u_{1,g} \\ u_{2,1} & u_{2,2} & \cdots & u_{2,g} \\ \vdots & \vdots & & \vdots \\ u_{g,1} & u_{g,2} & \cdots & u_{g,g} \\ u_{i,1} & u_{i,2} & \cdots & u_{i,g} \end{pmatrix}$$

Now, given any column generator of N, right border the above matrix with the corresponding entries $v_1, \ldots, v_g, v_i$ of this column to get a $(g+1)\times(g+1)$ matrix whose columns are elements of N. These generate a submodule of N, hence has rank at most g. Therefore, the corresponding $(g+1)\times(g+1)$ determinant vanishes. Expanding this determinant by Laplace along the bottom row, one finds

$$\Delta v_i = \Delta_{\hat{1}2\ldots gv} u_{i,1} + \Delta_{1\hat{2}3\ldots gv} u_{i,2} + \cdots + \Delta_{12\ldots\hat{g}v} u_{i,g}, \tag{3.4.6.1}$$

where $\Delta_{12\ldots\hat{j}\ldots gv}$ denotes the (signed) g-minor with column v in place of the jth column.

If, on the other hand, $i \in \{1, \ldots, g\}$ then one obtains again a $(g+1)\times(g+1)$ matrix by first bordering the initial $g \times g$ submatrix with the entries $v_1, \ldots, v_g$ and then repeating the ith row of this matrix on the bottom. Clearly, this determinant is zero; expanding it as before along the repeated row, one finds a similar expression as (3.4.6.1), with the same fixed g-minors as multipliers. This shows that the entire column generator $v \in N$ is conducted by Δ inside M. □

Less elementary, still very useful is the following result. An ideal $I \subset R$ is said to be *height unmixed* (or, simply *unmixed*) if all its associated prime ideals have the same height.

Proposition 3.4.7 (O. Goldman). *Let R be a Noetherian normal domain and let $M \subset N$ stand for finitely generated R-modules of the same rank such that M is reflexive and N is torsion-free. Then $M :_R N$ is an unmixed ideal of height* 1.

Proof. **Claim 1.** One can assume that $N = M + Ru$, for some $u \in N$.

To see this, take generators $u_1, \ldots, u_n$ of N. Then $M :_R N = \bigcap_{i=1}^n M :_R Ru_i$. Clearly, if every $M :_R Ru_i$ is unmixed of height one then so is $M :_R N$.

Next, let K denote the field of fractions of R, so that $\mathrm{Hom}_R(M,R)\otimes_R K \simeq \mathrm{Hom}_K(M\otimes_R K, K)$. Given $h \in \mathrm{Hom}_R(M,R)$, let $\tilde{h} = h/1 = h\otimes 1$.

Claim 2. $M :_R N = \{a \in R \mid \tilde{h}(au) \in R, \text{for every} h \in \mathrm{Hom}_R(M,R)\}$.

Indeed, the inclusion $\subset$ is clear, so let $a \in R$ belong to the right-side member. Thus, one has an R-homomorphism $\mathrm{Hom}_R(M,R) \to R$ given by $h \mapsto \tilde{h}(au)$. Since M is reflexive, one has $\mathrm{Hom}_R(\mathrm{Hom}_R(M,R),R) = M$, hence there is an element $v \in M$ such that $\tilde{h}(au) = h(v) = \tilde{h}(v)$ for every $h \in \mathrm{Hom}_R(M,R)$. It follows that $\tilde{h}(au - v) = 0$ for every $h \in \mathrm{Hom}_R(M,R)$. This implies that $au = v$, *i. e.*, $a \in M :_R N$.

Sum up for the conclusion: letting $\{h_1,\dots,h_m\}$ be a set of generators of $\mathrm{Hom}_R(M,R)$ clearly $M :_R N = \{a \in R \mid \tilde{h_j}(au) \in R, j = 1,\dots,m\}$. Setting $\tilde{h_j}(u) = a_i/b$, one gets $M :_R N = \bigcap_j (b) : a_i$. Since R is normal, the principal ideal (b) is unmixed of height one, hence so is each factor $(b) : a_i$. □

3.5 Historic note

3.5.1 Composition series

Interestingly enough, the discovery of chain conditions for rings and modules, as crystallized in the hands of E. Noether and W. Krull, was an offspring of the early development of group theory. With Lagrange's and Vandermone's preliminary incursion, followed by Cauchy's solid theory of subgroups of the symmetric group, a whole theory of substitutions was going around. Unfortunately, so it appears, Cauchy left the arena quite early, while Galois didn't live enough to complete his remarkable work. True, no disastrous vacuum took place, with group theory continuing to flash its colors in many other forms, specially in the line of S. Lie's differential-minded infinite groups—a line of work that had its climax in Klein's famous Erlangen program. It is said that Klein, being mostly inclined to physics and geometry, benefited from conversation with the algebraist-analyst C. Jordan about the principles of group theory. Thus, one arrives at the crux of the birthplace of the idea of a composition series. It was Jordan that established a fairly complete theory in his famous *Traité* ([86]). One has to understand the boldness of Jordan's treatise within an intense period of mathematical output in Europe, where strong-minded scholars like Kronecker, Klein and Dedekind were imposing their influence. Finite group theory didn't look like a bright prospect to most of them. But there he went, Jordan, writing his second treatise (first one was in analysis). Today's readers may find the language and notation of the book a bit unsavored, but the style is clear and perfectly readable. One would think that writing on group theory, nearly half a century after Cauchy's remarkable paper, would bring the style closer to our notation these days. It had to wait a bit more for it to happen, with O. Hölder's subsequent paper ([77]), about 20 years after Jordan's treatise came out. Jordan used the French *composé* for a finite group having proper normal subgroups—hence the

subsequent terminology involving the word *composition*. For example, he called *facteurs de composition* the orders of the successive quotient groups in a composition series—while nowadays this is the terminology for the quotient groups themselves—and named *degré de composition* what one calls the length of the group. Of course, the twentieth century metamorphosis to modules had to deal with the fact that these were very rarely finite structures, so the analogy would have to come from the already established theory of vector spaces, where the individual terms have infinite cardinality, but finite dimension. On the bright side, at least in the commutative case, all submodules are trivially normal in the sense of group theory. Therefore, the emphasis on building a nontrivial theory would have to move to imposing finite composition series, thus arriving at the center of Noether's ideas about chain conditions. For the sake of correctness, it should be remarked that the idea of a composition series for finitely generated modules over a commutative ring essentially aims at having the notion of length, not having the same depth that it has in other fields, such as finite non-Abelian group theory or modules over noncommutative rings and certain categorical generalizations.

3.5.2 Fitting ideals

The remarkable feature of the Fitting ideals is that they give invariants of a finitely generated module M over a Noetherian ring R. For each particular structured module, the invariants thus obtained may show under diverse disguise. A systematic use was by Kähler, who employed them to create the so-called *Kähler differents* (see Section 4.4). These differents are intimately related to others (Dedekind, Noether), only their are easier for computation and relationship with ideal theory. Since M is tantamount to some of its free presentations, understanding the Fitting ideals of M gives a way of putting some of its numerical invariants back in the ring. Although the Noether different was only totally available to the public after her death, thanks to N. Jacobson, it was known to her prior to Fitting's paper ([58]). The relation between the two differents became the subject of many works in the immediate period thereafter.

3.6 Exercises

Exercise 3.6.1. Let R be a commutative ring and $\mathcal{M}$ an R-module.

(1) (Zassenhaus) Let $M' \subset M$ and $N' \subset N$ be submodules of $\mathcal{M}$. Prove the existence of a "crosswise" isomorphism

$$\frac{M' + M \cap N}{M' + M \cap N'} \simeq \frac{N' + M \cap N}{N' + M' \cap N}.$$

(Hint: for each side apply the familiar isomorphism $L + K/K \simeq L/L \cap K$.)

(2) (Schreier) Two sequences of submodules of $\mathcal{M}$ sharing the same ends

$$N = M_0 \subset \cdots \subset M_m = M \quad \text{and} \quad N = N_0 \subset \cdots \subset N_n = M$$

can be refined to sequences of the same length and isomorphic factors (up to ordering).
(Hint: use (1).)

(3) (Jordan–Hölder) Two composition series of an R-module have the same length and isomorphic factors (up to ordering).

Exercise 3.6.2. Let M be an R-module and let $\varphi : M \to M$ be an R-homomorphism.

(1) If M is Artinian and φ is injective, then φ is an isomorphism.
(Hint: consider the iterated images of φ.)

(2) If M is Noetherian and φ is surjective, then φ is an isomorphism.
(Hint: iterate inverse images of φ.)

Exercise 3.6.3 (Project: the Krull–Remak–Schmidt–Wedderburn theorem). Recall that an R-module is *indecomposable* if it does not admit any proper direct summand. Prove: an R-module M of finite length admits a unique (up to order) decomposition into a finite set of submodules.

(Hint: step 1: finite length implies that M decomposes into a finite set of indecomposables, so take two such; step 2: write the identity isomorphism 1 of M as a convenient sum of maps induced by the two decompositions; step 3: show that one of these maps must be an isomorphism; step 4: induct on the number of direct summands of one of the two decompositions; step 5: for the initial step of the induction prove that any endomorphism of an indecomposable module of finite length is either nilpotent or else an isomorphism.)

Exercise 3.6.4. Given an exact sequence $0 \to M' \to M \to M'' \to 0$ of R-modules, where any two terms have a rank, show that the third module has a rank and the respective ranks add up (in fact, it suffices to assume that the sequence is exact locally at the associated primes of R).

Exercise 3.6.5. If M has a finite free resolution, $0 \to F_m \to \cdots \to F_0 \to M \to 0$ show that M has a rank and this rank is $\sum_{i=0}^{m} (-1)^i \operatorname{rank} F_i$.
(See Subsection 6.2.2.1.)

Exercise 3.6.6. Let R be any ring, K its total ring of fractions and M a finitely generated R-module. The following are equivalent:

(i) $M/\tau_R(M)$ is a free R-module.

(ii) $M \otimes_R K$ is a free K-module, M^* is R-free of finite rank and the natural map $M \to M^{**}$ is surjective

(Hint: dualizing into R and tensoring with K both ignore R-torsion; now play with the commutative diagram

$$\begin{array}{ccc} M & \to & M^{**} \\ \downarrow & & \downarrow \\ M/\tau_R(M) & \to & (M/\tau_R(M))^{**}, \end{array}$$

where the right vertical arrow is bijective.)

Exercise 3.6.7. Let R denote an arbitrary ring, $I \subset R$ an ideal and $N \subset M$ R-modules. The *I-saturation* of N in M is the submodule

$$N :_M I^\infty := \bigcup_{t\geq 1}(N :_M I^t) \subset M,$$

where $N :_M J = \{f \in M \mid Jf \in N\}$ for an ideal $J \subset R$.

(1) Suppose, moreover, that R is Noetherian and M is finitely generated. Prove that the following conditions imply that $\tau_R(M) = 0 :_M I^\infty$: (i) $\operatorname{grade} I \geq 1$; (ii) M_P is R_P-torsion-free for every prime $P \not\supset I$.
(2) Deduce that, if M has a rank, then $\tau_R(M) = 0 :_M \mathcal{F}_r(M)^\infty$.

Exercise 3.6.8. Let M be an R-module.

(1) Show that the natural surjection $M \twoheadrightarrow M/\tau_R(M)$ is universal with respect to R-maps $M \to M'$ with M' torsion-free.
(2) Let $L = \ker(M \to M^{**})$. Deduce from (i) a natural surjective. R-map $M/\tau_R(M) \twoheadrightarrow M/L$.
(3) Let L as in (ii). Show that if M is finitely generated with a rank then both $M/\tau_R(M)$ and M/L have (the same) rank and the previous surjection is injective.
(4) Let L and M be as in (iii). Deduce that $L = 0 :_M \mathcal{F}_r(M)^\infty$ (the torsion of M).

Exercise 3.6.9 (Vasconcelos). Let M be a finitely generated module over an arbitrary ring. Show that any surjective R-homomorphism $\varphi : M \to M$ is injective (hence, an automorphism).

(Hint: make M into an $R[x]$-module (x an indeterminate) by setting $xm = \varphi(m)$ for $m \in M$; then $M = xM$, allowing to apply the determinantal trick.)

Exercise 3.6.10. Let R be a Noetherian ring and let M be a finitely generated R-module. The largest integer p such that $\bigwedge^p M \neq \{0\}$ is called the *exterior rank* of M, denoted $\wedge\_\operatorname{rank}(M)$. Show that if $(R, \mathfrak{m})$ is a Noetherian local ring then $\wedge\_\operatorname{rank}(M) = \dim_{R/\mathfrak{m}}(M/\mathfrak{m}M)$.

Exercise 3.6.11. Let $(R, \mathfrak{m})$ be a Noetherian local ring and let M be a finitely generated R-module. The *pth invariant factor* of M is the annihilator of $\bigwedge^p M$. If $R^s \xrightarrow{\varphi} R^n \to M \to 0$ is a free presentation of M with $n = \wedge\_\operatorname{rank}(M)$ show that the nth invariant factor of M is the ideal generated by the entries of φ.

Exercise 3.6.12 (Auslander–Buchsbaum). Let R be an arbitrary ring and let M be a finitely generated R-module. Let $\rho\_\,\mathrm{rank} := \sup\{\dim_{R/\mathfrak{m}}(M/\mathfrak{m}M) \mid \mathfrak{m} \text{ maximal}\}$ and let $\alpha(M)$ denote the annihilator of $\bigwedge^n M$, where $n = \wedge\_\,\mathrm{rank}(M)$.

(i) Show that $\rho\_\,\mathrm{rank} = \wedge\_\,\mathrm{rank}(M)$.

(ii) Show that $\rho\_\,\mathrm{rank}$ is attained at a maximal ideal $\mathfrak{m}$ if and only if $\alpha(M) \subset \mathfrak{m}$.

Exercise 3.6.13 (Flanders). Let R be an arbitrary ring and let $M \subset N$ be free R-modules.

(i) Show that the induced R-homomorphism $\bigwedge^p M \to \bigwedge^p N$ is injective for all $p \geq 1$. (Hint: the assertion is easy if M is a direct summand of N; in general, it may require the antisymmetrization map from exterior powers to tensor powers.)

(ii) (McCoy (1948)) Deduce that a square matrix $\mathcal{A}$ over R has a nonzero syzygy if and only if $\det \mathcal{A}$ is a zero-divisor.

4 Derivations, differentials and Jacobian ideals

4.1 Preliminaries

A derivation is the formalization of the idea of the derivative of a function, stressing linearity and the Leibniz rule. It keeps very little of the traditional taking limits, and yet embodies a strong differential angle. Some versions of Wikipedia still bring up a definition of derivations when actually referring to so-called *Kähler differentials*. Both concepts will be considered in this chapter.

Let R denote a commutative ring (with unit 1) and let M stand for an R-module.

Definition 4.1.1. A *derivation* of R into M is a map $D : R \to M$ such that, for any $f, g \in R$:
- $D(f + g) = D(f) + D(g)$
- $D(fg) = fD(g) + gD(f)$.

The notion is quite flexible, as it can have another ring in both sides. Namely, M can be a ring S when the latter comes with a ring homomorphism $R \to S$; or, there may be given a ring homomorphism $\iota : A \to R$, in which case one may decide to add the condition $D(\iota(a)f) = \iota(a)D(f)$, $a \in A$, $f \in R$. Then one refers to it as an A-derivation or an A-linear derivation.

Quite generally, one denotes the set of derivations of R into M by $\mathrm{Der}(R, M)$. If $k \subset R$ is a subring, the set of k-linear derivations of R into M is denoted $\mathrm{Der}_k(R, M)$. Both sets are R-modules under the natural action $(fD)(g) = fD(g)$, for $f, g \in R$. The case where $M = R$, *i. e.*, $\mathrm{Der}_k(R, R)$, has special properties and in many aspects tells us about the numerical invariants of R itself. One sets $\mathrm{Der}_k(R) := \mathrm{Der}_k(R, R)$ for short.

Among the first elementary properties of derivations is its expected behavior under taking fractions, pretty much as the traditional derivative of a fraction, namely in the following.

Lemma 4.1.2. *Let $\mathfrak{S}$ be a multiplicatively closed subset of R having no nilpotent elements and let $\mathfrak{S}^{-1}R$ denote the corresponding ring of fractions. Then any derivation $D \in \mathrm{Der}(R)$ extends to a derivation $\mathfrak{S}^{-1}D$ of $\mathrm{Der}(\mathfrak{S}^{-1}R)$ defined by*

$$(\mathfrak{S}^{-1}D)(f/g) = (D(f)g - fD(g))/g^2,$$

for $f \in R$, $g \in \mathfrak{S}$.

Proof. Left to the reader. □

One is tempted to think that the abstract definition above follows the classical stage of polynomials and rational fractions. Thus, it seems appropriate to formalize this situation once for all.

Let $R := k[x_1, \ldots, x_n]$ be a polynomial ring over a ring k. Taking $M = R$, the usual partial derivative $\partial/\partial x_i$, with $\partial x_j/\partial x_i = \delta_{ij}$, is a k-linear derivation of R into R.

The following properties, with interchangeable parts, take place.

https://doi.org/10.1515/9783110616989-004

Proposition 4.1.3. *Let $R := k[x_1, \dots, x_n]$ be as above.*

(1) *For any $D \in \mathrm{Der}_k(R)$, the values of D at $x_1, \dots, x_n$ determine it uniquely. More precisely, for any set of polynomials $f_1, \dots, f_n$ there is a unique k-derivation D such that $D(x_i) = f_i$, $i = 1, \dots, n$.*

(2) *If D is a k-derivation of R, then $D(f) = \sum_{i=1}^{n} (\partial f/\partial x_i) D(x_i)$, for any $f \in R$.*

(3) *$\mathrm{Der}_k(R)$ is a free R-module with basis the partial derivatives.*

Proof. (1) To see this, note that given $D(x_i) = f_i$, $i = 1, \dots, n$, the formula $D = \sum_i f_i \partial/\partial x_i$ defines a derivation, a direct verification using the defining rules. For uniqueness, let $D' \in \mathrm{Der}_k(R)$ such that $D'(x_i) = D(x_i)$, $i = 1, \dots, n$, and let $f \in R$ be arbitrarily given. Induct on the total degree of f. For total degree 0, there is nothing to prove. Now, given $f \in R \setminus k$, write $f = \sum_i g_i x_i$, for certain polynomials g_i. Then $D'(f) = \sum_i D'(g_i) x_i + g_i D(x_i)$. Since the total degree of g_i is strictly less than that of f, one has $D'(g_i) = D(g_i)$, $i = 1, \dots, n$, by the inductive hypothesis. Thus, one is through.

(2) This formula has been obtained in the proof of (1).

(3) Follows from (1) and (2). □

In case k is a field, similar properties hold for the corresponding field of fractions $K = k(x_1, \dots, x_n)$. Going beyond the scope of polynomial rings and purely transcendental extensions makes the theory of derivations very colorful. One of the facets of the play is that rings and fields go quite apart, with different approaches in average. A situation where one can bring them together is in the case a finitely generated domain R over a field k and its fields of fractions, via the ideal of polynomial relations of R over k. This kind of approach will be better understood with the method of Section 4.2.1.

Here, the focus is on the ring theoretic side of the theory; nevertheless, a few bits will be provided next.

Proposition 4.1.4. *The following conditions are equivalent for a finitely generated field extension $K|k$ in characteristic zero (or else, assume separability):*

(1) *$K|k$ is algebraic*

(2) $\mathrm{Der}_k(K) = 0$.

Proof. (1) $\Rightarrow$ (2)

Let $D \in \mathrm{Der}_k(K)$. Pick any $a \in K$ and let $f \in k[X]$ denotes its minimal polynomial over k. By separability, one has $f = (X - a)g$, with $g \in k[X]$ such that $g(a) \neq 0$. Then $df/dX = g + (X - a)(dg/dX)$, hence $(df/dX)(a) = g(a)$. Write $f = \sum_i \alpha_i X^i \in k[X]$. Now

$$0 = D(0) = D(f(a)) = \sum_i \alpha_i D(a^i) = \left(\sum_i i\alpha_i a^{i-1} \right) D(a)$$

as follows from the rules of derivations. Since $\sum_i i\alpha_i a^{i-1} = (df/dX)(a) = g(a) \neq 0$, one must have $D(a) = 0$.

(2) ⇒ (1) By Section 1.2.2, K is finite over $k(x_1, \dots, x_r)$, where $\{x_1, \dots, x_r\}$ is a transcendence basis out of a set $\{x_1, \dots, x_r, x_{r+1}, \dots, x_n\}$ of generators of K over k. Suppose, by way of contradiction, that $r \geq 1$. By induction on r it suffices to prove the following assertions.

Claim 1. If $K|k$ is a simple algebraic extension (char. 0 or separable), then every derivation of k extends to K.

Say, $K = k(a)$, where a is algebraic over k with minimal polynomial $p = p(X) \in k[X]$. Note that $k(a) = k[a]$, *i.e.*, K is the free k-subalgebra generated by a. As prior, $(dp/dX)(a) \neq 0$. Given a derivation D of k, define $D_X(\sum_i \alpha_i X^i) = \sum_i D(\alpha_i)X^i$. This is a derivation of $k[X]$ extending D.

Set $u := -D_X(p)(a)/(dp/dX)(a) \in k[a]$. Now consider the sum $\tilde{D} := D_X(p) + \tilde{u}(dp/dX)$, where $\tilde{u} \in k[X]$ is a preimage of u. Evaluating at a one gets zero. This means that $\tilde{D}$ is a multiple of p in $k[X]$, thus implying that it yields a map of $K = k[a]$, which is clearly a derivation and, moreover, extends D.

Claim 2. If $K|k$ is a simple transcendental extension, then every derivation of k extends to K.

Say, $K = k(a)$, with a transcendent over k. Then $k[a] \subset K$ is a polynomial ring over k with field of fractions $k(a) \subset K$. Set $a = X$ for psychological enhancement. Given a derivation D of k and any element $p(X) \in k[X] \subset K$, one defines a map $\tilde{D} : k[X] \to k[X]$ by $\tilde{D} = D_X + p(X)(d/dX)$ with D_X as above. It is clear that $\tilde{D}$ is a derivation of $k[X]$ since both summands are. Moreover, it extends D since the first summand does and the second summand vanishes on k. Now, this derivation extends to $k(X)$ by Lemma 4.1.2. □

Proposition 4.1.5 (Integrability). *Assume that k contains the field of rational numbers. Given $f_1, \dots, f_n \in k[x_1, \dots, x_n]$, there exists $F \in k[x_1, \dots, x_n]$ such that $\partial F/\partial x_i = f_i$, for all i if and only if*

$$\partial f_j/\partial x_i = \partial f_i/\partial x_j,$$

for all i, j.

Proof. One implication is immediate since the Hessian matrix of any $F \in k[x_1, \dots, x_n]$ is symmetric. Conversely, under the assumed symmetry, F can be taken in the following way: if $f_i = \sum_\alpha a_\alpha^{(i)} \mathbf{x}^\alpha$, where $\alpha = (\alpha_1, \dots, \alpha_n)$ and $\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, then the equality $\partial f_j/\partial x_i = \partial f_i/\partial x_j$ means that whenever

$$(\alpha_1, \dots, \alpha_{i-1}, \alpha_i - 1, \alpha_{i+1}, \dots \alpha_n) = (\alpha_1, \dots, \alpha_{j-1}, \alpha_j - 1, \alpha_{j+1}, \dots \alpha_n)$$

then

$$\frac{1}{\alpha_j} a^{(i)}_{(\alpha_1, \dots, \alpha_{i-1}, \alpha_i - 1, \alpha_{i+1}, \dots \alpha_n)} = \frac{1}{\alpha_i} a^{(j)}_{(\alpha_1, \dots, \alpha_{j-1}, \alpha_j - 1, \alpha_{j+1}, \dots \alpha_n)}.$$

One now sets $F = \sum_\beta b_\beta \mathbf{x}^\beta$, where

$$b_\beta = \begin{cases} 0 & \text{if } \beta = (0,\dots,0) \\ \frac{1}{\alpha_i} a^{(i)}_{(\alpha_1,\dots,\alpha_{i-1},\alpha_i-1,\alpha_{i+1},\dots\alpha_n)} & \text{if some } \alpha_i \neq 0 \end{cases}$$

The verification that F is a required integral is left to the reader. □

Proposition 4.1.6 (Basis criterion). *Let $R = k[x_1,\dots,x_n]$ as above. A set of derivations $D_1,\dots,D_n \in \mathrm{Der}_k(R)$ is a free basis if and only if the $n \times n$ matrix $(D_i(x_j))$ is invertible.*

Proof. If $\{D_1,\dots,D_n\}$ is a basis, write the partial derivations as combinations of $D_1,\dots,D_n$ with coefficients in R. Then the matrix of coefficients will give the inverse.

The converse is similar and is left to the reader. □

Other bases that look alike the partial derivations can be obtained as follows. Given $\mathbf{g} = \{g_1,\dots,g_n\} \subset R$, introduce a generalized Kronecker delta:

$$\delta^{\mathbf{g}}_{ij} = \begin{cases} g_i & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

Define $(\partial^{\mathbf{g}}/\partial x_i)(x_j) := \delta^{\mathbf{g}}_{ij}$. By the above, the set of these derivations form a basis if and only each g_i is a unit. This may be useful when one takes $g_i \in k$, the latter having enough units, or else by localization at the powers of an element in k.

If the interest lies away from free basis, the idea may still be useful. Here is an example.

Example 4.1.7 (Polarization). Let $k = A[y_1,\dots,y_n]$ be itself a polynomial ring over a ring A and set $R := k[x_1,\dots,x_n] = A[y_1,\dots,y_n,x_1,\dots,x_n]$. Take $\mathbf{g} = \mathbf{y} := \{y_1,\dots,y_n\}$ The sum $D^{\mathbf{y}} = \partial^{\mathbf{y}}/\partial x_1 + \cdots + \partial^{\mathbf{y}}/\partial x_n$ is called *polarization* of R with respect to $\mathbf{y}$. This sort of operation, often in modified form, is useful in various algebraic situations.

4.1.1 Derivations of subalgebras

So far, one the only subalgebras effectively considered were subfields of a field. Here one makes a brief incursion in the case of k-subalgebras of a polynomial ring over a field k. Often the results may depend on the nature of $\mathrm{char}(k)$. For example, we have the following.

Proposition 4.1.8. *Let $K = k(x_1,\dots,x_n)$ in characteristic zero and let $f_1,\dots,f_n \in K$. The following conditions are equivalent:*

(1) *$f_1,\dots,f_n$ are algebraically independent over k.*
(2) *The Jacobian determinant $\|\partial f_i/\partial x_j\|$ does not vanish.*
(3) $\mathrm{Der}_{k(f_1,\dots,f_n)}(K) = 0$.

Proof. (1) ⇔ (3) This follows from the equivalence in the previous proposition because condition (1) is necessary and sufficient in order that

$$\operatorname{trdeg}_k k(f_1, \ldots, f_n) = n.$$

As to (1) ⇔ (2), one shows next a more general statement.

For this, one reinstates the notation as follows. Let A be a finitely generated k-subalgebra of a polynomial ring $B := k[\mathbf{t}] = k[t_1, \ldots, t_d]$. Say, $A = k[\mathbf{g}]$, where $\mathbf{g} = \{g_1, \ldots, g_n\}$ is assumed to belong to the maximal ideal $(\mathbf{t})k[\mathbf{t}]$. Fix a presentation ideal I (necessarily prime) of A induced by $\mathbf{g}$. Thus, $k[\mathbf{X}]/I \simeq A$ under the k-algebra homomorphism $X_j \mapsto g_j$, where $\mathbf{X} = \{X_1, \ldots, X_n\}$.

Denote by $\Theta(\mathbf{g})$ the Jacobian matrix of $\mathbf{g}$ with respect to $\mathbf{t}$. Further, if $\mathbf{f}$ is a set of polynomials in $k[\mathbf{X}]$, the symbol $\Theta(\mathbf{f})$ (resp., $\Theta(\mathbf{f})(\mathbf{g})$) will denote the Jacobian matrix of $\mathbf{f}$ with respect to $\mathbf{X}$ (resp., further evaluated on the elements of $\mathbf{g}$). Clearly, $\Theta(\mathbf{f})(\mathbf{g})$ is the same matrix that results from taking $\Theta(\mathbf{f})$ modulo the ideal I and then using the isomorphism $k[\mathbf{X}]/I \simeq A$. Moreover, the rank of $\Theta(\mathbf{f})(\mathbf{g})$ is the same regardless from whether it is considered as a matrix over the subring A or over the ambient polynomial ring B.

Proposition 4.1.9. *If k is a field of characteristic zero, then* $\dim A = \operatorname{rank} \Theta(\mathbf{g})$.

Proof. Let as above $A \simeq k[\mathbf{X}]/I$, where $\mathbf{X} = \{X_1, \ldots, X_n\}$. Picking a set of generators $\mathbf{f} = \{f_1, \ldots, f_m\}$ of I and applying the chain rule of derivatives to its elements yields a short complex (in the sense of Subsection 6.2.3) of free B-modules

$$B^m \xrightarrow{\Theta(\mathbf{f})(\mathbf{g})^t} B^n \xrightarrow{\Theta(\mathbf{g})^t} B^d, \tag{4.1.9.1}$$

where ^{t} means transpose. From this follows that $\operatorname{rank} \Theta(\mathbf{g}) \leq n - \operatorname{rank} \Theta(\mathbf{f})(\mathbf{g})$. On the other hand, using the isomorphism $A \simeq k[\mathbf{X}]/I$, the matrix $\Theta(\mathbf{f})(\mathbf{g})$ fits in the well-known fundamental exact sequence of differentials

$$A^m \xrightarrow{\Theta(\mathbf{f})(\mathbf{g})^t} A^n \longrightarrow \Omega(A/k) \to 0, \tag{4.1.9.2}$$

where $\operatorname{rank} \Omega(A/k) = \dim A$ (see Proposition 4.2.13).

It follows that $\operatorname{rank} \Theta(\mathbf{g}) \leq \dim A$.

To show inequality in the other direction, after convenient reordering, let $\mathbf{g}' = g_1, \ldots, g_r$ be a transcendence basis of A over k. In particular, $\dim A = r = \dim k[\mathbf{g}']$. Obviously, $\operatorname{rank} \Theta(\mathbf{g}) \geq \operatorname{rank} \Theta(\mathbf{g}')$. Therefore, the required inequality follows from the proposition in special case where A is generated by algebraically independent elements over k.

Thus, assume that $\mathbf{g}$ is algebraically independent over k and argue by induction on the difference $d-n$, where $\mathbf{t} = \{t_1, \ldots, t_d\}$. If $n = d$, one is to show that $\det(\Theta(\mathbf{g})) \neq 0$. For every i, $1 \leq i \leq n$, let $\mathbf{g}(i)$ denote the augmented set $\{g_1, \ldots, g_n, t_i\}$. By assumption, each

such set is algebraically dependent over k, so let $F_i \in k[T_1, \dots, T_{n+1}]$ stand for a nonzero polynomial relation thereof of least possible degree. Since $\operatorname{char} k = 0$, $\frac{\partial F_i}{\partial T_{n+1}}(\mathbf{g}(i)) \neq 0$.

Letting $\Theta(\mathbf{g}(i))$ denote the Jacobian matrix of $\mathbf{g}(i)$, since F_i vanishes at $\mathbf{g}(i)$, the chain rule of derivatives yields

$$\left(\frac{\partial F_i}{\partial T_1}(\mathbf{g}(i)), \dots, \frac{\partial F_i}{\partial T_{n+1}}(\mathbf{g}(i))\right) \cdot \Theta(\mathbf{g}(i)) = 0, \tag{4.1.9.3}$$

for each i, $1 \leq i \leq n$. Now clearly, $\Theta(\mathbf{g}(i))$ is the matrix obtained from $\Theta(\mathbf{g})$ by further stacking it with the row vector e_i, where $e_i = (0, \dots, \underbrace{1}_{i}, \dots, 0)$. Therefore, (4.1.9.3) implies

$$\left(\frac{\partial F_i}{\partial T_1}(\mathbf{g}(i)), \dots, \frac{\partial F_i}{\partial T_n}(\mathbf{g}(i))\right) \cdot \Theta(\mathbf{g}) = -\frac{\partial F_i}{\partial T_{n+1}}(\mathbf{g}(i)) \cdot e_i, \tag{4.1.9.4}$$

for each i, $1 \leq i \leq n$. Since $\frac{\partial F_i}{\partial T_{n+1}}(\mathbf{g}(i)) \neq 0$, for each i, $1 \leq i \leq n$, this implies that the $k(\mathbf{t})$-linear map of $k(\mathbf{t})^n$ defined by $\Theta(\mathbf{g})$ is invertible. Therefore, $\det(\Theta(\mathbf{g})) \neq 0$ and one is through.

Now let $d - n \geq 1$. Pick a polynomial $h \in k[t_1, \dots, t_d]$ such that $\{\mathbf{g}, h\}$ is algebraically independent over k. By the inductive hypothesis, $\Theta(\mathbf{g}, h)$ is of rank $n+1$, hence the ideal of $(n+1)$-minors $I_{n+1}(\Theta(\mathbf{g}, h)) \subset k[t_1, \dots, t_d]$ is nonzero. Since the latter is contained in the ideal $I_n(\Theta(\mathbf{g}))$, the latter is nonzero as well, hence $\Theta(\mathbf{g})$ has rank at least $n = \dim A$, as desired. □

Remark 4.1.10. The lack of exactness of the complex (4.1.9.1) is related to the *polarizability* question studied in [18], [19] and [144] (see also [24, main lemma (i)]).

4.1.2 Derivations with values on a larger ring

So far, considering k-derivations of a k-algebra A with values in some R-module or overing has been pretty much in the way of thinking of the latter as a dummy object with no true impact in the theory. The setup of the previous part is quite enticing in this regard, namely, when A is a k-subalgebra of a polynomial ring $B = k[\mathbf{t}] = k[t_1, \dots, t_d]$; after all, this is the classical case of algebras admitting a parametrization (or, in a fancier language, "unirational" algebras).

Thus, one considers the k-derivations $\operatorname{Der}_k(A, B)$ of A with values in B, which is still an A-module but in addition also a B-module. One is mainly interested in its structure as B-module.

As in the previous part, one lets $A = k[\mathbf{g}] = k[g_1(\mathbf{t}), \dots, g_n(\mathbf{t})] \subset B$.

The main actor is again the Jacobian matrix $\Theta(\mathbf{g})$ with entries in B. Let $B\Theta(\mathbf{g}) \subset B^n$ denote the B submodule generated by the columns of $\Theta(\mathbf{g})$.

Lemma 4.1.11. *The notation being as above, upon identification* $\mathrm{Hom}_A(A^n, B) \simeq B^n$*, one has* $B\Theta(\mathbf{g}) \subset \mathrm{Der}_k(A, B)$ *as submodules of* B^n*.*

Proof. Let $A \simeq k[\mathbf{x}]/(\mathbf{f})$ as in the notation of the previous part. By the complex (4.1.9.1), the columns of $\Theta(\mathbf{g})$ are syzygies of the B-module generated by $\Theta(\mathbf{f})(\mathbf{g})$.

On the other hand, by taking B-duals on the exact sequence (4.1.9.2) says that $\mathrm{Der}_k(A, B)$ is the kernel of $\Theta(\mathbf{f})(\mathbf{g})$, where the latter is considered as a matrix over B and upon identification $\mathrm{Hom}_A(A^n, B) \simeq B^n$. Therefore, the assertion follows. □

Theorem 4.1.12. *Let k be a field of characteristic zero and let $A = k[\mathbf{g}] \subsetneq B = k[\mathbf{t}]$ be as above. Assume that* $\mathrm{ht}\, I_r(\Theta(\mathbf{g})) \geq 2$ *and that* $B(\Theta(\mathbf{g})) :_{B^n} I_r(\Theta(\mathbf{g})) = B(\Theta(\mathbf{g}))$*, where* $r = \dim A$*. Then* $\mathrm{Der}_k(A, B) = B(\Theta(\mathbf{g}))$.

Proof. One has the following.

Claim 1. $\mathrm{rank}\, B(\Theta(\mathbf{g})) = \mathrm{rank}\, \mathrm{Der}_k(A, B)$.

This is because, at one end, $\mathrm{rank}\, B(\Theta(\mathbf{g})) = \dim A$ by Proposition 4.1.9, and, at the other end, one has

$$\begin{aligned}\mathrm{rank}\big(\mathrm{Der}_k(A, B)\big) &= n - \mathrm{rank}\big(\Theta(\mathbf{f})(\mathbf{g})_B\big) = n - \mathrm{rank}\big(\Theta(\mathbf{f})(\mathbf{g})\big)\\ &= n - \big(n - \mathrm{rank}(\Omega_{A/k})\big) = \mathrm{rank}(\Omega_{A/k}) = \dim A,\end{aligned}$$

Claim 2. $\mathrm{Der}_k(A, B)$ is reflexive B-module.

This is because it is a second syzygy module, being the kernel of a map between free B-modules (Proposition 3.4.5).

Claim 3. The inclusion $B\Theta(\mathbf{g}) \subset \mathrm{Der}_k(A, B)$ is an equality locally in a codimension one.

This is due to the assumption $\mathrm{ht}\, I_r(\Theta(\mathbf{g})) \geq 2$.

Therefore, it follows that $B\Theta(\mathbf{g}) = \mathrm{Der}_k(A, B)$ since the assumption $B(\Theta(\mathbf{g})) :_{B^n} I_r(\Theta(\mathbf{g})) = B(\Theta(\mathbf{g}))$ means that the cokernel of $B\Theta(\mathbf{g})$ is torsion-free. □

Corollary 4.1.13. *With the notation and assumptions as in the last proposition, assume moreover that A has maximal dimension (i. e.,* $\dim A = \dim B$*). Then* $\mathrm{Der}_k(A, B)$ *is a free B-module of rank* $\dim B$*.*

Note that, as a consequence, $\mathrm{coker}\, \Theta(\mathbf{f}(\mathbf{g}))$ has homological dimension 2 as a B-module (in the sense of Section 6.2.2). A couple of examples will be given in the exercises.

4.2 Differential structures

4.2.1 A first structure theorem

For many purposes, there is nothing particular about k being a field. One can go reasonably far by just assuming that k is an arbitrary commutative ring and $R =$

$k[x_1, \dots, x_n]$ is a polynomial ring with coefficients in k. Then $\mathrm{Der}_k(R)$ is still a free R-module with basis the partial derivatives.

Any finitely generated k-algebra can be expressed as a residue of R by an ideal I and the R/I-module of derivations $\mathrm{Der}_k(R/I)$ is also an R-module in a natural way via the canonical map $R \twoheadrightarrow R/I$.

Lemma 4.2.1. *Let* $\mathrm{Der}_I(R) := \{D \in \mathrm{Der}_k(R) \mid D(f) \in I, \forall f \in I\}$. *Then:*
(1) $\mathrm{Der}_I(R)$ *is an* R*-submodule of* $\mathrm{Der}_k(R)$ *containing the* R*-submodule* $I\,\mathrm{Der}_k(R)$.
(2) *There is a natural isomorphism* $\mathrm{Der}_I(R)/I\,\mathrm{Der}_k(R) \simeq \mathrm{Der}_k(R/I)$ *of* R/I*-modules.*

Proof. (1) This is clear from the definitions.

(2) Any element $D \in \mathrm{Der}_I(R)$ is in particular a map $D : R \to R$ such that $D(I) \subset I$. Therefore, it induces a map $\overline{D} : R/I \to R/I$ by setting $\overline{D}(\bar{f}) = \overline{D(f)}$.

Claim 1. $\overline{D} \in \mathrm{Der}_k(R/I)$.

Clear from the definition of $\overline{D}$.

Claim 2. The assignment $D \mapsto \overline{D}$ gives an R-module homomorphism $\mathrm{Der}_I(R) \to \mathrm{Der}_k(R/I)$.

Left to the reader.

Claim 3. The kernel of the homomorphism in Claim 2 is the submodule $I\,\mathrm{Der}_k(R)$.

$\overline{D} = \overline{0}$ means that $D(f) \in I$ for every $f \in R$. In particular, $D(x_i) \in I$ for $1 \le i \le n$. Then $D = \sum_i D(x_i)\partial/\partial x_i \in I\,\mathrm{Der}_k(R)$. The converse is obvious.

Summing up, one has a natural injective R/I-module homomorphism

$$\mathrm{Der}_I(R)/I\,\mathrm{Der}_k(R) \hookrightarrow \mathrm{Der}_k(R/I). \tag{4.2.1.1}$$

In order to show that this map is also surjective, one has to work harder. In the next part it will be shown that $\mathrm{Der}_k(R/I)$ is also naturally contained in a free module over R/I, so the above homomorphism extends to a map of free modules over R and R/I, respectively. □

4.2.2 The universal module of differentials

As in most definitions of universal objects, one proceeds by taking free generators subject to relations.

Definition 4.2.2. Let R be an algebra over a ring k. Let F^{dR} denote the R-free module on the set $dR : \{df \mid f \in R\}$ and let $\mathfrak{D}$ denote the submodule generated by the elements

$$\begin{cases} d(\alpha f + \beta g) - \alpha df - \beta dg & \text{for } \alpha, \beta \in k, f, g \in R \\ d(fg) - f dg - g df & \text{for } f, g \in R \end{cases}$$

The *universal module of differentials* of R over k is the quotient module $\Omega_{R/k} := F^{dR}/\mathfrak{D}$.

The map $d : R \to \Omega_{R/k}$, given by $f \mapsto df \bmod \mathfrak{D}$, is clearly an element of $\mathrm{Der}_k(R, \Omega_{R/k})$; it is called the *universal k-linear derivation*.

As expected, being a sort of universal object, $\Omega_{R/k}$ has a universal property.

Proposition 4.2.3. *For any R-module M and any $D \in \mathrm{Der}_k(R, M)$, there exists a unique R-module homomorphism $\varphi : \Omega_{R/k} \to M$ factoring $D = \varphi \circ d$.*

Proof. Existence of φ is obvious: map F^{dR} to M by $df \mapsto D(f)$. Since D is a k-linear derivation, this map induces a required R-module homomorphism $\varphi : \Omega_{R/k} \to M$ factoring D.

The rest is left to the reader. □

Corollary 4.2.4. *For any R-module, there is a natural isomorphism of R-modules $\mathrm{Der}_k(R, M) \simeq \mathrm{Hom}_R(\Omega_{R/k}, M)$. In particular, $\mathrm{Der}_k(R)$ is isomorphic to the R-dual module of the universal module $\Omega_{R/k}$ of differentials.*

Quite generally, from the definition one sees immediately that for any set of generators $\mathcal{S}$ of R as a k-algebra, the set image $d\mathcal{S}$ is a set of generators of $\Omega_{R/k}$ as an R-module.

Example 4.2.5. Let $R = k[x_1, \ldots, x_n]$ denote a polynomial ring over k. Then $\Omega_{R/k}$ is a free R-module with basis the set $\{dx_i \mid 1 \le i \le n\}$.

Proof. Taking $M = R$ and $D = \partial/\partial x_i$ in the universal property, with φ_i the corresponding map $\Omega_{R/k} \to R$, one sees that $\partial f/\partial x_i = \varphi_i(df)$, for every $f \in R$. Assuming a relation $\sum_j g_j dx_j = 0$ and applying φ_i one gets $g_i = 0$, for any i. □

Remark 4.2.6. Beware of trying to extend this to any R such that $\mathrm{Der}_k(R)$ is R-free.

4.2.3 The conormal exact sequence

Definition 4.2.7. For any ideal $I \subset R$, the R/I-module I/I^2 is called the *conormal module* of R/I (the R/I-dual of the conormal module is often called the *normal module*)

Given any ideal $I \subset R$, there are two basic homomorphisms of R/I-modules:

$$\Omega_{R/k}/I\Omega_{R/k} \to \Omega_{R/I/k}.$$

This is induced by applying the universal property of $\Omega_{R/k}$ to the composite of $R \twoheadrightarrow R/I$ and the universal derivation of $\Omega_{R/I/k}$, whereby the latter is also an R-module. This map is surjective, as follows easily from a previous remark on generators and the surjection $R \twoheadrightarrow R/I$.

The other basic homomorphism is

$$I/I^2 \to \Omega_{R/k}/I\Omega_{R/k}.$$

This comes out from restricting the universal derivation of $\Omega_{R/k}$ to I, using the Leibniz rule and then applying to I^2 to get zero. The reader should workout these details to his (her) satisfaction.

It is straightforward to see that the composite of the above homomorphisms is zero. From this, one gets a complex of R/I-modules

$$I/I^2 \to \Omega_{R/k}/I\Omega_{R/k} \to \Omega_{R/I/k} \to 0. \tag{4.2.7.1}$$

This complex is coordinate-free. To see its exactness, one chooses coordinates by identifying $\Omega_{R/k} \simeq \bigoplus_{i=1}^n R dx_i$. Then it is the same as the following.

Proposition 4.2.8. *Suppose that $R = k[x_1, \dots, x_n]$ is a polynomial ring over a Noetherian ring k and $I = (f_1, \dots, f_m)$. Then $\Omega_{R/I/k}$ has a free presentation*

$$(R/I)^m \xrightarrow{\Theta^t} \bigoplus_{i=1}^n (R/I)dx_i \to \Omega_{R/I/k} \to 0,$$

where Θ^t is the transpose of the Jacobian matrix Θ of $f_1, \dots, f_m$, taken modulo I.

To see this coordinate based complex, take a surjective homomorphism $R^m \twoheadrightarrow I$ induced by the generators $I = (f_1, \dots, f_m)$ and tensor with R/I over R to get a surjective R/I-module homomorphism $\rho : (R/I)^m \twoheadrightarrow I/I^2$. Then compose ρ with the map $I/I^2 \to \Omega_{R/k}/I\Omega_{R/k} \simeq \bigoplus_{i=1}^n (R/I)dx_i$.

An important additional exact complex is obtained by taking the R/I-dual of (4.2.7.1):

$$0 \to \mathrm{Der}_k(R/I) \to \bigoplus_{i=1}^n (R/I)\frac{\partial}{\partial x_i} \xrightarrow{\Theta} (R/I)^{m*}, \tag{4.2.8.1}$$

where $(R/I)^{m*}$ is the R/I-dual of $(R/I)^m$. Here, $\{\partial/\partial x_i \mid 1 \le i \le n\}$ is the dual basis of $\{dx_i \mid 1 \le i \le n\}$ since the R-dual of $\bigoplus_{i=1}^n R dx_i$ is $\bigoplus_{i=1}^n (R/I)\frac{\partial}{\partial x_i}$ and by the universal property. Therefore, the k-linear derivations of R/I form the kernel modulo I of the Jacobian matrix of any finite generating set of I.

In particular, contrary to the module of differentials, the module of derivations is torsion-free (this is of course the case of any dual module).

Corollary 4.2.9. *The map* (4.2.1.1) *is surjective.*

Proof. Write any given $D \in \mathrm{Der}_k(R/I)$ as an element $\sum_i \overline{g}_i \frac{\partial}{\partial x_i} \in \bigoplus_{i=1}^n (R/I)\frac{\partial}{\partial x_i}$. Since $\Theta(D) = 0 \bmod I$, this means that $\sum_i g_i \frac{\partial}{\partial x_i}(f_j) = \sum_i g_i \frac{\partial f_j}{\partial x_i} \in I$ for all $j = 1, \dots, m$. Therefore, D is the image of a derivation of R preserving the ideal I. □

Remark 4.2.10. One of the interesting questions is the explicit calculation of a set of generators of $\mathrm{Der}_k(R/I)$, even when k is a field. Although this is easily established by a syzygy computation in any of the available computer algebra programs, one still lacks a good method to envisage the general case or even special classes of ideals. For some reason the question becomes a lot easier in the case where R is graded and I is a homogeneous ideal. A few easy cases will be in the exercises.

An alternative to computing the syzygies of the Jacobian matrix Θ over R/I is to search directly for generators of the R-submodule $\mathrm{Der}_I(R)$. This module has importance on itself, since it appears in many a context, *e.g.*, in the case I is a principal ideal, as the algebraic version of the so-called *Derlog* (short for "logarithmic derivations") module of R/I.

Quite surprisingly, this can be computed in a sort of strategic case.

Proposition 4.2.11 ([23]). *Suppose that k is a field and I is generated by monomials in the variables of $R[x_1, \dots, x_n]$. Assume that either* $\mathrm{char}(k) = 0$ *or else the exponents of the variables throughout are prime to* $\mathrm{char}(k)$. *Then*

$$\mathrm{Der}_k(R/I) = \bigoplus_{i=1}^{n} (I : (I : x_i)/I)\, \frac{\partial}{\partial x_i} \subset \bigoplus_{i=1}^{n} (R/I)\, \frac{\partial}{\partial x_i}.$$

It has the following consequence for a well-known homological conjecture, stated independently by J. Herzog and W. Vasconcelos.

Corollary 4.2.12. *Suppose that k is a field and I is generated by monomials in the variables of $R = k[\mathbf{x}]$. Assume that either* $\mathrm{char}(k) = 0$ *or else the exponents of the variables throughout are prime to* $\mathrm{char}(k)$. *If $\mathrm{Der}_k(R/I)$ has finite homological dimension over R/I, then R/I is a polynomial ring.*

Proof. By the assumption and Proposition 4.2.11, each $(I : (I : x_i))/I$ has finite homological dimension over R/I, hence admits a finite free graded resolution over R/I (see Section 6.2.2). This implies that $(I : (I : x_i))$ contain an element a which is regular on R/I [10]. This forces the inclusion $I : x_i \subset I$, otherwise a would belong to some associated prime of I. Thus, $(I : x_i) = I$ for every variable x_i. Since I is generated by monomials, it follows that I is generated by some subset of variables. □

The following result is often useful.

Proposition 4.2.13. *If S is finitely generated domain* (*reduced and equidimensional would suffice*) *S over a perfect field k, then* $\mathrm{rank}\, \mathrm{Der}_k(S) = \mathrm{rank}\, \Omega_{S/k} = \dim S$.

Proof. There are several ways to prove this assertion. Here are the main steps for one of them.

- Write $S \simeq R/P$, with $R = k[x_1, \dots, x_n]$ a polynomial ring and $P \subset R$ a prime ideal, and apply the conormal exact sequence.
- **Claim:** The kernel of the leftmost map is the torsion submodule of P/P^2.

- The torsion submodule of P/P^2 is $P^{(2)}/P^2$, where the numerator is the P-primary part of P^2; hence, the kernel of the right map of the conormal sequence gets identified with $P/P^{(2)}$. In particular, $\operatorname{rank} P/P^{(2)} = \operatorname{rank} P/P^2$.
- Since P_P is generated by a regular sequence of $\operatorname{ht} P$ elements then P/P^2 is locally free at P of rank $\operatorname{ht} P$. Therefore, $\operatorname{rank} P/P^{(2)} = \operatorname{ht} P$.
- Since R is a polynomial ring, dimension and height add up, and since ranks add up along an exact sequence, it follows that $\operatorname{rank} \Omega_{S/k} = n - \operatorname{ht} P = \dim S$. □

Remark 4.2.14. As seen, the rank of the Jacobian matrix over R/I is the height of the ideal I on R, at least if I is a reduced and unmixed ideal in a polynomial ring over a perfect field. It naturally raises the question as to whether the number of generators of I has any impact whatsoever for derivations.

For this, one can consider the syzygies $\operatorname{Syz}_R(\Theta)$ of the Jacobian matrix on the polynomial ring R, since every such syzygy yields modulo I an element of $\operatorname{Der}_k(R/I)$. Unfortunately, one faces two problems at the outset: first, the rank of $\operatorname{Syz}_R(\Theta)$ over R can substantially drop over R/I; second, the residues of these syzygies may turn out to be high order combinations of minimal generators of $\operatorname{Der}_k(I)$ to be of any significance.

Some of these aspects will be taken up in the exercises.

4.2.4 Kähler differentials

E. Kähler (1930; see also [90]) proposed a new version of the universal module of differentials. This version would shape up to a definite form in [33], in terms of a conormal module of an ideal in another ring.

Definition 4.2.15. Let R be an algebra over a ring k. Let $\mathbb{D}$ denote the kernel of the ring homomorphism $R \otimes_k R \to R$ defined by $a \otimes b \mapsto ab$. The *module of Kähler differentials* of R over k is $\mathbb{D}/\mathbb{D}^2$, which is an R-module via the natural isomorphism $(R \otimes_k R)/\mathbb{D} \simeq R$.

The map $\delta : R \to \mathbb{D}/\mathbb{D}^2$ defined by $a \mapsto 1 \otimes a - a \otimes 1 \bmod \mathbb{D}^2$ can be seen to be an element of $\operatorname{Der}_k(R, \mathbb{D}/\mathbb{D}^2)$. The universal property then gives a homomorphism $\Omega_{R/k} \to \mathbb{D}/\mathbb{D}^2$ factoring δ which can be further checked to be an isomorphism.

In this new disguise, δ becomes the universal derivation.

4.2.4.1 Zariski differentials

The following variant of the module of differentials was used by O. Zariski.

Definition 4.2.16. The *Zariski module of differentials* is the R-dual of the module of derivations $\operatorname{Der}_k(R)$; in other words, the reflexive closure $\Omega^{**}_{R/k}$.

The canonical map $\Omega_{R/k} \to \Omega^{**}_{R/k}$ is far from being either injective or surjective in general.

Remark 4.2.17. A hard problem is the torsion $\tau(\Omega_{R/k}) \subset \Omega_{R/k}$. Say, R is a domain with fraction field K. Then tensoring the map $\Omega_{R/k} \to \Omega^{**}_{R/k}$ with K yields that its kernel is $\tau(\Omega_{R/k})$. The torsion is a difficult question even in dimension 1 (Berger conjecture).

4.3 The issue of regularity in algebra and geometry

4.3.1 The Jacobian ideal

Before the advent of the homological boom in commutative algebra in the mid past century, including the spectacular homological characterization of a regular local ring, the issue of regularity in algebraic geometry was totally dominated by the celebrated following result.

Theorem 4.3.1 (Jacobian criterion). *Let S be a finitely generated algebra over a field k and let $\wp \subset S$ be a prime ideal such that the field extension $K(S/\wp)|k$ is separable. Choose a k-algebra isomorphism $S \simeq R/I$, with R a polynomial ring over k. Let $P \subset R$ denote the corresponding prime ideal containing I. The following are equivalent:*
(i) *$S_\wp$ is regular.*
(ii) *The rank modulo P of the Jacobian matrix of some (any) generating set of I is* $\operatorname{ht} I_P$.

A much less celebrated terminology, but equally important.

Definition 4.3.2. Let S be a finitely generated algebra over a field k. The *Jacobian ideal* of S over k is the Fitting ideal of order $\dim S$ of the module of differentials $\Omega_{S/k}$.

In other words, let $S \simeq k[\mathbf{X}]/I$, where $k[\mathbf{X}]$ is a polynomial ring over k, with I an ideal of height g. The Jacobian ideal of S is the ideal of g-minors of the Jacobian matrix of one (any) set of generators of I viewed as an ideal modulo I. There is a slight abuse by which one often takes the ideal of g-minors itself in the polynomial ring $k[\mathbf{X}]$ as the Jacobian ideal of S. In this case, in order to keep the invariant properties of the Jacobian ideal, one should always take the g-minors summed to I. By a suggestive classical terminology, one would then refer to the ideal of g-minors as the *critical ideal* of S.

Since one has identified $\Omega_{S/k}$ with the module of Kähler differentials, the Jacobian ideal is classically known as a *Kähler different*. Actually, there is a series of Kähler differents associated to S, one of which is the Jacobian ideal. Its overall relevance comes from the following fact.

Proposition 4.3.3. *Let S be a finitely generated equidimensional (e. g., a domain) algebra over a perfect field k. Then, given a prime $\wp \subset S$, the ring $S_\wp$ is regular if and only if $\wp$ does not contain the Jacobian ideal of S over k.*

Quite generally, $\mathcal{F}_r(M)$ denotes the Fitting ideal of order r of a finitely generated module M over a Noetherian ring S, as introduced in Section 3.3. Repeat Corollary 3.3.9 here for convenience.

Proposition 4.3.4. *If M is finitely generated with rank r, then $\mathcal{F}_r(M)$ is the nonfree locus of M; in other words, $M_\wp$ is $S_\wp$-free of rank r for a prime ideal $\wp \subset S$ if and only if $\mathcal{F}_r(M) \not\subset \wp$.*

Putting together the various results so far, one has the following.

Corollary 4.3.5. *Let S denote a finitely generated reduced equidimensional algebra over a perfect field k. Then S is locally regular everywhere if and only if $\Omega_{S/k}$ is a projective (i. e., locally free everywhere) S-module.*

Often this result is thought of as the Jacobian criterion itself.

4.3.2 Hypersurfaces

In the case where S is a hypersurface ring, *i. e.*, $S = k[\mathbf{X}]/(f)$, for some $f \in k[\mathbf{X}]$, the Jacobian ideal viewed in $k[\mathbf{X}]$ is the ideal $(\partial f, f)$ where ∂f stands for the critical ideal of f, often called the *gradient ideal* of f. One says that f is *Eulerian* if $f \in \partial f$—as is the case when f is homogeneous (or quasi-homogeneous) and $\operatorname{char}(k) = 0$.

The algebraic facet of the gradient ideal could start from the following simple general results.

Proposition 4.3.6. *Let R be a Noetherian ring, let $f \in R$ be a regular element and let $\varphi : G \to R$ be an R-homomorphism, with G a free module of finite rank. Set $I = \operatorname{Im}(\varphi)$, $Z = \ker \varphi$ and $Z_{[f]} = \ker \varphi_{[f]}$, where $\varphi_{[f]}$ is the composite of φ and the residue map $R \twoheadrightarrow R/(f)$.*

(i) *There are exact sequences of R-modules*

$$0 \to Z \to Z_{[f]} \to I : (f) \to 0, \tag{4.3.6.1}$$

and of $R/(f)$-modules

$$0 \to Z/Z \cap fG \to Z_{[f]}/fG \to \frac{I : (f)}{I} \to 0. \tag{4.3.6.2}$$

(ii) *Let f also denote the isomorphism $R \simeq (f)$ given by multiplication by f and consider the induced surjective R-homomorphism $\psi := \varphi \oplus f : G \oplus R \longrightarrow (I, f)$. Then $Z_{[f]} \simeq \ker(\psi)$ and $Z_{[f]}$ is reflexive.*

Proof. (i) The first exact sequence goes as follows: if $u \in Z_{[f]}$, then $\varphi(u)$ vanishes in $R/(f)$ by definition. Thus, $\varphi(u) = a_u f$, for a unique $a_u \in R$ (uniqueness comes from the assumption that f is regular). Moreover, since $\varphi(G) = I$, then $a \in I : (f)$. Therefore, one has a map $Z_{[f]} \to I : (f)$ given by $u \mapsto a_u$. Clearly, conversely, one has that this map is surjective. It is clear that this map is an R-homomorphism. Finally, $a_u = 0$ if and only if $u \in \ker \varphi = Z$.

For the second exact sequence, using the map $Z_{[f]} \to I : (f)$ in the first exact sequence, one sees that if $u = fe \in fG \subset Z_{[f]}$, with $e \in G$, then $\varphi(u) = \varphi(e)f$, hence u is mapped to $\varphi(e)$. Therefore, the restriction to fG maps onto I. This gives the right part of the exact sequence. Now, a straightforward verification gives that kernel of $Z_{[f]}/fG \to \frac{I:(f)}{I}$ is $Z + fG/fG \simeq S/Z \cap fG$.

(ii) Let $\widetilde{Z_{[f]}} = \ker(\psi)$. It is easy to see that, since f is a regular element, projection of $G \oplus R$ onto the first summand induces a bijection of $\widetilde{Z_{[f]}}$ onto $Z_{[f]}$.

Since f is a regular element, the ideal (I, f) has grade at least one, hence it has a well-defined rank (one) as an R-module. Therefore, $\widetilde{Z_{[f]}}$ being a first syzygy of such a module, it too has a well-defined rank. But a finitely generated second syzygy with this property is reflexive (Proposition 3.4.5). □

Corollary 4.3.7. *With the notation of* Proposition 4.3.6 *one has:*

(a) *If $f \in I$, then $Z_{[f]} \simeq Z \oplus R$.*

(b) *Suppose that projective R-modules of finite rank are free. If the ideal (I, f) is proper and has grade at least two, then $Z_{[f]}$ is a free module if and only (I, f) is a codimension two perfect ideal.*

Proof. (a) The first assertion is obvious since $I : (f) = R$ and R is free. Note, en passant, that a splitting map ρ will map 1 to a vector $\mathfrak{z}$ such that $\varphi(\mathfrak{z}) = f$.

(b) If $Z_{[f]}$ is free, then (I, f) has projective dimension one, hence it must be a codimension two perfect ideal because it has grade at least two. Conversely, if (I, f) is a codimension two perfect ideal, then it has projective dimension one. Since $Z_{[f]}$ is a first syzygy thereof, it must be a projective module (of finite rank) by a well-known device, hence it is free. □

These simple ideas now apply to the case where one sets $R = k[\mathbf{X}] = k[X_1, \ldots, X_n]$, $0 \neq f \in k[\mathbf{X}]$ and $I = \partial f$. Let

$$0 \to Z = Z(\partial f) \to G = R^n \to I = \partial f \to 0$$

be a presentation of I. In order to make the setup more canonical, identify R^n with $\mathrm{Der}_k(R)$, the latter being free with basis the partial derivations $\partial/\partial X_i$ $(1 \leq i \leq n)$. Then it is easy to see that Z is the R-module of syzygies of the partial derivatives $\partial f/\partial X_i$ $(1 \leq i \leq n)$. Likewise, one sees that $Z_{[f]}$ gets identified with the module $\mathrm{Der}_f(R)$ (Derlog of f).

Proposition 4.3.8. *There are exact sequences of R-modules*

$$0 \to Z(\partial) \to \mathrm{Der}_f(R) \to I : (f) \to 0, \tag{4.3.8.1}$$

and of $R/(f)$-modules

$$0 \to \frac{Z(\partial)}{Z(\partial) \cap f \,\mathrm{Der}_k(R)} \to \mathrm{Der}_k(R/(f)) \to \frac{I : (f)}{I} \to 0. \tag{4.3.8.2}$$

In particular, when f is Eulerian one has:

(1) *There is a direct sum decomposition of R/I-modules* $\mathrm{Der}_f(R) = Z(\partial) \oplus R\epsilon$, *where*

$$\epsilon = X_1 \frac{\partial}{\partial x_1} + \cdots + X_n \frac{\partial}{\partial x_n}$$

is the Euler derivation of R

(2) (Zariski [103]) *The module* $\mathrm{Der}_k(R/(f))$ *of k-derivations is generated by the syzygies of the gradient ideal of f modulo those that have coefficients in (f) and the induced Euler derivation.*

The details can be filled in by the reader. The last proposition and the previous corollary give the basic commutative algebra for handling the so-called *free divisors* introduced by K. Saito ([130]).

4.4 Differents and ramification

This is a very brief account on the concept of a different, as originally introduced by E. Noether ([119]). These ideas are so deeply entrenched in the theory of Kähler differentials that it becomes rather miraculous that they have a strong relation to the notion of ramification, the latter having been very clearly explained by M. Auslander and D. Buchsbaum in [10].

Naturally then, the short lines here will draw from these sources.

4.4.1 Ramification

Let $\varphi : R \to S$ be a homomorphism of Noetherian rings through which S is an R-algebra essentially of finite type.

Recall the basic exact sequence for the definition of Kähler differentials:

$$0 \to \mathbb{D} \to S \otimes_R S \xrightarrow{\boldsymbol{\mu}} S \to 0, \tag{4.4.0.1}$$

where $\boldsymbol{\mu}$ denotes the multiplication map $s \otimes s' \mapsto ss'$ (Section 4.2.4).

Note, for later use, that $\mathbb{D}$ is generated by differences of pure tensors as follows: $1 \otimes s - s \otimes 1$. To see this, write any pure tensor in the form $t \otimes s = ts \otimes 1 + t(1 \otimes s - s \otimes 1)$. Then a general element will be written in the form

$$\sum_i t_i \otimes s_i = \left(\sum_i t_i s_i \right) \otimes 1 + \sum_i t_i (1 \otimes s_i - s_i \otimes 1).$$

Now, if $\boldsymbol{\mu}(\sum_i t_i \otimes s_i) = 0$, then also $\sum_i t_i s_i = \boldsymbol{\mu}((\sum_i t_i s_i) \otimes 1) = 0$. Therefore, $\sum_i t_i \otimes s_i = \sum_i t_i (1 \otimes s_i - s_i \otimes 1)$.

Definition 4.4.1. The *Noether different* of the map φ is the ideal

$$\mathfrak{N}_{S/R} := \boldsymbol{\mu}(0 :_{S\otimes_R S} \mathbb{D}) \subset S.$$

A special setup may clarify how to obtain the Noether different.

Let $R = k$ be a field and let $S = k[\mathbf{x}]/I = k[x_1, \dots, x_m]/I$ be a finitely generated k-algebra. Then $S \otimes_k S \simeq k[\mathbf{x}, \mathbf{y}]/(I, I(\mathbf{y}))$, where $\mathbf{y}$ is a clone of $\mathbf{x}$ and $I(\mathbf{y})$ is the ideal of $k[\mathbf{y}]$ image of I by the k-isomorphism $x_i \mapsto y_i$. Then

$$0 :_{S\otimes_R S} \mathbb{D} = \big(I, I(\mathbf{y})\big) : \widetilde{\mathbb{D}}/(I, I(\mathbf{y})),$$

where $\widetilde{\mathbb{D}} = (x_i - y_i | 1 \le i \le m)$ and the Noether different is obtained by applying to the colon ideal $(I, I(\mathbf{y})) : \widetilde{\mathbb{D}}$ the "diagonal" homomorphism $k[\mathbf{x}, \mathbf{y}] \to k[\mathbf{x}]$ such that $x_i \mapsto x_i$, $y_i \mapsto x_i$.

Example 4.4.2. Suppose that $I = (f_1, \dots, f_m)$ is a regular sequence of length m. Then $k[\mathbf{x}]/I$ is an Artinian Gorenstein ring (see Section 5.4.2) and the Noether different turns out to be the socle, *i. e.*, the Jacobian determinant of $f_1, \dots, f_m$ modulo I.

The Noether different is related to the classical Dedekind different, defined in terms of the trace map, and the Kähler different, defined in terms of the Fiting ideals of the module of differentials.

Next, one deals with basic notions of ramification. Given a prime ideal $q \in \operatorname{Spec} S$ one says that q is *unramified* in the map φ, or that S is *unramified over R at q* if $qS_q = \varphi(p)S_q$, where $p = \varphi^{-1}(q)$, and the residue field extension $R_p/pR_p \subset S_q/qS_q$ is separable algebraic.

Otherwise, S is said to be *ramified over R at q*. One also says that S is unramified over R if every prime ideal of S is unramified and, moreover, every prime ideal of R is the contraction of at most finitely many prime ideals of S.

In order to state the high points of the present theory, a couple of lemmas of independent interest are next.

Lemma 4.4.3. *The exact sequence* (4.4.0.1) *splits as $S \otimes_R S$-modules if and only if $\mathfrak{N}_{S/R}$ is the unit ideal in S.*

Proof. Assume that the sequence splits and let $\iota : S \to S \otimes_R S$ be a splitting $S \otimes_R S$-homomorphism. Set $\mathfrak{s} := \iota(1)$. Then $\mathfrak{s}(s \otimes 1) = \mathfrak{s}(1 \otimes s)$ for every $s \in S$. Since $\mathbb{D}$ is generated by such differences $s \otimes 1 - 1 \otimes s$ it follows that $\mathfrak{s} \in 0 :_{S\otimes_R S} \mathbb{D}$, hence $\boldsymbol{\mu}(\mathfrak{s}) = \boldsymbol{\mu}(\iota(1)) = 1 \in \mathfrak{N}_{S/R}$.

The converse is similar and is left to the reader. □

Lemma 4.4.4. *If any maximal ideal in S is unramified over R, then $\operatorname{Der}_R(S, M) = 0$ for any finitely generated S-module M.*

Proof. Let $D \in \operatorname{Der}_R(S, M)$ and let $\mathfrak{M}$ be any maximal ideal of S. Extending D to $D_{\mathfrak{M}} \in \operatorname{Der}_{R_{\mathfrak{M}}}(S_{\mathfrak{M}}, M_{\mathfrak{M}})$, it suffices to show that $D_{\mathfrak{M}} = 0$. Contracting $\mathfrak{M} \cap R = \mathfrak{m}$, since $D_{\mathfrak{M}}$ is over $R_{\mathfrak{M}}$, then $D_{\mathfrak{M}}(\mathfrak{m}) \subset \mathfrak{m}M_{\mathfrak{M}}$.

Since $\mathfrak{M}$ is unramified, then $\mathfrak{m}S_{\mathfrak{M}} = \mathfrak{M}S_{\mathfrak{M}}$; hence, $D_{\mathfrak{M}}(\mathfrak{M}S_{\mathfrak{M}}) \subset \mathfrak{M}M_{\mathfrak{M}}$. This induces a derivation $\overline{D} \in \mathrm{Der}_k(K, M_{\mathfrak{M}} \otimes_{S_{\mathfrak{M}}} K)$, where $K = S/\mathfrak{M}$ and $k = R/\mathfrak{m}$. Since one is now in the field case, one has $\overline{D} = 0$ (Proposition 4.1.4). It follows that $D_{\mathfrak{M}}(S_{\mathfrak{M}}) \subset \mathfrak{M}M_{\mathfrak{M}}$. Iterating the procedure, one finds that $D_{\mathfrak{M}}(S_{\mathfrak{M}}) \subset \bigcap_i \mathfrak{M}^i M_{\mathfrak{M}}$, so Krull's intersection theorem (Theorem 5.2.18) takes over. □

The main result of this section is the following theorem.

Theorem 4.4.5 (Ramification criterion). *The following conditions are equivalent:*
(i) *The exact sequence* (4.4.0.1) *splits.*
(ii) *S is unramified over R.*
(iii) $\mathrm{Der}_R(S, M) = 0$ *for any finitely generated S-module M.*

(i) ⇒ (ii). Let $\wp \in \mathrm{Spec}\, R$ be contracted from a prime in S. Since (4.4.0.1) splits, then tensoring with the residue field $k := R_\wp/\wp R_\wp$ yields a split exact sequence

$$0 \to \mathcal{D} \to A \otimes_k A \to A \to 0,$$

where A is a finite dimensional k-algebra. Therefore, A is a separable (commutative) k-algebra ([43, Proposition 1.1]). Since $\dim A = 0$, Proposition 2.5.16 implies that A is a direct sum of local Artinian rings which must each be a (separable) field extension of k since separability prohibits nontrivial nilpotents. Each such field extension corresponds to a prime $\mathfrak{P} \subset S$ contracting to $\wp$, implying the equality $\wp S_{\mathfrak{P}} = \mathfrak{P}S_{\mathfrak{P}}$.

(ii) ⇒ (iii). This is Lemma 4.4.4.

(iii) ⇒ (i). By Corollary 4.2.4, one has $\mathrm{Hom}_S(\Omega_{S/R}, M) = \mathrm{Der}_R(S, M)$ for any S-module M. Taking $M = \Omega_{S/R} = \mathbb{D}/\mathbb{D}^2$, one has $\mathrm{Hom}_S(\mathbb{D}/\mathbb{D}^2, \mathbb{D}/\mathbb{D}^2) = 0$ by the assumption. Therefore, $\mathbb{D}/\mathbb{D}^2 = 0$. This implies that there exists an $u \in \mathbb{D}$ such that $vu = v$ for every $v \in \mathbb{D}$.

Then the $S \otimes_R S$-map $\pi : S \otimes_R S \to \mathbb{D}$ given by $\pi(1) = u$ is a splitting projection since $\pi(v) = v(\pi(1) = vu = v)$ for every $v \in \mathbb{D}$. □

4.4.2 Purity

The *branch locus* $\mathrm{Branch}(S/R)$ of S over R is the subset of $\mathrm{Spec}\, S$ consisting of all primes where S is ramified over R.

The relation to the branch locus goes as follows:

Proposition 4.4.6. *With the above setup and notation, one has*

$$\mathrm{Branch}(S/R) = V(\mathfrak{N}_{S/R}).$$

Proof. Let $\mathfrak{P} \in \mathrm{Spec}\, S$ be a prime not containing the different $\mathfrak{N}_{S/R}$ and let $\wp$ be its contraction in R. Then $(\mathfrak{N}_{S/R})_{\mathfrak{P}} = S_{\mathfrak{P}}$. Applying Lemma 4.4.3 with $S_{\mathfrak{P}}$ in place of S, the "localized" exact sequence $0 \to \widetilde{\mathbb{D}} \to \widetilde{(S \otimes_R S)} \to S_{\mathfrak{P}} \to 0$ splits, where $\tilde{}$ denotes fractions with respect to the multiplicatively closed subset $(S \setminus \mathfrak{P}) \otimes (S \setminus \mathfrak{P})$.

By Theorem 4.4.5, $S_{\mathfrak{P}}$ is unramified over $R_{\wp}$, *i. e.*, $\wp_{\wp} S_{\mathfrak{P}} = \mathfrak{P}_{\mathfrak{P}} S_{\mathfrak{P}}$, which is clearly the same as $\wp S_{\mathfrak{P}} = \mathfrak{P} S_{\mathfrak{P}}$.

The converse is similar and follows from the implication (ii) $\Rightarrow$ (i) of Theorem 4.4.5 and Lemma 4.4.3. □

Corollary 4.4.7. *With the above notation,* $\operatorname{Branch}(S/R) = \operatorname{supp} \Omega(S/R)$.

Proof. Since $\Omega_{S/R} = \mathbb{D}/\mathbb{D}^2$ and $\operatorname{supp} \Omega(S/R) = V(0 :_S \Omega_{S/R})$, it is clear by the definition of the Noether different that $\operatorname{supp} \Omega(S/R) \subset V(\mathfrak{N}_{S/R})$. On the other hand, a power of $\mathfrak{N}_{S/R}$ lies in the zeroth Fitting ideal of $\Omega_{S/R}$ ([17, II. Satz 3 und 4]). The result then follows from Proposition 4.4.6. □

One is really interested in sizing up $\operatorname{Branch}(R/S)$ in some sense. Classically, this problem became known as the *purity of the branch locus* after the seminal paper by Zariski ([167]) and a 2-dimensional case by Serre (unpublished), followed by [10] and, in a more general form, by Nagata ([111]). There are other sophisticated versions involving sections of sheaves and étale maps, but nothing really that will make the theory easier or deeper.

The basic result can be stated as follows.

Theorem 4.4.8 (Purity of the branch locus). *Let* $(R, \mathfrak{m})$ *be a regular local ring with field of fractions* K*, and let* S *be a Noetherian normal integral extension of* R *in a finite separable field extension of* K*. If* $\mathfrak{P} \in \operatorname{Spec} S$ *is ramified then* $\operatorname{Branch}(R/S)$ *is locally at* $\mathfrak{P}$ *defined by a height* 1 *unmixed ideal.*

Regrettably, the proof exceeds the purpose of the book.

The problem can be stated for nonintegral extensions. For a fairly recent account on this and the relation to the theory of tangent star cones and starlike linear varieties, see [146].

4.5 Historic note

The notion of a derivation and its theory grew up as an abstraction of methods of differential geometry. One of its segments has a pretty classical history, namely, the so-called differential algebra. The latter has its origins in the Picard–Vessiot theory of algebraic differential equations back in nineteenth century. One of the great achievements along this line is the Cartan–Kähler generalization of the Cauchy–Kowalewski theorem, where a central role is taken by a differential ideal.

Another segment took up the study of properties of algebras by looking at their module of derivations. Both are active fields as a rule, although the ring theoretic properties stemming from the existence of derivations of special kind seems to be more intense in noncommutative ring theory, in particular, in Lie algebra theory.

In commutative algebra and algebraic geometry, the focus has been mainly in properties of the associated modules and their cohomological theory, with emphasis

in important developments in the geometric theory of differentials and Hodge theory. It becomes difficult to pinpoint without gross error the origins of the use of derivations in commutative algebra, although it is easy to give a list of many important papers that more or less imprinted the main directions to the theory.

Beyond the prevalent ideas of differential algebra and ideals, the systematic use of derivations seems to have become universally used in the twenties/thirties of last century, with the work of A. Weil and the German school, which had Kähler as one of the founders. The main didactic work of Kähler about derivations and the exterior calculus is the *Geometria Aritmetica* ([90]), written in a perfect Italian, as a reflexion of his intensive interchange with the Italian algebraic geometry school, under the leadership of G. Castelnuovo, F. Enriques and B. Segre and others. This 400-page manuscript (a paper, not a book), written before the Second War and augmented in the 1950s afterwards, is not an easy reading for the modern taste. It starts with the definition of derivations and differentials, but uses a language of infinitesimal elements (meaning, nilpotents). The reader might expect to find a clue about what one calls nowadays Kähler differentials in terms of the conormal module of the diagonal ideal, but to one's dismay nothing like it meets the eye. It would look that this way of thinking appeared clearly stated for the first time in [33]. In a much later paper (1953), Kähler converts parts of the Geometria Aritmetica to German, where some of the weird terminology gets a little updated. But still one finds the same notion of differentials by means of giving the module Ω_R/k in terms of the image of the universal differential and the exterior rule $da \wedge db = 0$.

The reader avid to know more about this intense period of differential activity, caught in-between the World War II, is urged to read [91], specially the neat account by one of the editors (R. Berndt).

4.6 Exercises

Exercise 4.6.1. Let R stand for an k-algebra and let $\mathcal{A} = (a_{i,j})$ denote an $r \times r$ matrix with entries in R. For any $D \in \mathrm{Der}_k(R)$, show that

$$D(\det \mathcal{A}) = \sum_{i,j} \Delta_{i,j} D(a_{i,j}),$$

where $\Delta_{i,j}$ is the signed (i,j)-cofactor of $\mathcal{A}$.

(Hint: First, do the case where the $a_{i,j}$ are independent indeterminates over k.)

Exercise 4.6.2. Let $R = k[x_1, \ldots, x_n]$ be a polynomial ring over a field of characteristic zero and let $I \subset R$ be a homogeneous ideal in the standard degree of R.

(1) Show that $\sum_{i=1}^{n} \overline{x_i}\partial/\partial x_i$ is a derivation of $\mathrm{Der}_k(R/I)$, where "bar" denotes residue modulo I (this is called the *Euler derivation*).
(2) Suppose that $I = (f)$ is principal.

(a) Give a direct argument to prove that $\mathrm{Der}_k(R/(f))$ is generated by the Euler derivation and the residues of a set of generating syzygies of the gradient of f on R.
(b) If, moreover, the gradient ideal of f on R is $(x_1, \dots, x_n)$-primary then $\mathrm{Der}_k(R/(f))$ is generated by the Euler derivation and the trivial relations of the derivatives of f ("Koszul"). Apply to the case of a smooth plane projective curve of degree m to show that $\mathrm{Der}_k(R/(f))$ is generated in degrees $m-1$, besides the Euler derivation.

Exercise 4.6.3. Let $R = k[x,y]$ and $I = (x,y)^2$. Let Θ denote the Jacobian matrix of $\{x^2, xy, y^2\}$.
(1) Show that $\mathrm{Syz}_R(\Theta) = \{0\}$.
(2) Show that $\mathrm{Der}_k(I) = ((x,y)/I)\frac{\partial}{\partial x} \bigoplus ((x,y)/I)\frac{\partial}{\partial y}$.
(Caveat: (2) is a special case of Proposition 4.2.11, but the intention is that the calculation be redone in this simple case.)

Exercise 4.6.4. Let $R = k[x_1, \dots, x_n]$ be a polynomial ring over a field of characteristic zero and let $I \subset R$ be an ideal. Suppose that I admits a system of generators $f_1, \dots, f_s$ such that $\dim k[f_1, \dots, f_s] = \dim R$.
(1) Show that the Jacobian matrix of $f_1, \dots, f_s$ has no nonzero syzygies.
(2) Let $I = \ker k[x_1, \dots, x_6] \twoheadrightarrow k[t^2, tu, tv, u^2, uv, v^2] \subset k[t,u,v]$.
(a) Show that I is generated by the 2-minors of the 3×3 generic symmetric matrix $\mathcal{S}$ ("Veronese").
(b) Show that I satisfies the standing hypothesis above.
(Hint: prove that the determinant of the Jacobian matrix is the square of that of the symmetric matrix.)
(c) Argue that the formula in Exercise 4.6.1 is compatible with the argument in Exercise 4.6.2.

Exercise 4.6.5. Consider the example (2) of Exercise 4.6.4, setting $B = k[t,u,v]$. Let Θ denote the Jacobian matrix of the generators of I (the 2-minors of the 3×3 generic symmetric matrix). Show that the B-module M generated by the columns of Θ evaluated at the defining parameters has the following properties:
(1) M is torsion-free.
(2) M has rank 3.
(3) M is locally free except at the maximal ideal (t,u,v).
(4) The B-dual of M is a free module.

(Such modules are sometimes called *ideal modules*; moreover, in this case, it is the module of sections of a rank 2 vector bundle in $\mathbb{P}^2$.)

Exercise 4.6.6. Let $I = \ker k[x_1, \dots, x_4] \to k[t^3, t^2u, tu^2, u^3] \subset B = k[t,u]$ such that $x_1 \mapsto t^3$, $x_2 \mapsto t^2u$, $x_3 \mapsto tu^2$, $x_4 \mapsto u^3$ ('rational normal cubic'). Let θ denote the Jacobian matrix of the given parameters and let $\mathfrak{Z} \subset B^3$ denote the module of relations ('syzygies') of θ^t; let Θ stand for the Jacobian matrix of a set $\mathbf{f}$ of generators of I and set $\mathfrak{D} := \Theta^t(\mathbf{f}) \subset B^3$ for the evaluated transpose.

(1) Show that $\mathfrak{D} \subset \mathfrak{Z}$.
(2) Compute the condutor $\mathfrak{D} :_B \mathfrak{Z}$ and show it contains the Jacobian ideal of $A = k[\mathbf{x}]/I$ evaluated at the parameters.
(Obs: (1) comes off 4.1.9.1, but it is intended to have a direct computation in this example.)

Exercise 4.6.7. Consider the k-subalgebra

$$k[t_1t_2, t_2t_3, t_3t_4, t_4t_5, t_5t_6, t_1t_6, t_1t_3, t_3t_5, t_1t_5] \subset k[t_1, t_2, t_3, t_4, t_5, t_6]$$

over a field of characteristic zero and let $I \subset k[\mathbf{x}]$ denote its defining ideal induced by the given parameters.

(1) Prove that I has codimension 3.
(Hint: show that the algebra has maximal dimension (= 6) by giving a nonvanishing 6-minor of the Jacobian matrix of the parameters.)
(2) Establish that I is generated by three quadrics forming a regular sequence, plus a cubic. (Hint: to avoid a computer calculation, apply the interpretation of the parameters as edges of a simple graph, so the relations will pop up of the independent even circuits.)
(3) In the notation of Exercise 4.6.6 show that $\mathfrak{D} = \mathfrak{Z}$ and this module is only 3-generated (so the cubic generator has been differentially absorbed by the quadrics!).

Exercise 4.6.8. Consider the parametrization consisting of the first six parameters as in the previous exercise and the two additional parameters t_2t_4, t_2t_6.

(1) Prove that the defining ideal I has height 2.
(Hint: check a nonzero 6-minor of the Jacobian matrix of the parameters—as in the previous exercise, one can use the minor corresponding to the first six parameters.)
(2) Prove that I is the ideal of the maximal minors of a 3×2 matrix.
(Hint: Show that there is a quadratic binomial generator, giving an obvious 2×2 matrix, then "complete" it to the whole matrix.)
(3) Show that the second symbolic power of I coincides with its usual second power. (hence, the conormal module I/I^2 is a torsion-free $k[\mathbf{x}]/I$-module).
(This turns out to be theoretically harder—use a computer calculation instead.)
(4) I/I^2 is a reflexive module.
(This is even harder—it would follow from knowing that the module of differentials $\Omega_{k[\mathbf{x}]/I/k}$ is torsion-free.)

Exercise 4.6.9. Consider the homogeneous polynomial $f = x^6 + x^3y^3 + x^2y^4 + y^5z \in R = \mathbb{C}[x, y, z]$ in 3 variables and let J denote its gradient ideal.

(1) Show that R/J is not Cohen–Macaulay.

(2) Let $J^{\text{un}} \subset R$ denote the unmixed part of J. Prove that the initial degree of J^{un}/J is ≥ 6.
(Hint: try x^2y^4.)

(3) Prove that the partial derivatives of f are algebraically independent over $\mathbb{C}$, but admit nonzero polynomial relations of degree 2 with coefficients of degree ≥ 1 in R.

Exercise 4.6.10. Go through the steps of the previous exercise, this time around with $f = xyz(x + y)(x + z)(y + z)$. What differences do you find?

5 Basic advanced theory

5.1 Dimension theory

5.1.1 Annihilators, 1

Throughout, as before, R denotes a commutative ring. Since enough of the required preliminaries for this part has been developed in a previous section, one can proceed immediately to the main concepts.

A useful way of associating an ideal to an R-module M is by way of its annihilator $0 :_R M := \{a \in R \mid ax = 0\ \forall x \in M\}$. If R is understood from the context, one simply writes $0 : M$.

Let $\operatorname{Spec} R$ denote the set of prime ideals of R. The *support* of an R-module M is the set $\operatorname{supp} M := \{P \in \operatorname{Spec} R \mid 0 : M \subset P\}$.

Clearly, $0 : M \subset P \Leftrightarrow M_P \neq 0$, thus justifying the terminology in a slightly more geometric way. Notably, $\operatorname{supp} R = \operatorname{Spec} R$.

A basic property of a finitely generated R-module M is the equality

$$\operatorname{supp} M = \operatorname{supp} R/(0 : M).$$

To see this, say, $M = \sum_{i=1}^n Rx_i$. Then $\operatorname{supp} M = \bigcup_{i=1}^n \operatorname{supp} Rx_i$. On the other hand, clearly $0 : M = \bigcap_{i=1}^n (0 : x_i)$, from which $\operatorname{supp} R/(0 : M) = \bigcup_{i=1}^n \operatorname{supp} R/(0 : x_i)$. But, quite generally, $Rx \simeq R/(0 : x)$ for any $x \in M$. Thence, the assertion.

The following elementary property of annihilators is often useful.

Proposition 5.1.1. *Let M denote a finitely generated R-module and $I \subset R$ an arbitrary ideal. Then the ideals $(0 : M, I)$ and $0 : M/IM = IM : M$ have the same radical.*

Proof. The inclusion $(0 : M, I) \subset 0 : M/IM$ is clear. Conversely, let $M = \sum_{i=1}^m Rx_i$ and pick $a \in 0 : M/IM$. Write each ax_i as R-linear combinations of the x_i's and apply the determinantal trick (see Remark 2.2.2) to deduce that some power of a belongs to $(0 : M, I)$. □

More refined properties of finitely generated modules regarding their annihilators are given in the next subsection.

5.1.2 The Nakayama lemma

A great advantage of modules over vector spaces is the flexibility of changing the coefficient ring in a compatible way with various module operations. The abstract way of dealing with this is via tensor product. Thus, if $R \to R'$ is a ring homomorphism and M is an R-module, then $M \otimes_R R'$ is the R'-module obtained by change of rings (or by base change).

https://doi.org/10.1515/9783110616989-005

For the two basic ring homomorphisms of fractions and residue, one can rewrite the resulting module in terms of the respective data. Thus, if $R' = R_{\mathfrak{S}}$, with $\mathfrak{S} \subset R$ a multiplicatively closed set, then $M \otimes_R R' \simeq M_{\mathfrak{S}}$ is the usual module of fractions with denominators in $\mathfrak{S}$, while if $R' = R/I$, with $I \subset R$ an ideal, then $M \otimes_R R' \simeq M/IM$. Of course, both $M_{\mathfrak{S}}$ and M/IM are a priori bonafide modules over $R_{\mathfrak{S}}$ and R/I, respectively.

Now, from the theory of fractions one knows that if M is finitely generated, a necessary and sufficient condition for $M_{\mathfrak{S}} = \{0\}$ is that $\mathfrak{S} \cap (0 : M) \neq \emptyset$. One can ask if a similar condition holds for expressing $M/IM = \{0\}$, *i. e.*, for expressing the equality $M = IM$.

And indeed, one has the following.

Lemma 5.1.2. *Let M stand for a finitely generated R-module and let $I \subset R$ denote an ideal. Then $M = IM \Leftrightarrow (1 + I) \cap (0 : M) \neq \emptyset$, where $1 + I = \{1 + a \mid a \in I\}$.*

Proof. Note that $1 + I \subset R$ is a multiplicatively closed set, hence the result is equivalent to the assertion that $M/IM = \{0\} \Leftrightarrow M_{1+I} = \{0\}$. Alas, this format does not lead in essence to an easier way out.

Any way, assume first that $(1 + I) \cap (0 : M) \neq \emptyset$ and let $1 + a$ be any element thereof. Clearly, then $(1 + a)M = \{0\}$ implies that $M \subset aM \subset IM$.

Conversely, let $\{x_1, \ldots, x_n\}$ generate M. Writing out the condition $M \subset IM$ in terms of these generators yields a Cramer system whose determinant $\Delta \in R$ annihilates every x_i, hence $\Delta M = \{0\}$. On the other hand, $\Delta \in 1 + I$. □

The following result is somewhat an anticlimax, being an easy consequence of the lemma. In fact, there are other proofs that also show the elementary face of this acclaimed fact.

Proposition 5.1.3 (The Krull–Akizuki–Nakayama lemma). *Let M stand for a finitely generated R-module and let $I \subset R$ denote an ideal contained in every maximal ideal of R. If $M = IM$ then $M = \{0\}$.*

Proof. If $M \neq \{0\}$, let $P \in \operatorname{supp} M$ (Zorn). By Lemma 5.1.2, one can find $a \in I$ such that $1 + a \in 0 : M$. In particular, $1 + a \in P$, hence $1 + a \in \mathfrak{m}$, for some maximal ideal $\mathfrak{m}$ of R. On the other hand, by hypothesis $a \in \mathfrak{m}$, hence $1 \in \mathfrak{m}$, which is absurd. □

In this book, one will often incur in the abuse of referring to the above result as "the Nakayama lemma," hoping it will not mean any dishonor to the other authors.

Remark 5.1.4. The main assumption on I in the previous proposition is essential. For example, if I is itself a maximal ideal and $J \subset R$ is another maximal ideal then $I + J = R$, so that if one takes $M := R/J$ then $M/IM = \{0\}$.

Corollary 5.1.5. *Let M stand for a finitely generated R-module and let $I \subset R$ denote an ideal. Then*

$$\operatorname{supp} M/IM = \operatorname{supp} M \cap \operatorname{supp} R/I.$$

Proof. Given $P \in \operatorname{Spec} R$, one has $M_P = I_P M_P$ if and only if either $I_P = R_P$—*i. e.*, $P \notin \operatorname{supp} R/I$—or else $I_P \subset P_P$, in which case, $M_P = 0$ by Proposition 5.1.3. □

A finite set $\{x_1, \dots, x_n\}$ generating a module M is said to be *essential* if for every $i \in \{1, \dots, n\}$, one has $\sum_{j \neq i} Rx_j \neq M$. In general, two essential sets of generators of the same module M may have different cardinalities. In the classical ideal theory literature, such a set was called a *minimal base*. For example, if k is a field, the homogeneous maximal ideal $\mathfrak{m} = (x, y, z)$ of $R = k[x, y, z]$ admits essential sets of generators with more than 3 elements, one such easily seen to be $(x + z, x^2 + y, xy, x(x^2 + 1))$. Note, however, that locally at $\mathfrak{m}$ the element $x^2 + 1$ is invertible, and in fact the cardinality of the essential sets of generators of $\mathfrak{m}_{\mathfrak{m}}$ is fixed.

The phenomenon behind the scenes here is the lemma of Krull–Akizuki–Nakayama. More exactly, one has the following.

Corollary 5.1.6. *Let $(R, \mathfrak{m})$ be a local ring and let M stand for a finitely generated R-module. Then:*

(i) *For any ideal $I \subset \mathfrak{m}$ the natural homomorphism $M \to M/IM$ induces a bijection between the family of essential sets of generators of the R-module M and the family of essential sets of generators of the R/I-module M/IM.*

(ii) *Any two essential sets of generators of M have the same cardinality and the latter coincides with the dimension of the $R/\mathfrak{m}$-vector space $M/\mathfrak{m}M$.*

Proof. (i) Let a bar over an element of M denote its residue in M/IM. A moment reflexion convinces us that it suffices to prove the following assertion: if $\{x_1, \dots, x_m\} \subset M$ is such that $\{\overline{x}_1, \dots \overline{x}_m\} \subset M/IM$ generates M/IM as R/I-module, then it generates M. For proving this, set $N := \sum_{i=1}^{m} Rx_i \subset M$. By construction, $M = IM + N$, hence $M/N = (IM + N)/N = I(M/N)$. By Proposition 5.1.3, $M/N = \{0\}$.

(ii) The special case of (i) with $I = \mathfrak{m}$ implies that any essential set of generators of M has the same cardinality as one of the $R/\mathfrak{m}$-module $M/\mathfrak{m}M$. But the latter is a vector space, hence the conclusion. □

As a consequence, one can freely talk about the *minimal number* of generators of a finitely generated module over a local ring R. The following notation will be used for this number: $\mu_R(M)$, or simply, $\mu(M)$ when R is clear from the context.

5.1.3 The Krull dimension and systems of parameters

The Krull dimension of a module M is an invariant of the structure of $\operatorname{supp} M$ as a partially ordered set.

Definition 5.1.7. Let R denote a commutative ring and let M stand for an R-module. The *dimension* of M is the supremum over the lengths of chains of prime ideals

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_\ell,$$

with $P_0 \in \operatorname{supp} M$.

The notation $\dim M$ will be employed throughout.

By the preliminaries in Subsection 5.1.1, one has $\dim M = \dim R/0 : M$. Thus, the dimension of a module boils down to the notion of dimension for rings.

One sets $\dim\{0\} = -1$ as a harmless convention.

Remark 5.1.8.

(1) Even if R and/or M are Noetherian, $\dim M = \infty$ may take place, in which case the supremum is not attained by any individual chain of prime ideals.

(2) Letting $\operatorname{Min}(C)$ denote the set of minimal elements of a partially ordered set C, one has $\dim M = \max\{\dim R/P \mid P \in \operatorname{Min}(\operatorname{supp} M)\}$. Consequently, if R is Noetherian, it suffices to look at the chains starting from a finite set of prime ideals, but in principle one still has to consider infinitely many such chains for each prime ideal of this finite set.

(3) Given a submodule $N \subset M$, one has $\operatorname{supp} N \subset \operatorname{supp} M$ and $\operatorname{supp} M/N \subset \operatorname{supp} M$, an easy consequence of the basic properties of annihilators. Therefore, $\dim N \leq \dim M$ and $\dim M/N \leq \dim M$.

The zero-dimensional case is quite clear:

Proposition 5.1.9. *Let R denote a Noetherian ring and let M stand for an R-module. The following conditions are equivalent:*

(i) $\dim M = 0$.

(ii) *Every $P \in \operatorname{supp} M$ is a maximal ideal.*

(iii) $\operatorname{Min}(M) = \operatorname{supp} M$.

(iv) $\operatorname{Min}(M)$ *is a finite set of maximal ideals.*

(v) $\operatorname{supp} M$ *is a finite set of maximal ideals.*

Proof. Left to the reader. □

Proviso. Henceforth, for the rest of this section, unless otherwise stated, $(R, \mathfrak{m})$ will denote a Noetherian local ring and its unique maximal ideal.

Definition 5.1.10. Let $M \neq \{0\}$ stand for a finitely generated module over $(R, \mathfrak{m})$. A *system of parameters* of M is a set of elements $a_1, \ldots, a_s \in R$, with s least possible, such that $\dim M/(a_1, \ldots, a_s)M = 0$.

As preliminaries, one has:

- The definition does not depend on the order of the elements in a system of parameters.
- The condition $\dim M/(a_1,\dots,a_s)M = 0$ implies that $\{a_1,\dots,a_s\} \subset \mathfrak{m}$.
- By the Krull–Akizuki–Nakayama lemma, $M/\mathfrak{m}M \neq \{0\}$, hence $\dim M/\mathfrak{m}M = 0$ as well. In particular, $s \leq \mu(\mathfrak{m})$.
- $s(M) = s(R/0 : M)$.

Let $s(M)$ denote the cardinality of a system of parameters of M. This notation will next be superseded. The main result of this part is the celebrated

Theorem 5.1.11 (Krull–Chevalley). *Let $M \neq \{0\}$ stand for a finitely generated module over $(R,\mathfrak{m})$. Then $\dim M$ is finite and $s(M) = \dim M$.*

Proof. First, note that since $s(M) = s(R/0 : M)$ and $\dim M = \dim R/0 : M$, one may assume that M is of the form R/I for some ideal $I \subset \mathfrak{m}$. Since $(R/I, \mathfrak{m}/I)$ is still local, one may assume that $M = R$. Then $s(R)$ is the least possible number of generators of an $\mathfrak{m}$-primary ideal of R.

(1) $\dim R \leq s(R)$.
This is a straightforward consequence of Krull's theorem (Theorem 2.5.27). Indeed, let $I \subset \mathfrak{m}$ denote an $\mathfrak{m}$-primary ideal with $\mu(I) = s(R)$. Since $\dim R = \operatorname{ht}\mathfrak{m}$, then $\dim R \leq \mu(I)$.

(2) $s(R) \leq \dim R$.
This inequality is Chevalley's discovery. One proceeds by induction on $\dim R$, which is finite by the first inequality.

If $\dim R = 0$, $\emptyset$ is a system of parameters of R. If $\dim M > 0$, then $\mathfrak{m} \notin P$ for every $P \in \operatorname{Min}(R)$ such that $\dim R = \dim R/P$. By the prime avoidance principle (Lemma 2.5.22), one can choose

$$a \in \mathfrak{m} \setminus \bigcup_{\dim R/P = \dim R} P.$$

One claims that $\dim R/(a) \leq \dim R - 1$. Indeed, consider a chain $P_0 \subsetneq \cdots \subsetneq P_\ell$ of prime ideals such that $P_0 \in \operatorname{Min}(R/(a))$ and $\dim R/(a) = \dim R/P_0$. Clearly, $a \in P_0$. Let $P \subset P_0$ be a minimal prime of R. If $a \in P$, then $\dim R/P < \dim R$ by the choice of a and hence $\dim R/(a) = \dim R/P_0 \leq \dim R/P < \dim R$, as required. If $a \notin P$, then $P \subsetneq P_0$, hence $P \subsetneq P_0 \subsetneq \cdots \subsetneq P_\ell$ is a chain of prime ideals in R, thus saying that $\dim R \geq \dim R/(a) + 1$. Therefore, in any case the dimension goes down at least by one.

Now by the inductive hypothesis, $s(R/(a)) \leq \dim R/(a)$. On the other hand, if $\{a_1,\dots,a_r\}$ is a system of parameters of $R/(a)$, then

$$R/(a,a_1,\dots,a_r) \simeq \big(R/(a)\big)/(a_1,\dots,a_r)\big(R/(a)\big),$$

has dimension zero, thus implying that $s(R) \leq s(R/(a)) + 1$.

Confronting the two sort of inequalities obtained, one deduces that $s(R) \leq \dim R$. □

Note that the proof of the inequality $s(R) \leq \dim R$ above suggests how to pick up an explicit system of parameters. More exactly, one has the following.

Proposition 5.1.12. *Let $M \neq \{0\}$ stand for a finitely generated module over $(R, \mathfrak{m})$. Given elements $a_1, \ldots, a_r \in \mathfrak{m}$, the following hold:*

(i) $\dim M \leq \dim M/(a_1, \ldots, a_r)M + r$.

(ii) *The following conditions are equivalent:*

(a) *The inequality in* (i) *is an equality.*

(b) *For every $j = 1, \ldots, r$ and for every $P \in \operatorname{supp} M/(a_1, \ldots, a_{j-1})M$ such that $\dim R/P = \dim M/(a_1, \ldots, a_{j-1})M$, one has $a_j \notin P$*

(c) *$\{a_1, \ldots, a_r\}$ is a subset of a system of parameters of M.*

Proof. (i) This follows from Theorem 5.1.11 and from the inequality $s(N) \leq s(N/aN) + 1$, which holds for any module N and any element $a \in \mathfrak{m}$.

(a) ⇒ (b) First, one can see that if the equality holds for a certain r then applying (i) for any lower value yields the following intermediate equalities:

$$\dim M/(a_1, \ldots, a_j)M = \dim M/(a_1, \ldots, a_{j-1})M - 1, \quad j = 1, \ldots, r.$$

This reduces to showing that, for any finitely generated R-module N and any $a \in \mathfrak{m}$ such that $\dim N/aN = \dim N - 1$ then a does not belong to any prime $P \in \operatorname{supp} N$ with $\dim N = \dim R/P$. In fact, if $a \in P$ then Corollary 5.1.5 implies that $P \in \operatorname{supp} N/aN$. It follows that $\dim N/aN \geq \dim R/P = \dim N = \dim N/aN + 1$, which is absurd.

(b) ⇒ (c) This is essentially the argument of the proof of (2) in Theorem 5.1.11.

(c) ⇒ (a) By definition, there are elements $a_{r+1}, \ldots, a_d \in \mathfrak{m}$, with $d = \dim M$, such that $\{a_1, \ldots, a_r, a_{r+1}, \ldots, a_d\}$ is a system of parameters of M. Now, the isomorphism

$$\big(M/(a_1, \ldots, a_r)M\big)/(a_{r+1}, \ldots, a_d)\big(M/(a_1, \ldots, a_r)M\big) \simeq M/(a_1, \ldots, a_r, a_{r+1}, \ldots, a_d)M$$

implies that $s(M/(a_1, \ldots, a_r)M) \leq d - r = \dim M - r$. Applying Theorem 5.1.11, this inequality establishes the inequality in the reverse direction as that of item (i). Thus, one has an equality as stated. □

Remark 5.1.13. One has thus seen that, although Chevalley's original concept of a system of parameters has to do with minimal cardinalities of $\mathfrak{m}$-primary ideals, the nature of a set of generators thereof is essentially combinatorial in the sense that it depends on a principle of successive avoidance of a subset of minimal prime ideals of the iterated residual modules. The reader is refereed to a later section of the book (Theorem 7.4.31) where a third numerical invariant comes up, as introduced by P. Samuel. The equality of the three invariants is called the theorem of Krull–Chevalley–Samuel (historic order).

One of the most elementary and useful aspects of systems of parameters is the proof of the next result. As a matter of terminology, a homomorphism $\varphi : (R, \mathfrak{m}) \to (S, \mathfrak{n})$ of Noetherian local rings is said to be a *local homomorphism* if $\varphi(\mathfrak{m}) \subset \mathfrak{n}$.

Proposition 5.1.14 (Fiber dimension inequality). *Let $\varphi : (R, \mathfrak{m}) \to (S, \mathfrak{n})$ be a local homomorphism of Noetherian local rings. Then* $\dim S \leq \dim R + \dim S/\mathfrak{m}S$.

Proof. Note that $S/\mathfrak{m}S$ is a local ring with maximal ideal $\mathfrak{n}/\mathfrak{m}$. Set $\overline{S} = S/\mathfrak{m}S$. Choose systems of parameters $\{a_1, \ldots, a_r\} \subset \mathfrak{m}$ and $\{\overline{b}_1, \ldots, \overline{b}_s\} \subset S/\mathfrak{m}S$ of R and $S/\mathfrak{m}S$, respectively. By definition, some power of $\mathfrak{m}$ lands in the ideal $(a_1, \ldots, a_r) \subset R$ and some power of $\mathfrak{n}$ lands in the ideal $(\mathfrak{m}, b_1, \ldots, b_t) \subset S$. Therefore, some power of $\mathfrak{n}$ lands in the ideal $(a_1, \ldots, a_r, b_1, \ldots, b_t)$. This shows that $\dim S \leq r + t = \dim R + \dim S/\mathfrak{m}S$. □

Remark 5.1.15. Equality above takes place if φ is injective satisfying the going down property (in particular, if φ is flat—a notion introduced in Definition 6.2.56)

5.2 Associated primes and primary decomposition

The moral of this part is that to a Noetherian module one can associate a set of prime ideals endowed with a meaningful structure that allows to look at the module with powerful lens so to say. To this set corresponds a certain decomposition of the zero module into an intersection of simpler modules, called primary.

5.2.1 Annihilators, 2

If M is an R-module and $x \in M$ is a given element, the annihilator $0 : x := 0 :_M Rx \subset R$ of a cyclic submodule is the typical annihilator to have a prominent role in this part. Of course, by its very inception, such annihilators have significant impact in the properties of the zero divisors on M.

One lets $\mathcal{Z}(M) := \bigcup_{0 \neq x \in M} (0 : x)$ stand for the set of zero-divisors on M. Since the complementary set $R \setminus \mathcal{Z}(M)$ is multiplicatively closed, it follows that $\mathcal{Z}(M)$ is the union of the prime ideals it contains. This is however a loose assertion. With a few more restrictions, one can improve on this. The following result is so basic that it becomes difficult to find its origins (Krull?).

Proposition 5.2.1. *Let R denote a Noetherian ring and let $M \neq 0$ stand for a finitely generated R-module. Then $\mathcal{Z}(M)$ is the union of a finite family of prime ideals. More precisely, there exists a set of elements $\{x_1, \ldots, x_n\} \subset M$ such that each $0 : x_i$ is a prime ideal having the property that*

$$\mathcal{Z}(M) = \bigcup_{i=1}^{n} (0 : x_i).$$

Proof. By definition, $\mathcal{Z}(M)$ is the union of the full family of annihilators $0 : x$, with $0 \neq x \in M$. Since R is Noetherian, $\mathcal{Z}(M)$ is also the union of the subfamily of the maximal annihilators in the full family. Any such maximal annihilator is actually a prime ideal. Indeed, let $0 : x$ denote one such annihilator and let $a, b \in R$ be such that $ab \in 0 : x$, but $a \notin 0 : x$. Then $ax \neq 0$ and, on the other hand, clearly $0 : x \subset 0 : ax$. By the assumed maximality, necessarily $0 : x = 0 : ax$. Mas, since b annihilates ax by hypothesis, it follows $b \in 0 : x$, as required (According to I. Kaplansky, this simple argument is due to I. Herstein).

One next claims that the latter family of maximal annihilators is in fact finite. Consider the submodule $N \subset M$ generated by the elements $x \in M$ such that $0 : x$ is maximal as said. Since M is Noetherian, N is finitely generated. By Hilbert's device, fixing a finite subset of generators of N and expressing every element of this set in terms of the (possibly infinitely many) generators of N whose annihilator is maximal, one may assume that N is actually generated by finitely many generators whose annihilators are maximal; say, $N = \sum_{i=1}^{n} Rx_i$, where each $0 : x_i$ is maximal in the family of annihilators. To conclude, it suffices to show that any annihilator $0 : x$ which is maximal in the family of annihilators coincides with some $0 : x_i$. For this note that, as $x \in N$, then $0 : x \supset \bigcap_{i=1}^{n}(0 : x_i)$. Since $0 : x$ is a prime ideal then $0 : x \supset 0 : x_i$ for some $i \in \{1, \ldots, n\}$. Finally, by the maximality of $0 : x_i$, one must have $0 : x = 0 : x_i$. □

Remark 5.2.2. Note that the above result does not claim that, whenever $\mathcal{Z}(M)$ is expressed as the union of an arbitrary family of prime ideals then one can extract a finite subfamily thereon whose union is $\mathcal{Z}(M)$. As an example, take $M = R = k[X, Y]/(X, Y) \simeq k$. Then $\mathcal{Z}(M)$ is the union of the family of principal prime ideals contained in (X, Y), but certainly not the union of any finite subfamily thereof.

5.2.2 Associated primes

The preceding discussion motivates the following concept.

Definition 5.2.3. Let M stand for an R-module. A prime ideal $P \subset R$ is an *associated prime* of M if $P = 0 :_R x$, for some $x \in M$ (necessarily, $x \neq 0$).

Note that, quite generally, given $x \in M$, with $x \neq 0$, the annihilator $0 : x$ is the kernel of the R-module homomorphism $R \to M$ mapping 1 to x. Thus, looking for an associated prime of M is the same as searching for an element $x \in M$ such that $Rx \simeq R/P$ for some prime ideal $P \subset R$. As seen, this problem rests on a complicated recipe mixing properties of R-module homomorphisms—a "linear" notion—and those of ideals which depend on the multiplicative structure of R.

Let $\operatorname{Ass} M$ denote the family of associated primes of the R-module M.

Since the set M could have a structure of module over another ring S and the definition of an associated prime clearly depends of the coefficient ring in question, it

might be more precise to write $\mathrm{Ass}_R M$ for $\mathrm{Ass}\, M$. However, one will seldom use this more precise notation.

A basic result, to be shown a little later, is that this family is finite provided R is Noetherian and M is finitely generated. For the moment, one has easily the following.

Proposition 5.2.4. *Let R denote a Noetherian ring and let $M \neq 0$ stand for a finitely generated R-module. The set of maximal elements of the family of associated primes of M if finite.*

Proof. Let $P = 0 : x \in \mathrm{Ass}\, M$ be a maximal element in $\mathrm{Ass}\, M$. Since $x \neq 0$, then P is contained in a maximal element Q of the family of annihilators of nonzero elements of M. By the proof of Proposition 5.2.1, Q is a prime ideal, hence is an element of $\mathrm{Ass}\, M$. Since P is maximal in $\mathrm{Ass}\, M$, one must have $P = Q$, hence P is a maximal element of the family of all annihilators of nonzero elements of M. But the latter family is finite once more by the proof of Proposition 5.2.1. This shows that the set of maximal elements in $\mathrm{Ass}\, M$ is finite as well. □

Remark 5.2.5. A few preliminary properties of associated primes will hold assuming that either R or M is Noetherian, not necessarily both. For example, M could be a finitely generated algebra over a Noetherian ring R, but not so as R-module, and hence not Noetherian as such. In such a setup, $\mathrm{Ass}\, M$ may not be particularly interesting, giving way to the more interesting finite set $\mathrm{Ass}\, M$, where M is considered as a Noetherian ring. This situation, apparently paradoxical to the novice, will be part of the normal routine of the theory.

Next are a few elementary properties of associated primes.

Proposition 5.2.6. *Let R be a commutative ring and let M be an R-module.*

(i) $0 : M \subset P$ *for every* $P \in \mathrm{Ass}\, M$

(ii) *If $M = R/P$, with P a prime ideal, then* $\mathrm{Ass}\, M = \{P\}$ (*in particular, if R is a domain,* $\mathrm{Ass}\, R = \{0\}$)
Assume, moreover, that R is Noetherian.

(iii) $\mathrm{Ass}\, M = \emptyset \Leftrightarrow M = \{0\}$

(iv) *If $N \subset M$ is a submodule, then* $\mathrm{Ass}\, N \subset \mathrm{Ass}\, M \subset \mathrm{Ass}\, N \cup \mathrm{Ass}\, M/N$

(v) *Given R-modules $M_1, \ldots, M_n$, one has*

$$\mathrm{Ass}(M_1 \oplus \cdots \oplus M_n) = \mathrm{Ass}\, M_1 \cup \cdots \cup \mathrm{Ass}\, M_n.$$

In particular, $\mathrm{Ass}\, R^n = \mathrm{Ass}\, R$, *for any n.*

(vi) *If $M \subset R^n$, for some n, then* $\mathrm{Ass}\, M \subset \mathrm{Ass}\, R$. *In particular, if $M = I$ is an ideal of R, then* $\mathrm{Ass}\, I \subset \mathrm{Ass}\, R$.

(vii) *If $N \subset M$ is a submodule, then* $\dim N \leq \dim M$ *and* $\dim M/N \leq \dim M$; *moreover, at least one of these inequalities is an equality.*

(viii) *If M, N are finitely generated R-modules, then*

$$\mathrm{Ass}\big(\mathrm{Hom}(M, N)\big) = \mathrm{supp}\, M \cap \mathrm{Ass}(N).$$

Proof. (i) One has $P \in \operatorname{Ass} M \Rightarrow P = 0 : x$, for some $x \in M$. Clearly, $0 : M \subset 0 : x$.

(ii) Let a bar over a subset of R denotes its residual image in R/P. Then $P = \overline{0} : \overline{1}$, hence $P \in \operatorname{Ass} R/P$. Conversely, let $Q \in \operatorname{Ass} R/P$, say, $Q = \overline{0} : \overline{x} = P : x$. Since $x \neq 0$, one must have $Q = P$.

(iii) If $M = 0$, clearly $\operatorname{Ass} M = \emptyset$ since the notion of an associated prime involves the existence of a nonzero element of M. Conversely, let $x \in M, x \neq 0$. As R is Noetherian, $0 : x$ is contained in a maximal annihilator $0 : y$, with $y \in M, y \neq 0$ and the latter is prime by the proof of Proposition 5.2.1, hence is an element of $\operatorname{Ass} M$.

(iv) Since for $x \in N$ the kernel of a homomorphism $R \twoheadrightarrow Rx \subset M$ coincides with that of the composite of $R \twoheadrightarrow Rx \subset N$ with the inclusion $N \subset M$, the inclusion $\operatorname{Ass} N \subset \operatorname{Ass} M$ is obvious. From the other end, let $P = 0 : x \in \operatorname{Ass} M$ such that $P \notin \operatorname{Ass} N$. In particular, $x \notin N$. Now, $Rx \cap N$ is a submodule of both Rx e N. If $Rx \cap N \neq \{0\}$, then $\operatorname{Ass} Rx \cap N \neq \emptyset$ (by (iii)); hence, on one hand $P \in \operatorname{Ass} Rx \cap N$ (by (ii) and the first part) and, on the other hand $P \in \operatorname{Ass} N$ (again by the first part). From this contradiction, one must have $Rx \cap N = \{0\}$. This gives $N : x \subset 0 : x = P$. Since the opposite inclusion is trivial, one gets $N : x = P$. As $x \notin N$ then $P \in \operatorname{Ass} M/N$.

(v) This is an immediate consequence of (iv).

(vi) This follows from (iv) and (v).

(vii) Using the characterization of dimension in terms of the residue ring of the corresponding annihilator, the two inequalities are immediate. Now let $P \in \operatorname{Ass} M$ such that $\dim M = \dim R/P$. By (iv), one has $P \in \operatorname{Ass} N \cup \operatorname{Ass} M/N$. Say, $P \in \operatorname{Ass} N$. Then $\dim N \geq \dim R/P$, hence $\dim N = \dim M$. The alternative $P \in \operatorname{Ass} M/N$ works the same way.

(viii) The result is a lot easier if M, N are cyclic, say, $R/I, R/J$, respectively. Indeed, in this environment one has $\operatorname{Hom}(M, N) \simeq J : I/J$. Applying (iv) to the exact sequence

$$0 \to J : I/J \longrightarrow R/J \longrightarrow R/J : I \to 0$$

shows that $\operatorname{Ass}(\operatorname{Hom}(M, N)) = \operatorname{Ass}(J : I/J) \subset \operatorname{Ass}(R/J)$. The inclusion $\operatorname{Ass}(J : I/J) \subset \operatorname{Spec} R/I$ is clear: if $P \in \operatorname{Ass}(J : I/J) \setminus \operatorname{Spec} R/I$ then $(J : I/J)_P = \{0\}$, which is absurd. Let, conversely, $P \in \operatorname{Spec} R/I \cap \operatorname{Ass}(J : I/J)$. Then $P \notin \operatorname{Ass}(R/J : I)$, hence $P \in \operatorname{Ass}(J : I/J)$ once more by (iv).

For arbitrary modules, it is harder. Since R is Noetherian, one can reduce the problem to the case where $(R, \mathfrak{m})$ is a Noetherian local ring, in which case it will be enough to show that $\mathfrak{m} \in \operatorname{Ass}(\operatorname{Hom}(M, N))$ if and only if $\mathfrak{m} \in \operatorname{supp} M \cap \operatorname{Ass}(N)$. Assume the second; then $\mathfrak{m} \in \operatorname{supp} M$ implies $M \neq \{0\}$, hence there is a surjective composite $M \twoheadrightarrow M/\mathfrak{m}M \twoheadrightarrow R/\mathfrak{m}$. Since also $\mathfrak{m} \in \operatorname{Ass}(N)$, then the composite map $M \twoheadrightarrow R/\mathfrak{m} \hookrightarrow N$ gives an element of $\operatorname{Hom}(M, N)$ annihilated by $\mathfrak{m}$, hence $\mathfrak{m} \in \operatorname{Ass}(\operatorname{Hom}(M, N))$. The converse is similar, by picking an $\varphi \in \operatorname{Hom}(M, N)$ annihilated by $\mathfrak{m}$; in particular, $M \neq \{0\}$, and hence $\mathfrak{m} \in \operatorname{supp} M$, while $\operatorname{im}(\varphi) \subset N$ is annihilated by $\mathfrak{m}$. □

Remark 5.2.7. Note that, according to (vi) above, if R is a domain and $I \subset R$ is a nonzero ideal then $\operatorname{Ass} I = \{0\}$ is devoid of particular interest, whereas $\operatorname{Ass} R/I$ is a

very difficult object in general. The reader is adverted not to mix up these two sets of associated primes.

One now comes to the main finiteness character of the associated primes of a Noetherian module. In spite of its basic relevance to the theory, the main argument is rather an anticlimax, pretty much reminiscent of E. Noether's original devices.

The argument itself seems to have first appeared in [138] and [21, Chapter IV], but it might have been familiar to various sources.

Proposition 5.2.8. *Let R denote a Noetherian ring and let $M \neq 0$ stand for a finitely generated R-module. Then:*

(a) *M admits a finite sequence of submodules $\{0\} = M_0 \subset M_1 \subset \cdots \subset M_n = M$ such that, for every index $1 \leq i \leq n$, the residual module M_i/M_{i-1} is isomorphic to R/P_i, for some prime ideal $P_i \subset R$.*

(b) *$\operatorname{Ass} M$ is a finite set.*

Proof. (a) Let $P_1 \in \operatorname{Ass} M$. Write $R/P_1 \simeq M_1 \subset M$, for certain submodule $M_1 \subset M$. If $M = M_1$ one is done; otherwise, let $P_2 \in \operatorname{Ass} M/M_1$, so $R/P_2 \simeq M_2/M_1$, for some modulo M_2 such that $M_1 \subset M_2 \subset M$. Proceeding in this manner, one builds a chain of submodules $M_1 \subset M_2 \subset \cdots$ whose successive residual modules M_i/M_{i-1} are of the form R/P_i, for some prime ideal $P_i \subset R$. Since M is Noetherian, the chain stabilizes, say, after n steps. Then $M = M_n$ since otherwise one could go on by looking at $\operatorname{Ass} M/M_n$.

(b) It suffices to show that any $P \in \operatorname{Ass} M$ coincides with some prime P_i as obtained in the proof of (a). But this is clear as a result of applying Proposition 5.2.6 (iv) to the short exact sequences

$$0 \to M_{i-1} \to M_i \to M_i/M_{i-1} \to 0,$$

by descending recurrence. □

5.2.3 Primary decomposition

For understanding the main facts of primary decomposition of submodules, the knowledge of its didactically preceding primary decomposition of ideals is not required. Yet, if one wishes to delve into the present case by bringing in the basic theory for ideals, here is a small advice: primary decomposition is a relative theory in the sense that it tells us the structure of a module in terms of its simpler parts living in an ambient module. Thus, primary decomposition of an ideal is a theory dependent on the status of the ideal as a submodule of the ring. This is the all-out analogy to be kept in mind.

The required preliminaries lead to the following extension of the notion of the radical of an ideal, stressing its relative nature.

Definition 5.2.9. Let M stand for a module over a ring R and let $N \subset M$ denote a submodule. The *radical* of N in M, denoted $\sqrt{N : M}$, is the radical of the quotient $N : M$ as an ideal in R.

Note that the definition recovers the case of an ideal $I \subset R$ as $I : R = I$.

Next are some further properties.

Lemma 5.2.10. *Let R denote a Noetherian ring, let $M \neq 0$ stand for a finitely generated R-module and let $N \subset M$ stand for a submodule. Then:*

(i) $N : M \subset P$, *for every* $P \in \operatorname{Ass} M/N$ (*mnemonic from the ideal case:* $I : R = I \subset P$, *for every* $P \in \operatorname{Ass} R/I$).

(ii) $\sqrt{N : M} \subset \bigcap P_{P \in \operatorname{Ass} M/N} \subset \mathcal{Z}(M/N)$.

(iii) $\operatorname{Ass} M \subset \operatorname{supp} M$; *more generally, a prime ideal containing an element of* $\operatorname{Ass} M$ *belongs to* $\operatorname{supp} M$.

(iv) *If* $P \in \operatorname{supp} M$, *then* $P \supset P'$ *for some* $P' \in \operatorname{Ass} M$.

Proof. (i) Comes out of Proposition 5.2.6(i).

(ii) Follows from (i) and the definitions.

(iii) Let $P \subset P'$ be prime ideals, with $P \in \operatorname{Ass} M$. From general properties of localization, one has $M_P = (M_{P'})_{PR_{P'}}$. Thus, if $M_{P'} = 0$, then $M_P = 0$, too. By Proposition 5.2.6(iii), $\operatorname{Ass} M_P = \emptyset$. On the other hand, $P_P \in \operatorname{Ass} M_P$ since, as one easily verifies, if $P = 0 : x$, with $0 \neq x \in M$ then $P_P = 0 : R_P(x/1)$. This is a contradiction.

(iv) It suffices to show that every associated prime of the R_P-module M_P is of the form P'_P, for some $P' \subset P$ such that $P' \in \operatorname{Ass} M$. Now let $\tilde{P} \in \operatorname{Ass} M_P \subset \operatorname{Spec} R_P$. Since $\tilde{P}$ is a prime ideal of R_P, it has the form P'_P, for a uniquely determined prime ideal $P' \subset P$ of R. But, say, $\tilde{P} = 0 :_{R_P} (x/1)$ for certain $x \in M$ such that $x/1 \neq 0$, so one is tempted to guess that $P' = 0 : x$. In fact, the inclusion $0 : x \subset P'$ easily holds; unfortunately, the reverse inclusion may not always hold. One needs to adjust our first guess, namely, for each $a \in P'$, there is some $s \in R \setminus P$ such that $sax = 0$. Say, $P' = (a_1, \ldots, a_m)$ and for each $i = 1, \ldots, m$, let $s_i \in R \setminus P$ be such that $s_i a_i x = 0$. Set $s := \prod s_i$ and adjust x to $y := sx$, by which certainly $0 : x \subset 0 : y$. By construction, $yP' = (sx)P' = 0$, *i. e.*, $P' \subset 0 : y$. On the other hand, if $b \in 0 : y$, then $s(bx) = b(sx) = by = 0$, *i. e.*, $(b/1)(x/1) = 0$ holds in M_P, and hence $b/1 \in 0 : (x/1) = P'_P$. As P' is prime, one has $b \in P'$. This shows the reverse inclusion $0 : y \subset P'$. □

Recall the notation $\operatorname{Min}(\operatorname{supp} M)$ from the previous section and its analogue for subsets of $\operatorname{supp} M$.

Corollary 5.2.11. *Let R denote a Noetherian ring and let $M \neq 0$ stand for a finitely generated R-module. Then* $\operatorname{Min}(\operatorname{Ass} M) = \operatorname{Min}(\operatorname{supp} M) = \operatorname{Min}(\operatorname{supp} R/(0 : M))$. *In particular, for a submodule $N \subset M$ the equality*

$$\sqrt{N : M} = \bigcap_{P \in \operatorname{Ass} M/N} P$$

holds.

Proof. Follows from parts (ii) and (iv) of the previous lemma. □

Remark 5.2.12. Using Lemma 5.2.10(v), note that in particular the elements of $\operatorname{Min}(\operatorname{Ass} M) = \operatorname{Min}(\operatorname{supp} M) = \operatorname{Min}(\operatorname{supp} R/(0:M))$ belong to $\operatorname{Ass} M$. This set is often denoted simply $\operatorname{Min}(M)$ and its elements are called minimal associated primes of M for further emphasis.

The central notion of this part comes out of the following result.

Proposition 5.2.13. *Let R denote a Noetherian ring and let $M \neq 0$ stand for a finitely generated R-module. The following conditions are equivalent for a submodule $N \subset M$:*
(i) $\operatorname{Ass} M/N$ *consists of one element.*
(ii) $\mathcal{Z}(M/N) = \sqrt{N:M}$
(iii) $\mathcal{Z}(M/N) \subset \sqrt{N:M}$.
(iv) *Given $a \in R$ and $x \in M$ such that $ax \in N$, then $a \in N$ or $a \in \sqrt{N:M}$.*

Proof. Without loss of generality, one may assume that $N = \{0\}$ (why can one assume this?).

(i) $\Rightarrow$ (ii) By Corollary 5.2.11, $\sqrt{0:M} = \bigcap_{P \in \operatorname{Min}(M)} P$. Thus, if $\operatorname{Ass} M = \{P\}$, then, on one hand, $\operatorname{Min}(M) = \{P\}$ while $\mathcal{Z}(M) = P$ by Proposition 5.2.1 on the other hand.

(ii) $\Rightarrow$ (iii) Obvious.

(iii) $\Leftrightarrow$ (iv) Indeed, $ax = 0$, with $x \neq 0$, implies that $a \in \mathcal{Z}(M)$.

(iii) $\Rightarrow$ (i) Follow from Lemma 5.2.10 (i), by elementary properties of sets. □

Definition 5.2.14. Let R denote a Noetherian ring and let $M \neq 0$ stand for a finitely generated R-module. A submodule $N \subset M$ is called *primary* in M if any of the above equivalent conditions holds.

Remark 5.2.15.
(1) If $N \subset M$ is a primary submodule of M, then its radical in M is a prime ideal. Following the tradition in the case of ideals, one may say that then N is P-primary, where $P = \sqrt{N:M}$.
(2) A submodule $N \subset M$ is a primary submodule of M if and only if $\{0\}$ is primary in M/N (this allows in various discussions to reduce a "relative" situation to an "absolute" one). In particular, an ideal $I \subset R$ is primary $\Leftrightarrow$ $\{0\}$ is primary in R/I.
(3) If M is a cyclic module, then $\{0\}$ is primary in $M \Leftrightarrow M \simeq R/I$, for some primary ideal $I \subset R$.

The next result is often useful in an inductive argument.

Lemma 5.2.16 (Weak converse of Proposition 5.2.6(iii)). *Let R denote a Noetherian ring and let M stand for a finitely generated R-module. For an any subset $\mathcal{P} \subset \operatorname{Ass} M$, there exists some submodule $N \subset M$ such that $\operatorname{Ass} M/N = \mathcal{P}$ and $\operatorname{Ass} N = \operatorname{Ass} M \setminus \mathcal{P}$.*

Proof. Consider the family of submodules $L \subset M$ such that $\operatorname{Ass} L \subset \operatorname{Ass} M \setminus \mathcal{P}$. This family is nonempty since, *e. g.*, $\{0\}$ belongs to it. Any maximal element of this family will fulfill the statement. In fact, let $N \subset M$ be such a maximal element. By Proposition 5.2.6(iv), it suffices to show that $\operatorname{Ass} M/N \subset \mathcal{P}$. For this, let $P \in \operatorname{Ass} M/N$, say, $R/P \simeq L/N$ for some submodule $L \subset M$ containing N. Always by Proposition 5.2.6(iv), $\operatorname{Ass} L \subset \operatorname{Ass} N \cup \{P\}$. By the maximality of N in the family, necessarily $\operatorname{Ass} L \not\subset \operatorname{Ass} M \setminus \mathcal{P}$. A fortiori, $P \in \mathcal{P}$, as desired. □

Next is the main theorem of this part.

Theorem 5.2.17 (Primary decomposition for modules). *Let R denote a Noetherian ring, let $M \neq 0$ stand for a finitely generated R-module and let $N \subset M$ stand for a submodule. Then there exist submodules $Q_1, \ldots, Q_m$, primary in M, such that $N = \bigcap_{i=1}^{m} Q_i$. For any such decomposition, the following uniqueness properties hold:*

(i) $\{\sqrt{Q_1 : M}, \ldots, \sqrt{Q_m : M}\} = \operatorname{Ass} M/N$. *Consequently, the radicals of the primary components Q_i are uniquely determined by the residual module M/N.*

(ii) *If the decomposition is in addition reduced—in the sense that superfluous components in the intersection have been omitted and those admitting same radical have been collected by intersection in one single component—then the submodules Q_i such that $\sqrt{Q_i : M}$ is a minimal element of* $\operatorname{Ass} M/N$ *are also uniquely determined by the residual module M/N.*

Proof. Without loss of generality, one can assume that $N = \{0\}$. If $\{0\}$ is primary in M, there is nothing to be shown. In any case, for each $P \in \operatorname{Ass} M$, apply Lemma 5.2.16 with $\mathcal{P} = \{P\}$, thus obtaining a submodule $Q(P) \subset M$ such that $\operatorname{Ass} Q(P) = \operatorname{Ass} M \setminus \{P\}$ and $\operatorname{Ass} M/Q(P) = \{P\}$. In particular, for every $P \in \operatorname{Ass} M$, $Q(P)$ is primary in M. Now assume the existence of some $P' \in \operatorname{Ass} \bigcap_{P \in \operatorname{Ass} M} Q(P)$. This would say that $P' \in \operatorname{Ass} Q(P)$ for every $P \in \operatorname{Ass} M$, thus implying that $\operatorname{Ass} M$ consists of a single element, *i. e.*, that $\{0\}$ is primary in M. Thus, one is through.

(i) One may assume that the given primary decomposition $\{0\} = \bigcap_i Q_i$ has no superfluous components. Consider the diagonal module homomorphism $M \longrightarrow \oplus M/Q_i$ induced in each coordinate by the residual map $M \twoheadrightarrow M/Q_i$. Its kernel is $\bigcap_i Q_i$, hence is injective. By Proposition 5.2.6(iv), (v), every element of $\operatorname{Ass} M$ belongs to $\operatorname{Ass} M/Q_i$, for some i, hence is the radical of Q_i in M. This shows one inclusion.

Now, for any fixed index i, the hypothesis of reducedness gives $Q_i \cap (\bigcap_{j \neq i} Q_j) = \{0\}$. This yields

$$\bigcap_{j \neq i} Q_j = \Big(\bigcap_{j \neq i} Q_j\Big) \Big/ \Big(Q_i \cap \Big(\bigcap_{j \neq i} Q_j\Big)\Big) \simeq \Big(Q_i + \bigcap_{j \neq i} Q_j\Big)/Q_i \subset M/Q_i.$$

Therefore, $\operatorname{Ass}(\bigcap_{j \neq i} Q_j) \subset \operatorname{Ass} M/Q_i$ and since $\bigcap_{j \neq i} Q_j \neq \{0\}$, necessarily $\operatorname{Ass}(\bigcap_{j \neq i} Q_j)$ coincides with $\sqrt{Q_i : M}$. On the other hand, obviously, $\bigcap_{j \neq i} Q_j \subset M$, hence $\sqrt{Q_i : M} \in \operatorname{Ass}(M)$.

(ii) Since one is assuming that the decomposition is reduced, the required uniqueness follows from the following preliminary of localization theory: if $Q, Q' \subset M$ are primary submodules having the same radical $P \in \operatorname{Spec} R$, then $Q = Q'$ if and only if $Q_P = Q'_P$. For convenience, one gives an argument for the nontrivial implication. Say, $x \in Q$. By assumption, $x/1 = x'/s$, for certain $x' \in Q'$ and $s \in R \setminus P$. Canceling denominators, one finds some $t \in R \setminus P$ such that $tx \in Q'$. Since Q' is primary in M with radical P, Proposition 5.2.13(iv) gives that $x \in Q'$. By a symmetric argument, one is done. □

Theorem 5.2.18 (Krull's intersection theorem). *Let R denote a Noetherian ring, let M stand for a finitely generated R-module and let $I \subset R$ denote an ideal contained in every maximal ideal of R. Then $\bigcap_{k\geq 0} I^k M = \{0\}$.*

Proof. One first proves the following general assertion: if M is a Noetherian module and $N \subset M$ is a submodule, then $IN \supset N \cap I^s M$ for some integer s.

In order to prove this assertion, consider a primary decomposition of the submodule IN in M, say, $IN = (\bigcap_i \mathcal{Q}_i) \cap (\bigcap_j \mathcal{Q}'_j)$, where the components are split into two sets: $I \subset \sqrt{\mathcal{Q}_i : M}$ for every i in the first set, while $I \not\subset \sqrt{\mathcal{Q}_i : M}$ for every j in the second set. Choose $s \gg 0$ such that $I^s \subset \mathcal{Q}_i : M$, $\forall i$. Then $I^s M \subset \bigcap_i \mathcal{Q}_i$. It remains to show that $N \subset \bigcap_j \mathcal{Q}'_j$. For this, let $f \in N \subset M$. Choose $a \in I \setminus \sqrt{\mathcal{Q}'_j : M}$ for every index j of the second set. By construction, $af \in \mathcal{Q}'_j$ for every j. By Proposition 5.2.13(iv), one deduces that $f \in \mathcal{Q}'_j$ for every j, as was to be shown.

Now apply to $N = \bigcap_{k\geq 0} I^k M \subset M$, obtaining

$$IN \supset N \cap I^s M = \bigcap_{k\geq 0} I^k M \cap I^s M = \bigcap_{k\geq 0} I^k M = N.$$

By Proposition 5.1.3, $N = \{0\}$. □

Remark 5.2.19. Krull's intersection theorem is also a consequence of the celebrated Artin–Rees lemma, proved independently by these two authors in the early 1950s (see Subsection 7.3.2.2). In fact, the substance of the proof above is the inclusion $IN \supset N \cap I^s M$, which is akin to both approaches.

5.3 Depth and Cohen–Macaulay modules

In Subsection 5.1, one has accounted for those sets of elements in a local ring $(R, \mathfrak{m})$ that generate an $\mathfrak{m}$-primary ideal and have minimal possible cardinality thereof, called systems of parameters of R. This has been extended to a finitely generated R-module M as well, where such $\mathfrak{m}$-primary ideals belong to the class of ideals often called *ideals of definition* of M. A notable characterization of a system of parameters on M has been given in terms of avoiding certain minimal prime ideals of the iterated residual modules of M. The moral of the present part is to focus on such avoidance

strategy regarding the entire set Ass M instead. This will lead to the important notion of *depth* and its uses.

The central notion of this part is the following.

Definition 5.3.1. Let R denote a ring and let M stand for an R-module. An *M-sequence* (or a *regular sequence on M*) is a sequence of elements $\mathbf{a} = a_1, \ldots, a_n \in R$ such that:
(1) $\mathbf{a}M \neq M$
(2) $a_i \notin \mathcal{Z}(M/(a_1, \ldots, a_{i-1})M)$ for $i = 1, \ldots, n$

Note that condition (2) above means that the elements of the sequence are obtained by avoiding the associated prime ideals of the iterated residual modules of M.

As in the situation of dimensions in Subsection 5.1, one introduces a parallel notion, where one looks instead for a maximum of the number of elements in such sequences. Since for the moment R is arbitrary, one introduces a more flexible definition. For convenience, one calls the number of elements in an M-sequence its length.

Definition 5.3.2. Let R denote a ring and let M stand for an R-module. Given an ideal $I \subset R$, the *depth* of M on I (or the I-depth of M) is the maximum length of an M-sequence on I.

Notation: $\operatorname{depth}_I(M)$ or $\operatorname{depth}_I M$.

Clearly, there is no guarantee that such a length be finite. One will see in a moment that it is finite under finiteness restrictions.

A first preliminary on these concepts is the following.

Proposition 5.3.3. *Let R denote a ring and let M stand for an R-module. Let $J \subset R$ denote an ideal such that $J \subset 0 : M$. A sequence of elements $a_1, \ldots, a_n \in R$ is an M-sequence if and only if the sequence of residues $\overline{a}_1, \ldots, \overline{a}_n \in R/J$ is an M-sequence. In particular, for any ideal $I \supset 0 : M$, one has* $\operatorname{depth}_I(M) = \operatorname{depth}_{I/(0:M)}(M)$.

Proof. By induction on n, it suffices to check that given $a \in R$, then $a \notin \mathcal{Z}_R(M) \Leftrightarrow \overline{a} \notin \mathcal{Z}_{R/J}(M)$, which is a consequence of the structure of M as an R/J-module. □

Lemma 5.3.4 (Exchange property). *Let $\{a_1, \ldots, a_n\} \subset R$ stand for an M-sequence. Then, for any $1 \leq i \leq n$, the sequence obtained by interchanging a_i and a_{i+1} is an M-sequence if and only if $a_{i+1} \notin \mathcal{Z}(M/(a_1, \ldots, a_{i-1})M)$.*

Proof. From the definition of an M-sequence, the assertion is seen to be a consequence of the following one: if $\{a_1, a_2\} \subset R$ is an M-sequence, then $a_1 \notin \mathcal{Z}(M/a_2M)$. The latter assertion is shown by a straightforward argument left to the reader. □

For the definition of depth, it suffices to look at the M-sequences with maximal length, *i. e.*, not contained properly in another M-sequence. The first question is thus if and when such sequences exist at all. This is the easy part of the following basic result.

Theorem 5.3.5 (Maximal regular sequence length stability). *Let R denote a Noetherian ring, let M stand for a finitely generated R-module and let $I \subset R$ denote an ideal such that $IM \neq M$. Then:*

(i) *Any M-sequence contained in I is contained in one such of maximal length.*

(ii) *Any two M-sequences of maximal length in I have the same length.*

In particular, $\operatorname{depth}_I(M)$ *is finite and attained as the length of any M-sequence of maximal length in I.*

Proof. (i) This depends only on the hypothesis that R is Noetherian. In fact, the assumption that $a_i \notin \mathcal{Z}(M/(a_1, \ldots, a_{i-1})M)$ for $i = 1, \ldots, n$ triggers a chain of ideas $(a_1) \subsetneq (a_1, a_2) \subsetneq \cdots \subsetneq (a_1, \ldots, a_i) \subsetneq \cdots$ that is eventually stationary.

(ii) This assertion is a lot more delicate. The present argument resembles the usual matroid-like exchange property. To proceed, it suffices to show the following assertion: given two M-sequences of the same length in I, if one is maximal then so is the other. Fixing notation, let $\{a_1, \ldots, a_n\} \subset I$ and $\{b_1, \ldots, b_n\} \subset I$ be M-sequences, of which the first is of maximal length. One inducts on n.

If $n = 1$, change notation to $a \in I$ and $b \in I$, respectively. One is assuming that both a and b are nonzero divisors on M and in addition $I \subset \mathcal{Z}(M/aM)$. Then one aims to show that $I \subset \mathcal{Z}(M/bM)$, too. Now, under the present finiteness hypotheses, one can pick a single element $u \in M$ such that its residue class in M/aM is nonzero and annihilated by I. In other words, $u \in M \setminus aM$ such that $Iu \subset aM$; in particular, $bu \in aM$. Writing $bu = av, v \in M$, one claims that $v \notin bM$ and $Iv \in bM$, thus showing that $I \subset \mathcal{Z}(M/bM)$. For this claim, note that if $v = bw \in bM$ then $bu = abw$, hence $u = aw \in aM$ as b is a nonzero divisor on M—a contradiction. Next, one has $aIv = bIu \in baM$; this time around one can cancel a, hence $Iv \subset bM$ as required.

Now assume that $n > 1$. Write

$$M_i = M/(a_1, \ldots, a_{i-1})M, \quad M_i' = M/(b_1, \ldots, b_{i-1})M,$$

for $1 \leq i \leq n$—note that the respective last two residual modules are excluded. Then, by prime avoidance, one can choose an element $c \in I \setminus \{\operatorname{Ass} M_i \cup \operatorname{Ass} M_i'\}$, for $1 \leq i \leq n$.

Thus, the two elements a_n and c are both nonzero divisors on the residual module $M_n = M/(a_1, \ldots, a_{n-1})M$; the first is an M_n-sequence of maximal length by hypothesis, while c is also an M_n-sequence of maximal length by the case $n = 1$ of the induction.

Applying Lemma 5.3.4, one can pull c ahead of the M-sequence $a_1, \ldots, a_{i-1}$ one step at a time, so as to have $c, a_1, \ldots, a_{n-1}$ an M-sequence on its own. This sequence is maximal in I since $I \subset \mathcal{Z}(M/(a_1, \ldots, a_{n-1}, c)M) = \mathcal{Z}(M/(c, a_1, \ldots, a_{n-1})M)$. By a similar token, $c, b_1, \ldots, b_{n-1}$ is an M-sequence, but not necessarily of maximal length.

Updating the ground module to M/cM, one has that $a_1, \ldots, a_{n-1}$ and $b_1, \ldots, b_{n-1}$ are M/cM-sequences, with the first of these of maximal length. Applying the inductive assumption, the second is also of maximal length. In particular, as argued above,

this implies that $b_1, \dots, b_{n-1}, c$ is a maximal M-sequence. Finally, by an additional application of the induction case $n = 1$, it comes out that $b_1, \dots, b_{n-1}, b_n$ is a maximal M-sequence. □

There is at least one alternative to the argument in the proof of Theorem 5.3.5(ii). It has the advantage of identifying the depth as a homological invariant, based on Proposition 6.2.76.

Second proof of Theorem 5.3.5*(ii).* Let $\mathbf{a} := \{a_1, \dots, a_n\} \subset I$ denote an M-sequence. Then the assertion that $\mathbf{a}$ has maximal length in I is tantamount to the inclusion $I \subset \mathcal{Z}(M/\mathbf{a}M)$, which in turn is the same as $\mathbf{a}M \subsetneq \mathbf{a}M :_M I$, or finally, equivalent to $\operatorname{Hom}_R(R/I, M/\mathbf{a}M) \neq 0$.

By Proposition 6.2.76, as applied with $R/I = N$ (note the reverted notation), the nonvanishing of the module $\operatorname{Hom}_R(R/I, M/\mathbf{a}M)$ is equivalent to the nonvanishing of $\operatorname{Ext}^n_R(R/I, M)$ and, moreover, n is the least integer $m \geq 0$ such that $\operatorname{Ext}^m_R(R/I, M) \neq 0$. Now, if $\mathbf{b} \subset I$ is another M-sequence with maximal length m, one can assume without loss of generality that $m \leq n$. By the same token, $\operatorname{Ext}^m_R(R/I, M) \neq 0$. Hence, necessarily, $m \geq n$ and, therefore, $m = n$. □

Corollary 5.3.6. *Let R be a Noetherian ring and let M denote a finitely generated R-module. If $I \subset R$ is an ideal such that $IM \neq M$ then the depth of M on I is the least integer n such that* $\operatorname{Ext}^n_R(R/I, M) \neq 0$.

One should remark that, following Rees terminology, the depth of M on I is called the *grade* of I on M. The latter terminology is more convenient in the case where $M = R$, so the emphasis is on a property of the ideal I.

Remark 5.3.7. Under the same finiteness conditions, it is possible to introduce a notion $\operatorname{depth}_R M$ of depth, with $I = R$, by taking the least upper bound of lengths of M-sequences $\{a_1, \dots, a_n\} \subset R$. Though the condition $IM \neq M$ is no longer satisfied, one requires by definition that $M/(a_1, \dots, a_n)M \neq 0$. In this book, one will have no use for this global notion since it can be shown that $\operatorname{depth}_R M = \sup\{\operatorname{depth}_{\mathfrak{m}}(M)\}$, where $\mathfrak{m}$ runs through the maximal ideals of R containing $0 : M$.

5.3.1 Basic properties of depth

Depth obeys a similar rule as height.

Proposition 5.3.8 (Depth and associated primes. I). *Let R be a Noetherian ring and let M denote a finitely generated R-module. If $I \subset R$ is an ideal such that $IM \neq M$, then*

$$\operatorname{depth}_I(M) = \min\{\operatorname{depth}_P(M) \mid P \in \operatorname{Ass} M/IM\}. \tag{5.3.8.1}$$

If in addition I is generated by an M-sequence, then $\operatorname{depth}_I(M) = \operatorname{depth}_P(M)$ *for every* $P \in \operatorname{Ass} M/IM$.

Proof. Since $P \in \operatorname{Ass} M/IM \Rightarrow P \supset 0 : M/IM \supset I$, then $\operatorname{depth}_I(M) \leq \operatorname{depth}_P(M)$. It suffices to show the existence of some $P \in \operatorname{Ass} M/IM$ such that $\operatorname{depth}_P(M) \leq \operatorname{depth}_I(M)$. For this, let $\mathbf{a} = \{a_1, \ldots, a_n\}$ denote an M-sequence of maximal length in I. In particular, $I \subset \mathcal{Z}(M/\mathbf{a}M)$, hence $I \subset Q$ for some $Q \in \operatorname{Ass} M/\mathbf{a}M$. But $\operatorname{supp} M/\mathbf{a}M \subset \operatorname{supp} M$ implies that $Q \in \operatorname{supp} M/IM$. Let $P \in \operatorname{Ass} M/IM$ such that $P \subset Q$, so $\operatorname{depth}_P(M) \leq \operatorname{depth}_Q(M)$. Since $Q \subset \mathcal{Z}(M/\mathbf{a}M)$, $\mathbf{a}$ is an M-sequence of maximal length in Q, showing that $\operatorname{depth}_Q(M) = n$. □

Proposition 5.3.9 (Depth and fractions). *Let R be a Noetherian ring and let M denote a finitely generated R-module.*

(i) *If $\mathfrak{S} \subset R$ is a multiplicatively closed set and $\mathbf{a} = \{a_1, \ldots, a_n\} \subset R$ is an M-sequence such that $\mathbf{a}\mathfrak{S}^{-1}M \neq \mathfrak{S}^{-1}M$, then the image of $\mathbf{a}$ in $\mathfrak{S}^{-1}R$ by the canonical homomorphism of fractions is an $\mathfrak{S}^{-1}M$-sequence. In particular, if $I \subset R$ is an ideal such that $I\mathfrak{S}^{-1}M \neq \mathfrak{S}^{-1}M$, then* $\operatorname{depth}_I(M) \leq \operatorname{depth}_{\mathfrak{S}^{-1}I}(\mathfrak{S}^{-1}M)$.

(ii) *Let $I \subset R$ $I \subset R$ be an ideal such that $IM \neq M$.*

  (a) *If $\mathbf{a} = \{a_1, \ldots, a_n\} \subset I$ is an M-sequence of maximal length and Q is a prime ideal containing I and such that $Q \in \operatorname{Ass} M/\mathbf{a}M$, then* $\operatorname{depth}_I(M) = \operatorname{depth}_{I_P}(M_P)$ *for every prime ideal $P \supset Q$.*

  (b) *There exists some maximal ideal $\mathfrak{m} \supset I$ such that*

$$\operatorname{depth}_I(M) = \operatorname{depth}_{I_{\mathfrak{m}}}(M_{\mathfrak{m}}).$$

Proof. (i) The proof is straightforward and is left to the reader.

(ii) (a) By (i), $\operatorname{depth}_I(M) \leq \operatorname{depth}_{I_P}(M_P)$. Set $Q = 0 : x$, with $x \in M \setminus \mathbf{a}M$. By assumption, $I \subset Q$, hence $I_P \subset Q_P$. But, $Q_P \in \operatorname{Ass} M_P/\mathbf{a}_P M_P$ and again by (i), $\mathbf{a}_P$ is an M_P-sequence. Thus, $\operatorname{depth}_{I_P}(M_P) \leq \operatorname{depth}_{Q_P}(M_P) = n$, where the last equality follows from the supplementary assertion of Proposition 5.3.8.

(b) It suffices to note that the hypothesis of item (a) is not vacuous because there is always some prime $Q \in \operatorname{Ass} M/\mathbf{a}M$ containing I. Then any maximal ideal containing Q will contain I and satisfies the required condition. □

Remark 5.3.10. The result in items (a), (b) above keeps a convenient flexibility in choosing the prime ideal P in question. Occasionally, one wishes to have P quite small—such as an associated prime of M/IM in the case where M is Cohen–Macaulay (next section)—or maximal as it happens quite often. Clearly, (b) also shows the following.

Proposition 5.3.11 (Depth versus height). *Let R be a Noetherian ring, let M denote a finitely generated R-module and let $I \subset R$ stand for an ideal such that $IM \neq M$. Then* $\operatorname{depth}_I(M) \leq \operatorname{ht} I/(0 : M)$.

Proof. If $(R, \mathfrak{m})$ is local, it follows from Proposition 5.1.12 and from Theorem 5.1.11 that $\operatorname{depth} M := \operatorname{depth}_{\mathfrak{m}}(M) \leq \dim M$. Let then $Q \supset I$ denote a prime ideal such that $\operatorname{ht} Q/(0 : M) = \operatorname{ht} I/(0 : M)$. In particular, $Q \in \operatorname{supp} M/IM$, so $Q \supset P$ for some $Q \in \operatorname{Ass} M/IM$.

By Proposition 5.3.9(i), one gets

$$\begin{aligned}\operatorname{depth}_I(M) \le \operatorname{depth}_P(M) \le \operatorname{depth}_{P_Q}(M_Q) \le \dim M_Q \\ = \operatorname{ht} Q/(0:M) = \operatorname{ht} I/(0:M),\end{aligned}$$

as was to be shown. □

For convenience, the simplified notation will be used throughout in the local case: $\operatorname{depth} M := \operatorname{depth}_{\mathfrak{m}}(M)$. The next result proves something stronger that the inequality $\operatorname{depth}_{\mathfrak{m}}(M) \le \dim M$ in the local case.

Proposition 5.3.12 (Depth and associated primes. II). *Let $(R, \mathfrak{m})$ be a local ring and $M \neq \{0\}$, a finitely generated R-module. Then*

$$\operatorname{depth} M \le \dim R/P, \quad \forall P \in \operatorname{Ass} M$$

Proof. Induct on $\dim R/P$, which is finite by Section 5.1. If $\dim R/P = 0$, then $P = \mathfrak{m}$, while clearly, $\operatorname{depth} M = 0$. Assume that $\dim R/P \ge 1$ and write $P = 0 : x$, with $x \in M \setminus \{0\}$. If $\operatorname{depth} M = 0$, there is nothing to prove.

If $\operatorname{depth} M \ge 1$, let $a \in \mathfrak{m} \setminus \mathcal{Z}(M)$. By Theorem 5.2.18, $\bigcap_{r\ge 0} a^r M = \{0\}$. Thus, choose $m \ge 0$ such that $x \in a^{m-1}M \setminus a^m M$ and set $b := a^m$. Then $b \in \mathfrak{m} \setminus \mathcal{Z}(M)$, while $x \notin bM$ by the choice of m. Therefore, $bM : x \subset Q$, for some $Q \in \operatorname{Ass} M/bM$ and, for even more reason, $P = 0 : x \subset Q$. Obviously, $bx \in bM$, hence $b \in Q$.

Thus, $(P, b) \subset Q$. In particular, as $b \notin P \subset \mathcal{Z}(M)$, it follows that $P \subsetneq Q$ and, consequently, $\dim R/Q < \dim R/P$. Applying the inductive hypothesis, one has

$$\operatorname{depth} M = \operatorname{depth} M/bM + 1 \le \dim R/Q + 1 \le \dim R/P + 1 - 1 = \dim R/P,$$

as was to be shown. □

For the nonlocal situation, one can file the following.

Corollary 5.3.13. *Let R be a Noetherian ring and let M stand for a finitely generated R-module. Then* $\operatorname{depth}_Q(M) \le \dim R/P,\ \forall P \in \operatorname{Ass} M,\ \forall Q \supset P,\ Q \in \operatorname{Spec} R$.

Proof. Localize at Q and apply Proposition 5.3.12. □

5.3.2 Mobility of depth

It is often very useful to move M-sequences around and see how the resulting depth behaves.

Proposition 5.3.14 (Permutability of M-sequences). *Let R be a Noetherian ring and let M stand for a finitely generated R-module. If $a_1, \dots, a_n$ is an M-sequence contained in the Jacobson radical of R, then any permutation of its elements still gives an M-sequence.*

Proof. By iteratively transposing adjacent elements, one can assume that $n = 2$. Set $a = a_1, b = a_2$ for further visibility. First, the inclusion $a \in Z(M/bM)$, which actually does not require that b belong to the Jacobson radical. Indeed, say $ax \in bM$, for some $x \in M$. Write $ax = by, y \in M$. By assumption, $b \notin Z(M/aM)$, hence $y \in aM$. Set $y = az, z \in M$. Substituting, as $a \notin Z(M)$ by assumption, it follows that $x = bz \in bM$.

To see that $b \notin Z(M)$, consider the submodule $N := 0 :_M b \subset M$. One claims that $N = aN$ and concludes that $N = \{0\}$, by the Krull–Akizuki–Nakayama lemma. In fact, given $x \in N$, one has $bx = 0$, say, $x = ay$, for some $y \in M$ because $b \notin Z(M/aM)$. Therefore, $aby = 0$, and hence, $by = 0$ since $a \notin Z(M)$. By construction, $y \in N$. Thus $x \in aE$, as claimed. □

Proposition 5.3.15 (Exponentiation in M-sequences). *Let R be a Noetherian ring and let M stand for a finitely generated R-module. If $a_1, \ldots, a_n$ is an M-sequence, then so is $a_1^r, \ldots, a_n^r$ for any integer $r \geq 1$.*

Proof. Induct on n. For $n = 1$, the result is clear as $a \notin Z(M) \Rightarrow a^r \notin Z(M)$. Assume that $a_1^r, \ldots, a_{n-1}^r$ is an M-sequence and show that the kernel of multiplication by a_n^r in $M/(a_1^r, \ldots, a_{n-1}^r)M$ is null. For this, localize at an arbitrary prime ideal P de R. If any amongst $a_1, \ldots, a_n$ does not belong P, the result is obvious. If $\{a_1, \ldots, a_n\} \subset P$, localizing at P and changing notation, one can assume that $(R, \mathfrak{m})$ is local and $a_1, \ldots, a_n \in \mathfrak{m}$. Since $a_1, \ldots, a_{n-1}, a_n^r$ is an M-sequence by the case $n = 1$, Proposition 5.3.14 implies that $a_n^r, a_1, \ldots, a_{n-1}$ is an M-sequence. Repeating this strategy with a sequence $a_n^r, a_1, \ldots, a_{n-2}, a_{n-1}$, one has that $a_n^r, a_1, \ldots, a_{n-2}, a_{n-1}^r$ is still an M-sequence and obtain, by the same token, that $a_{n-1}^r, a_n^r, a_1, \ldots, a_{n-2}$ is an M-sequence. Continuing this way, one eventually gets the full required result. □

Next is the main use of the above proposition.

Corollary 5.3.16 (Depth versus radical). *Let R be a Noetherian ring and let M stand for a finitely generated R-module. If $I, J \subset R$ are ideals having the same radical and such that $IM \neq M, JM \neq M$, then* $\operatorname{depth}_I(M) = \operatorname{depth}_J(M)$.

Proposition 5.3.17 (Depth and hypersurface sections). *Let R be a Noetherian ring and let M stand for a finitely generated R-module. If $I \subset R$ is an ideal such that $IM \neq M$, then for every element a belonging to the Jacobson radical of R, one has*

$$\operatorname{depth}_{(I,a)}(M) \leq \operatorname{depth}_I(M) + 1$$

Proof. Taking an M-sequence of maximal length $\mathbf{a} \subset I$ and passing to $M/\mathbf{a}M$, one can upon changing notation, assume that $\operatorname{depth}_I(M) = 0$, in which situation the goal is to show that $\operatorname{depth}_{(I,a)}(M) \leq 1$. One can assume in addition that $(I, a) \not\subset \mathcal{Z}(M)$, otherwise $\operatorname{depth}_{(I,a)}(M) = 0$. Thus, $\operatorname{depth}_{(I,a)}(M) \geq 1$. By prime avoidance, one can pick a regular element on M of the form $a + b$, for suitable $b \in I$. Since $b \in I \subset \mathcal{Z}(M)$, one can safely replace $a + b$ by a. To conclude, it is enough to show that $I \subset \mathcal{Z}(M/aM)$ with the knowledge that $a \notin \mathcal{Z}(M)$. It is at this point that one uses the assumption that a

belongs to the Jacobson radical of R, the argument being the same as in the proof of Proposition 5.3.14. □

Example 5.3.18. If a lies outside the Jacobson radical, then easy examples show that $\operatorname{depth}_{(I,a)}(M)$ can jump arbitrarily. Thus, for any $n \geq 1$, if $R = k[X_1, \ldots, X_n, Y]$ is the polynomial ring over a field, $I = (1 - Y)(X_1, \ldots, X_n)$ and $a = Y$, then $(I, a) = (X_1, \ldots, X_n, Y)$, hence $\operatorname{depth} R_{(I,a)} = n + 1$.

If I itself is assumed to lie in the Jacobson radical, one has the following.

Proposition 5.3.19. *Let R be a Noetherian ring and let M stand for a finitely generated R-module. If $I = (a_1, \ldots, a_r) \subset R$ is an ideal contained in the Jacobson radical of R, then $\operatorname{depth}_I M = r$ if and only if $\{a_1, \ldots, a_r\}$ is an M-sequence.*

Proof. The "if" direction is obvious. Conversely, assume that $\operatorname{depth}_I M = r$. Induct on r. If $r = 0$, the result is trivially or vacuously true. Assuming $r \geq 1$, set $J := (a_1, \ldots, a_{r-1})$. By Proposition 5.3.17, $\operatorname{depth}_J M \geq \operatorname{depth}_I M - 1 = r - 1$. On the other hand, $\operatorname{depth}_J M \leq \operatorname{ht}(J + 0 : M/0 : M) \leq \operatorname{ht} J \leq r - 1$, where the rightmost inequality follows from Krull's prime ideal theorem (Theorem 2.5.27). Applying the inductive hypothesis to J, one finds that $\{a_1, \ldots, a_{r-1}\}$ is an M-sequence.

To conclude note that $I = (J, a_r)$, while $\operatorname{depth} IM = r$. Therefore, if a_r is a zero-divisor on M/JM then $I = (J, a_r) \subset \mathcal{Z}(M/JM)$, and hence the M-sequence $\{a_1, \ldots, a_{r-1}\}$ cannot be properly extended in I; this contradicts the assumption $\operatorname{depth}_I M = r$. □

Proposition 5.3.20 (Depth and exact sequences). *Let R be a Noetherian ring and let $0 \to N \to M \to K \to 0$ stand for an exact sequence of finitely generated R-modules. If $I \subset R$ is an ideal such that $IN \neq N$ and $IK \neq K$, then:*

(1) $\operatorname{depth}_I(M) > \operatorname{depth}_I(K) \Rightarrow \operatorname{depth}_I(N) = \operatorname{depth}_I(K) + 1$
(2) $\operatorname{depth}_I(M) < \operatorname{depth}_I(K) \Rightarrow \operatorname{depth}_I(N) = \operatorname{depth}_I(M)$
(3) $\operatorname{depth}_I(M) = \operatorname{depth}_I(K) \Rightarrow \operatorname{depth}_I(N) \geq \operatorname{depth}_I(M)$

Proof. With an eye for induction, one first deals with the following situations:

- $\operatorname{depth}_I(M) = 0$: here one is either in cases (2) or (3) of the statement. Thus, it is enough to argue that $\operatorname{depth}_I(K) > 0 \Rightarrow \operatorname{depth}_I(N) = 0$. In fact, since $I \subset \mathcal{Z}(M)$, one can pick $x \in M$ such that $Ix = \{0\}$. But then $\operatorname{depth}_I(K) > 0$ implies that $x \in N$. Thus, $I \subset \mathcal{Z}(N)$, and hence $\operatorname{depth}_I(N) = 0$, as claimed.
- $\operatorname{depth}_I(K) = 0$: here, one is either in cases (1) or (3) of the statement. It then suffices to show that $\operatorname{depth}_I(M) > 0 \Rightarrow \operatorname{depth}_I(N) = 1$. Evidently, $\operatorname{depth}_I(N) \geq 1$ as otherwise $\operatorname{depth}_I(K) > 0$. Let $a \in I \setminus \mathcal{Z}(M)$; in particular, $a \notin \mathcal{Z}(N)$. As $\operatorname{depth}_I(K) = 0$, there exists an $x \in M \setminus N$ such that $Ix \subset N$. In particular, $ax \in N$. However, $ax \notin aN$ since, by hypothesis, $a \notin \mathcal{Z}(M)$ and $x \notin N$. Thus, one has the element $ax \in N$ such that $Iax = aIx \subset aN$. This shows that ax is an N/aN-sequence of maximal length in I, hence $\operatorname{depth}_I(N/aN) = 0$. It follows that $\operatorname{depth}_I(N) = 1$, as was to be shown.

Now, assume that $\operatorname{depth}_I(K) > 0$ and $\operatorname{depth}_I(M) > 0$. Let $a \in I \setminus \mathcal{Z}(K)$. Then the sequence

$$0 \to N/aN \to M/aM \to K/aK \to 0$$

is again exact, as is well known: $\ker(N/aN \to M/aM) = (N \cap aM)/aN = \{0\}$ for $a \notin \mathcal{Z}(K)$. On the other hand, since $\operatorname{depth}_I(M) > 0$, one can readjust matters to pick $a \in I \setminus (\mathcal{Z}(M) \cup \mathcal{Z}(K))$, in which case the depth of every one of the modules in the residual exact sequence goes down exactly by 1. Thus, one can apply the inductive hypothesis. □

5.4 Cohen–Macaulay modules

The notion goes back to the problem considered by F. S. Macaulay ([106]) as how to characterize the so-called ideals of the principal class. Starting in 1950, it gradually took a central position in commutative ring theory as a natural generalization of the notion of a complete intersection. Its impact is in that it appears in multiple forms and disguises throughout, part of which will be taken up in this section.

The concept is essentially local in its inception.

Definition 5.4.1. Let $(R, \mathfrak{m})$ denote a local ring. A finitely generated R-module M is a *Cohen–Macaulay module* if $\operatorname{depth} M = \dim M$. If R is Noetherian, one says that M is Cohen–Macaulay if the localization $M_{\mathfrak{m}}$ is Cohen–Macaulay for every maximal ideal $\mathfrak{m} \in \operatorname{Spec} R$.

By convention, $\{0\}$ is a Cohen–Macaulay module.

A Noetherian ring R is a Cohen–Macaulay ring if it is so as an R-module.

Next are some basic properties of this notion.

Proposition 5.4.2. *Let $(R, \mathfrak{m})$ denote a Noetherian local ring and let M stand for a finitely generated R-module.*

(1) *If M is Cohen–Macaulay, then* $\operatorname{depth} M = \dim R/P$ *for every* $P \in \operatorname{Ass} M$. *In particular,* $\operatorname{Ass} M = \operatorname{Min}(M)$.

(2) *If M is Cohen–Macaulay, then every subset* $\mathbf{a} \subset \mathfrak{m}$ *of a system of parameters on M is an M-sequence and $M/\mathbf{a}M$ is Cohen–Macaulay.*

(3) *If R is a Cohen–Macaulay ring, then a syzygy module of M of sufficiently large order is Cohen–Macaulay and, in addition,* $\operatorname{depth} M = \dim R$.

Proof. (1) It follows immediately from Proposition 5.3.12.

(2) It follows from the equality $\operatorname{Ass} M = \operatorname{Min}(M)$, established in (1), and from Proposition 5.1.12.

(3) Let $0 \to Z \to R^m \to M \to 0$ stand for a finite free presentation of M. Set $\operatorname{depth}(M) = n$. If $n = \dim R$, M itself satisfies the statement. Otherwise, $\operatorname{depth}(R^m) =$

$\operatorname{depth}(R) = \dim R > n$, hence $\operatorname{depth}(Z) = n + 1$ by Proposition 5.3.20. Iterating this procedure, one eventually meets a desired module. □

The notion can be further stated in various other ways.

Theorem 5.4.3 (Cohen–Macaulay equivalences). *Let $(R, \mathfrak{m})$ denote a local ring and let M stand for a finitely generated R-module. The following conditions are equivalent:*
(i) *M is Cohen–Macaulay.*
(ii) $\operatorname{depth}_{\mathfrak{m}} M = \dim M_{\mathfrak{m}}$ *for every maximal ideal* $\mathfrak{m} \in \operatorname{supp} M$.
(iii) $\operatorname{depth}_I M = \operatorname{ht}(I/(0 : M))$ *for every ideal* $I \supset 0 : M$.
(iv) $\operatorname{depth}_P M = \dim M_P$ *for every prime ideal* $P \in \operatorname{supp} M$.
(v) *M_P is a Cohen–Macaulay R_P-module for every prime ideal* $P \in \operatorname{supp} M$.

Proof. (i) ⇒ (ii) If $\mathfrak{m} \in \operatorname{supp} M$ is a maximal ideal, then $\operatorname{depth}_{\mathfrak{m}}(M) = \operatorname{depth}_{\mathfrak{m}_{\mathfrak{m}}}(M_{\mathfrak{m}})$ by Proposition 5.3.9(ii)(b) as applied with $I = \mathfrak{m}$. The result follows immediately.

(ii) ⇒ (iii) This implication is the core of the theorem. Given an ideal $I \supset 0 : M$, fix a maximal ideal $\mathfrak{m} \supset I$ such that $\operatorname{depth}_I M = \operatorname{depth}_{I_{\mathfrak{m}}} M_{\mathfrak{m}}$ (Proposition 5.3.9(ii)(b)). One can reduce the implication to the case where the ground ring is the localization $R_{\mathfrak{m}}$, the module is $M_{\mathfrak{m}}$, and the given deal is $I_{\mathfrak{m}}$. Indeed, the hypothesis is preserved since $\operatorname{depth}_{\mathfrak{m}_{\mathfrak{m}}} M_{\mathfrak{m}} \geq \operatorname{depth}_{\mathfrak{m}} M = \dim M_{\mathfrak{m}}$, while the conclusion holds provided it holds in the local case since then

$$\operatorname{depth}_I M = \operatorname{depth}_{I_{\mathfrak{m}}} M_{\mathfrak{m}} = \operatorname{ht}\big(I_{\mathfrak{m}}/(0 : M_{\mathfrak{m}})\big) \geq \operatorname{ht}\big(I/(0 : M)\big)$$

and the inequality $\operatorname{depth}_I(M) \leq \operatorname{ht}(I/(0 : M))$ is always valid by Proposition 5.3.11. Refreshing the notation, $(R, \mathfrak{m})$ is now a local ring, M is Cohen–Macaulay and $0 : M \subset I \subset \mathfrak{m}$.

Proceeding by contradiction, assume that $I \supset 0 : M$ is an offender maximal possible relative to inclusion. In particular, $I \neq \mathfrak{m}$. Pick $a \in \mathfrak{m} \setminus P$, for every $P \in \operatorname{Min}(R/I)$. By Proposition 5.3.17, $\operatorname{depth}_{(I,a)} M \leq \operatorname{depth}_I M + 1$. One has

$$\begin{aligned} \operatorname{depth}_{(I,a)} M &\leq \operatorname{depth}_I M + 1 < \operatorname{ht}\big(I/(0 : M)\big) + 1 \\ &\leq \operatorname{ht}\big((I, a)/(0 : M)\big), \end{aligned}$$

hence $(I, a) \in \operatorname{supp} M$ is an offender properly containing I.

(iii) ⇒ (iv) This is clear as

$$\dim M_P = \dim R_P/0 :_{R_P} M_P = \dim R_P/(0 : M)_P = \operatorname{ht} P_P/(0 : M)_P = \operatorname{ht} P/0 : M.$$

(iv) ⇒ (v) By the localization properties of depth, $\operatorname{depth}_P M \leq \operatorname{depth}_{P_P} M_P$, hence $\operatorname{depth}_P(M) \leq \dim M_P = \operatorname{depth}_P M$ by assumption. Therefore, $\operatorname{depth}_{P_P} M_P = \dim M_P$, as required.

(v) ⇒ (i) Obvious. □

The next result, quite useful in an argument, is really implicit in the details of Theorem 5.4.3.

Corollary 5.4.4. *Let* $(R, \mathfrak{m})$ *denote a local ring and let* M *stand for a finitely generated* R*-module. If* M *is Cohen–Macaulay, then* $\operatorname{depth}_P M = \operatorname{depth}_{P_P} M_P$ *for every prime ideal* $P \in \operatorname{supp} M$.

Proof. By Theorem 5.4.3(v), M_P is Cohen–Macaulay as an R_P-module, hence

$$\begin{aligned}\operatorname{depth} M_P &= \dim M_P = \dim R_P/0 :_{R_P} M_P = \operatorname{ht} P_P/0 :_{R_P} M_P = \operatorname{ht} P/0 : M \\ &= \operatorname{depth}_P M,\end{aligned}$$

the last equality by Theorem 5.4.3(iii). □

5.4.1 Special properties of Cohen–Macaulay modules

One says that a finitely generated module M over a Noetherian ring R is *equicodimensional* (resp., has *pure dimension*) if $\dim M = \dim M_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m} \in \operatorname{supp} M$ (resp., $\dim M = \dim R/P$ for every $P \in \operatorname{Ass} M$.)

Proposition 5.4.5. *If* M *is a finitely generated equicodimensional Cohen–Macaulay module then* $\dim M = \dim M_P + \dim M/PM$ *for every* $P \in \operatorname{supp} M$.

Proof. The inequality $\dim M \geq \dim M_P + \dim M/PM$ holds regardless and is easily checked. Now, take a maximal ideal $\mathfrak{m}$ containing P and suppose that the statement holds for $M_{\mathfrak{m}}$ over the localization $R_{\mathfrak{m}}$. Then

$$\begin{aligned}\dim M = \dim M_{\mathfrak{m}} &= \dim M_{P_{\mathfrak{m}}} + \dim M_{\mathfrak{m}}/P_{\mathfrak{m}}M_{\mathfrak{m}} \\ &= \dim M_P + \dim(M/PM)_{\mathfrak{m}} \leq \dim M_P + \dim M/PM.\end{aligned}$$

Therefore, for the reverse inequality, one can assume that $(R, \mathfrak{m})$ local.

Let $\mathbf{a} = \{a_1, \ldots, a_r\} \subset P$ denote an M-sequence of maximal length. Since M is Cohen–Macaulay, $\dim M_P = \operatorname{depth}_{P_P} M_P = \operatorname{depth}_P M = r$. Now, P is contained in some associated prime of $M/\mathbf{a}M$ and, from the other end, it contains such a prime ideal. But, $M/\mathbf{a}M$ is Cohen–Macaulay as well by Proposition 5.4.2 (3), hence $P \in \operatorname{Ass} M/\mathbf{a}M$. It follows in addition that $P \in \operatorname{Min}(M/PM)$. Thus, $\dim M/PM \geq \dim R/P = \dim M/\mathbf{a}M = \dim M = \dim M - r$, which is the desired inequality. □

Corollary 5.4.6. *If* M *is a finitely generated equicodimensional Cohen–Macaulay module, then* $\dim S = \dim S_P + \dim S/P$ *for every* $P \in \operatorname{Spec} S$*, where* $S := R/0 : M$*. In particular, if a local ring* R *has a finitely generated faithful Cohen–Macaulay module, then* $\dim R = \dim R_P + \dim R/P$ *for every* $P \in \operatorname{Spec} R$.

Remark 5.4.7. Unfortunately, the hypothesis of the supplementary assertion above may be hard to meet. It is trivially satisfied if R is a (complete) local ring of dimension

≤ 2 because the integral closure of R is Cohen–Macaulay. The existence of Cohen–Macaulay modules of maximal dimension over non-Cohen–Macaulay rings is a tall order, presently, a largely sophisticated theory involving number theoretical concepts and the so-called *perfectoid theory*. At the other end, when the base ring is Noetherian, classifying all maximal Cohen–Macaulay modules is also an important issue.

Corollary 5.4.8. *If $I \subset R$ is an ideal of a Noetherian ring R such that R/I is Cohen–Macaulay and equicodimensional, then R/I has pure dimension.*

Proof. By the previous corollary, one has $\dim R/I = \dim R_P/I_P + \dim R/P$, for every $P \in \operatorname{Ass} R/I$. But since R/I is Cohen–Macaulay, the ideal I_P is P_P-primary, hence $\dim R_P/I_P = 0$. □

Proposition 5.4.9. *Let $(R, \mathfrak{m}) \xrightarrow{\varphi} (S, \mathfrak{n})$ denote a homomorphism of local rings through which S is a finitely generated module over R. If N is a finitely generated S-module, then*
(a) $\operatorname{depth}_{\mathfrak{n}} N = \operatorname{depth}_{\mathfrak{m}} N$.
(b) *N is Cohen–Macaulay S-module if and only if it is Cohen–Macaulay as an R-module.*

Proof. (a) The finiteness of φ implies that $\varphi(\mathfrak{m}) \subset \mathfrak{n}$, an easy consequence of the "lying over" property (Corollary 2.2.10).

Consider a maximal N-sequence $\mathbf{a} = \{a_1, \ldots, a_n\} \subset \mathfrak{m}$. Clearly, the sequence $\varphi(\mathbf{a}) := \{\varphi(a_1), \ldots, \varphi(a_n)\} \subset \mathfrak{n}$ is an N-sequence as an S-module. As $\mathfrak{m} \in \operatorname{Ass}_R N/\mathbf{a}N$, there is an R-module homomorphism $R \to N/\mathbf{a}N$ with kernel $\mathfrak{m}$. This map can be extended to an S-module homomorphism $S \to N/\varphi(\mathbf{a})N$ by mapping $1 \in S$ to a generator of the cyclic image of R.

Claim: the S-ideal $J := \ker(S \to N/\varphi(\mathbf{a})N)$ is $\mathfrak{n}$-primary.

Indeed, $\varphi(\mathfrak{m})S \subset J$, while $\varphi(\mathfrak{m})S$ is $\mathfrak{n}$-primary since $\dim \varphi(R) = \dim S$ in a injective integral extension. It follows from the claim that $\mathfrak{n} \in \operatorname{Ass}_S N/\varphi(\mathbf{a})N$, thus implying that $\varphi(\mathbf{a}) \subset \mathfrak{n}$ is a maximal sequence of N as S-module.

(b) By (a), it suffices to show the dimension of N is the same as an R-module or as an S-module. But this is clear since the map φ induces an injective ring homomorphism $\overline{\varphi} : R/0 :_R N \to S/0 :_S N$ under which $S/0 :_S N$ is finitely generated as $R/0 :_R N$-module. Therefore, one has an injective integral extension. □

5.4.2 Numerical invariants: Gorenstein rings

Throughout this part, assume that $(R, \mathfrak{m})$ is a Noetherian local ring. The following notion plays an important role.

Definition 5.4.10. Let N be a finitely generated R-module. The *socle* of N is the submodule $\mathfrak{s}(N) := 0 :_N \mathfrak{m} \subset N$.

Clearly, $\mathfrak{s}(N) \neq 0$ if and only if $\mathfrak{m}$ is an associated prime of N. Therefore, the typical use of the socle is when $N = M/\mathbf{a}M$, where M is a finitely generated Cohen–Macaulay R-module and $\mathbf{a} \subset \mathfrak{m}$ is a system of parameters of M. Then $\mathfrak{s}(M/\mathbf{a}M)$ has finite vector dimension over $k := R/\mathfrak{m}$.

The *type* of a Cohen–Macaulay module M is defined to be $\mathrm{t}(M) := \dim_k \mathfrak{s}(M/\mathbf{a}M)$. One observes that $\mathrm{t}(M)$ depends only M, not on a particular system of parameters, a property that follows from Proposition 6.2.76 later in this book, since $\mathrm{t}(M/\mathbf{a}M) = 0_{M/\mathbf{a}M}\mathfrak{m} = \mathrm{Hom}_R(R/\mathfrak{m}, M/\mathbf{a}M)$. By the same token, if M is a Cohen–Macaulay module, one has $\mathrm{t}(M) = \dim_{R/\mathfrak{m}} \mathrm{Ext}^n_R(R/\mathfrak{m}, M)$, where $n = \dim M$.

One can check that $\mathrm{t}(M)$ is invariant under reduction by an M-sequence and pull-back by a surjective ring homomorphism $R \twoheadrightarrow S$.

A Cohen–Macaulay Noetherian local ring R is said to be *Gorenstein* if $\mathrm{t}(R) = 1$. (According to H. Bass, Gorenstein rings are ubiquitous ([16]) in the sense that they appear in various multifaceted disguises in many different areas.)

Let $(S, \mathfrak{n})$ denote a regular local ring. If an ideal $J \subset S$ is such that S/J is a Gorenstein ring, then one says by abuse that J is a Gorenstein ideal. In this environment, a Gorenstein ideals of height ≤ 2 is generated by a regular sequence. Clearly, only $\mathrm{ht}\, J = 2$ is interesting, in which case the result is attributed to Serre, but the proof over a regular local ring is really easy by using a finite minimal free resolution of R/I, which has the shape

$$0 \to R^{n-1} \longrightarrow R^n \longrightarrow R \longrightarrow R/I \to 0,$$

where n denotes the minimal number of generators of I. Drawing on the homological methods of Section 6.2.2, one can see that the type of R/I is the rank of the left-most nonzero free module. Therefore, $n = 2$, which implies the assertion.

In a the same vein, Gorenstein ideals of height 3 also have a particular structure, but the proofs are much more involved. In height 3, the ideal is generated by the (maximal) Pfaffians of a skew–symmetric matrix by the work of Buchsbaum–Eisenbud ([30]). In height 4, there is no unique structure. One important class is given by the ideals of submaximal minors of square matrices, whenever they have maximal possible height (= 4) ([66]) (*cf.* Corollary 6.4.10). However, a complete classification of Gorenstein ideals of grade 4 is still not known.

Approaching the problem from the point of view of the dimension of R/I instead, one can state the cases of dimension 0 and 1 without any assumption on the ambient ring.

Proposition 5.4.11. *Let $(R, \mathfrak{m})$ be an Artinian local ring. The following conditions are equivalent:*

(i) *R is Gorenstein.*

(ii) *$0 : (0 : I) = I$ for every ideal $I \subset R$.*

(iii) *$\lambda(R) = \lambda(I) + \lambda(0 : I)$ for every ideal $I \subset R$.*

Proof. (i) ⇒ (ii) This is the main implication. The main steps of the argument will be given with appropriate references.

Claim 1 ([16, 2.8]). R is self-injective (*i. e.*, injective as R-module).

The proof was originally given by J. Dieudonné in terms of Frobenius algebras ([44]). Here, since $\dim_{R/\mathfrak{m}}(R/\mathfrak{m}, R) = 1$ one has an equality of injective hulls $E(R) = E(R/\mathfrak{m})$. Then Matlis duality forces $E(R) = R$.

Claim 2 ([25, Proposition 3.2.12, (c)]). For any ideal $I \subset R$, the natural R-homomorphism

$$R/I \to \mathrm{Hom}_R(\mathrm{Hom}_R(R/I, R), R)$$

is an isomorphism.

The proof is by induction on $\lambda(R/I)$, by applying $\mathrm{Hom}_R(\_, R)$ to a short exact sequence $0 \to L \to R/I \to K \to 0$, with $\lambda(L) < \lambda(R/I)$, using that $\mathrm{Ext}^1_R(\_, R) = 0$ since R is self-injective (Proposition 6.2.73).

Now, by the same token, applying $\mathrm{Hom}_R(\_, R)$ to $0 \to 0 : I \to R \to R/0 : I \to 0$ one gets a short exact sequence

$$0 \to \mathrm{Hom}_R(R/0 : I, R) \to \mathrm{Hom}_R(R, R) \simeq R \to \mathrm{Hom}_R(0 : I, R) \to 0. \tag{5.4.11.1}$$

Observe, moreover, that, for any ideal $I \subset R$, one has $\mathrm{Hom}_R(R/I, R) \simeq 0 : I$. In particular, $\mathrm{Hom}_R(R/0 : I, R) \simeq 0 : (0 : I)$, while, by Claim 2, one has the $R/I \simeq \mathrm{Hom}_R(0 : I, R)$. Substituting upon (5.4.11.1) yields the exact sequence

$$0 \to 0 : (0 : I) \to R \to R/I \to 0,$$

from which $I \simeq 0 : (0 : I)$, and since $I \subset 0 : (0 : I)$, they must be equal.

(ii) ⇒ (iii) Let $\{0\} = I_0 \subsetneq I_1 \subsetneq \cdots \subsetneq I_r = I$ be a composition series of I, where $\lambda(I) = r$. The assumption implies that the induced sequence

$$R = 0 : I_0 \supsetneq 0 : I_1 \supsetneq \cdots \supsetneq 0 : I_r = 0 : I$$

is a proper chain and admits no proper refinement. Therefore, the induced sequence

$$R/0 : I \supsetneq 0 : I_1/0 : I \supsetneq \cdots \supsetneq 0 : I_r/0 : I = \{0\}$$

is a composition series of $R/0 : I$. Therefore, $\lambda(I) = \lambda(R/0 : I)$. But since one has an exact sequence $0 \to 0 : I \to R \to R/0 : I \to 0$, the asserted equality follows immediately.

(iii) ⇒ (i) This is certainly the easiest: applying with $I = \mathfrak{m}$, one gets $\lambda(0 : \mathfrak{m}) = \lambda(R) - \lambda(\mathfrak{m}) = 1$. But $0 : \mathfrak{m}$ is the socle of R. □

Next is the case of one-dimensional Gorenstein local rings.

Proposition 5.4.12. *Let $(R, \mathfrak{m})$ be a Noetherian local ring of dimension 1. The following are equivalent:*

(i) *R is Gorenstein.*

(ii) *For every regular element $a \in \mathfrak{m}$ the socle of $R/(a)$ has dimension 1 over $R/\mathfrak{m}$.*

(iii) *The R-module $\mathfrak{m}^{-1} := R :_K \mathfrak{m}/R$ has length 1, where K is the total ring of quotients of R.*

Proof. (i) $\Leftrightarrow$ (ii). Since a regular element in $\mathfrak{m}$ forms a system of parameters in the 1-dimensional ring R, the equivalence follows immediately from the definition of the type.

(ii) $\Leftrightarrow$ (iii). It suffices to show that, for any regular element $a \in \mathfrak{m}$, there is an R-isomorphism $(a) :_R \mathfrak{m}/(a) \simeq \mathfrak{m}^{-1}/R$.

Define an R-map $\gamma : (a) :_R \mathfrak{m} \to \mathfrak{m}^{-1} := R :_K \mathfrak{m}$ by $b \mapsto a^{-1}b$.

Claim 1. γ is surjective.

Indeed, let $c \in K$ be such that $c\mathfrak{m} \subset R$. In particular, $ca = b \in R$ since $a \in \mathfrak{m}$. This gives $a^{-1}b = c$. But $b\mathfrak{m} = ca\mathfrak{m} = a(c\mathfrak{m}) \subset (a)$, hence $b \in (a) :_R \mathfrak{m}$.

Claim 2. The kernel of the composite map of γ and the residue map $\mathfrak{m}^{-1} \twoheadrightarrow \mathfrak{m}^{-1}/R$ is (a).

This is obvious as $a^{-1}b \in R$ yields $b \in (a)$. □

Example 5.4.13. What are the examples of Cohen–Macaulay rings?

(1) Any zero-dimensional Noetherian ring is Cohen–Macaulay, and any Noetherian domain of dimension one is Cohen–Macaulay.

(2) If A is a Cohen–Macaulay ring then $R := A[X_1, \dots, X_n]$ is Cohen–Macaulay, where $A[X_1, \dots, X_n]$ is a polynomial ring. In particular, if k is a field, $k[X_1, \dots, X_n]$ is Cohen–Macaulay (Macaulay's theorem).
The proof is a straightforward extension argument: one can assume that $n = 1$, say, $R = A[X]$, and in addition, by localizing R at a given prime $P \in \operatorname{Spec} R$ and A at the contraction $P \cap A$, one can assume that $(A, \mathfrak{m})$ is local and that $P \cap A = \mathfrak{m}$. Say, $d = \dim A$ and pick an A-sequence $\mathbf{a} \subset \mathfrak{m}$ of length d. It is easy to see that $\mathbf{a}$ is still an R-sequence, hence an R_P-sequence as well. Therefore, depth $R_P \geq d$. As known from Section 2.5.4, $P = \mathfrak{m}R$ or else $P = (\mathfrak{m}, f)$, for some monic $f \in R$ generating $P/\mathfrak{m}P \subset R/\mathfrak{m}[X]R \simeq (A/\mathfrak{m})[X]$ modulo $\mathfrak{m}$. In the first case, one has $\dim R_{\mathfrak{m}R} = \dim R$ since $\operatorname{ht} \mathfrak{m}R = \operatorname{ht} \mathfrak{m}$. Thus, this case is immediately disposed of. In the second case, f is a nonzero divisor on $R_P/\mathbf{a}R_P$, hence depth $R_P \geq d + 1 = \dim R \geq \dim R_P$.

(3) A *regular* local ring is Cohen–Macaulay.
This has not yet been introduced (Section 6.1) but can be defined as a local ring $(R, \mathfrak{m})$ such that $\mathfrak{m}$ can be generated by an R-sequence, hence is obviously Cohen–Macaulay.

(4) A particular, but important case, is when $(R, \mathfrak{m})$ is a Cohen–Macaulay local ring and $\mathbf{a} \subset \mathfrak{m}$ is an R-sequence. Then R is Gorenstein if and only if $R/(\mathbf{a})$ is Gorenstein.

In this case, $R/(\mathbf{a})$ is called a *local complete intersection*. Clearly, by definition, a regular local ring is Gorenstein, hence the residue of a regular local ring R by an R-sequence is a local complete intersection, the kind that is typically met in algebraic geometry.

(5) Determinantal rings.
Generic determinantal rings are Cohen–Macaulay, as are many of their specializations (see Section 6.4). More precisely:
- ([75]) Let $\mathcal{A}$ denote an $r \times s (r \leq s)$ generic matrix over a Cohen–Macaulay Noetherian ring. Then, for every $1 \leq t \leq r$, the ideal $I_t(\mathcal{A})$ is Cohen–Macaulay. Here, the codimension is $(r-t+1)(s-t+1)$ and this is the required codimension for a nongeneric matrix to have a Cohen–Macaulay ideal of t-minors. Actually, the generic ideals over $\mathbb{Z}$ are generically perfect (in the sense of [47], [76]).
- ([100]) Let $\mathcal{S}$ denote an $s \times s$ generic symmetric matrix over a Cohen–Macaulay Noetherian ring. Then, for every $1 \leq t \leq r$, the ideal $I_t(\mathcal{S})$ is Cohen–Macaulay. Here, the required codimension for Cohen–Macaulayness is $\binom{s-t+2}{2}$ (Theorem 6.4.7).
- ([39], [162], also [55]) Let $\mathcal{H}$ denote a generic Hankel matrix over a Cohen–Macaulay Noetherian ring. Then, for every t the ideal of minors $I_t(\mathcal{H})$ is Cohen–Macaulay.
  Here, by a well-known trick, it suffices to consider the case of maximal minors.

(6) At a more advanced level, the rings of invariants of the actions of certain groups on the polynomial ring $k[X_1, \ldots, X_n]$ (k a field) are Cohen–Macaulay in many important cases. This is the most classical disguise of a Cohen–Macaulay ring.

5.5 Historic note

5.5.1 Dimension

In the basic theory of ideals and modules the notion of dimension comes as a combinatorial concept, at least at a first level of ideas. Part of its inception was possibly inspired in the idea of dimension from other fields, such as algebraic geometry, but the idea in its full algebraic shape is due to W. Krull in the early twentieth century. It is of this period that came out the various forms of the principal ideal theorem, a basic pillar of dimension theory. A closer vicinity to local algebraic geometry is through the notion of a system of parameters, first introduced by C. Chevalley and subsequently used as a fundamental tool in the dimension theory of local rings.

5.5.2 Primary decomposition

The moral of this part is that to a Noetherian module one can associate a set of prime ideals to help understanding the structure of the module. To this set corresponds a

certain decomposition of the module into an intersection of simpler modules, called primary. This theory proved successful by E. Lasker and E. Noether in the case of an ideal was further developed by H. Cartan, S. Eilenberg and J. P. Serre in the 1950s. It turns out that the theory is more natural as applied to the category of modules. Historically, primary decomposition came first and only later the idea of defining the radicals of the primary components in an a priori way was fully recognized. As is the modern habit in most books, one starts by looking first at the associated primes of the module as an independent concept and then show that they are exactly the radicals of the primary components.

5.5.3 The depth behind the curtains

The story behind Theorem 5.3.5(ii) is fun. Although it is highly dangerous to attribute priority amidst the amount of homological results on ideals and modules at the footstep of Cartan–Eilenberg seminal book, it seems correct to say that the pole position was the English school of Northcott and Rees. Lemma 5.3.4 above is Lemma 1.1 of their paper [122]. As for the main part of Theorem 5.3.5(ii), these authors give an argument in the case where $(R, \mathfrak{m})$ is local and $M = R$. Their Theorem 1.3 is the discovery that for two R-sequences $\mathbf{a}, \mathbf{b}$ in I of the same length one has a module isomorphism $\mathrm{Hom}_R(R/I, R/(\mathbf{a})) \simeq \mathrm{Hom}_R(R/I, R/(\mathbf{b}))$—this is the essential fact behind the above second proof of Theorem 5.3.5(ii). Curiously, the authors miss the opportunity to immediately derive the equality of the respective lengths of two R-sequences of maximal length—this was made explicit in [169, Theorem 1, Appendix 6]. Of course, Northcott and Rees were fully aware of this result, perhaps avoided stressing it in [122] because Rees had about the same time engaged in proving it by using the Ext technique, essentially described in Proposition 6.2.76 (see [128, 129]). The argument of the first proof of Theorem 5.3.5(ii) given above follows the one of Kaplansky [93, Theorem 121]—interestingly enough, the latter quotes this proof as being taken from [122].

5.5.4 The KruCheSam theorem

About 10 years after the appearance of Krull's book "Idealtheorie" ([98]), Chevalley published a paper ([34]) where he introduced the notion of a system of parameters in a local ring. In the Appendix to this paper, he showed the inequality $s(R) \leq \dim R$ required for Theorem 5.1.11. His original argument is slightly different from the one above, perhaps more technical. A few years later ([133]) Samuel published his landmark paper on a local version of Hilbert's function, nowadays known as the Hilbert–Samuel function. He then showed that the Hilbert–Samuel function of a finitely generated module M is asymptotically a polynomial whose degree coincides with $\dim M$, pretty much as in the case of the original Hilbert function in the graded case. Since

then it is customary to call the Krull–Chevalley–Samuel theorem (historical order) the result that states the equality of the three numerical invariants involved as described.

5.6 Exercises

Exercise 5.6.1. Let $(R, \mathfrak{m})$ be a Cohen–Macaulay Noetherian local ring and $P \subset Q \subset R$ prime ideals.
(i) Prove that $\operatorname{ht}(Q/P) = 1$ implies $\operatorname{grade} Q = \operatorname{grade} P + 1$.
(ii) Prove that any saturated chain of prime ideals between P and Q has length $\operatorname{grade} Q - \operatorname{grade} P$.

Exercise 5.6.2. Let $R = k[x, y]$ (k a field) and $I = (x^2, xy)$. Show that R/I is not unmixed (in particular, not Cohen–Macaulay).

Exercise 5.6.3. Let $R = k[x, y, z]$ (k a field) and $I = (xy, xz)$. Show that $\operatorname{depth} R/I = 1$ (hence, R/I is not Cohen–Macaulay).

Exercise 5.6.4. Let $R = k[x_1, x_2, x_3, x_4]$ (k a field) and $I = (x_1x_3, x_1x_4, x_2x_3, x_2x_4)$. Show that R/I is unmixed, but not Cohen–Macaulay. Determine $\operatorname{depth} R/I$.

Exercise 5.6.5. Let $R = k[x_1, x_2, x_3, x_4]$ (k a field) and $P \subset R$ a prime ideal such that $R/P \simeq k[t^4, t^3u, u^3, u^4] \subset k[t, u]$. Compute $\operatorname{depth} R/P$ to decide whether R/P is Cohen–Macaulay.

Exercise 5.6.6. Let $P \subset R := k[x_{2,0,0}, x_{1,1,0}, x_{1,0,1}, x_{0,2,0}, x_{0,1,1}, x_{0,0,2}]$ (k a field) such that $R/P \simeq k[t^2, tu, tv, u^2, uv, v^2] \subset k[t, u, v]$, by $x_{i,j,l} \mapsto t^iu^jv^l$, $i + j + l = 2$.
(i) Show that P is generated by the 2×2 minors of a suitable symmetric matrix.
(ii) Give an explicit regular sequence in R_P that generates P_P.
(iii) Is R/P Cohen–Macaulay?

Exercise 5.6.7. Let R be a Cohen–Macaulay Noetherian ring and let x be an indeterminate over R. Prove that $R[x]$ is Cohen–Macaulay.

(Hint: localizing will reduce to the case of $(R, \mathfrak{m})$ local and $P \subset R[x]$ a prime ideal contracting to $\mathfrak{m}$; then use the relation between prime ideals, as well as regular sequences, in the extension $R \subset R[x]$.)

Exercise 5.6.8. Let $I = (y - x^2, z - x^3) \subset k[x, y, z]$. Show that the homogenization P of I in $k[x, y, z, w]$ is the defining ideal of the rational normal cubic in $\mathbb{P}^3_k$. (Hint: geometry tells you this, but the intention is a purely algebraic argument—for the latter, show that $I : (w)$ contains a quadric, thus writing a subideal $J \subset P$ generated by 3 quadrics; show that J is prime by localizing at the powers of a suitable nonzero-divisor modulo J.)

Exercise 5.6.9. Let $I \subset (x,y,z)^2$ be an ideal generated by a subset of the monomial generators of $(x,y,z)^2$ containing x^2, y^2, z^2. Show that R/I is a Gorenstein ring if and only if $I = (x^2, y^2, z^2)$.

Exercise 5.6.10. Prove the following best general analogue of Krull's intersection theorem: if R is a Noetherian ring and M is a finitely generated R-module then

$$\bigcap_{\mathfrak{m}} \left(\bigcap_{i \geq 0} \mathfrak{m}^i M \right) = \{0\},$$

where $\mathfrak{m}$ runs through the maximal ideals of R.

(Hint: if $u \neq 0$ belongs to the full intersection, consider its annihilator, which must be contained in some $\mathfrak{m}$.)

Exercise 5.6.11. Let R be a Noetherian of finite Krull dimension, let $\mathbf{a} = \{a_1, \ldots, a_n\} \subset R$ be an R-sequence and let $\mathbf{x} = x_1, \ldots, x_n$ be indeterminates over R.

(i) Show that $\dim R[x_2, \ldots, x_n]/(a_2 - a_1x_2, \ldots, a_n - a_1x_n) = \dim R$.

(ii) Deduce that $\dim R[x_1, \ldots, x_n]/(a_ix_j - a_jx_i)_{1 \leq i < j \leq n} = \dim R + 1$.

(iii) Assume that $(R, \mathfrak{m})$ is a regular local ring with infinite residue field and that $\mathbf{a}$ is a regular system of parameters. Prove that the localization at $(\mathfrak{m}, \mathbf{x})$ of the ring in item (ii) is Cohen–Macaulay by exhibiting a system of parameters of the right length.

Exercise 5.6.12. Consider the ideal $I \subset k[x_1, \ldots, x_6]$ generated by the following polynomials:

$$\begin{aligned} f_1 &= x_2x_4 + x_3x_6, \quad f_2 = x_3x_5 + x_1x_6, \quad f_3 = x_1x_2 - x_2x_5 + x_3x_5 - x_5x_6, \\ f_4 &= x_2x_3 + x_2x_4 + x_2x_6 + x_6^2 \quad f_5 = x_3^2 + x_3x_4 + x_3x_6 - x_4x_6, \\ f_6 &= x_1x_3 + x_1x_4 + x_4x_5 + x_1x_6. \end{aligned}$$

Prove that R/I is Cohen–Macaulay of dimension 3.

(Hint: prove that $\{x_1 - x_2, x_2 + x_4 + x_5, x_6\}$ is a regular sequence modulo I.)

6 Homological methods

While large sectors of commutative algebra have their origins in or are closely related to the geometry of algebraic varieties, there is one sector whose development was quite independent, and that is the homological tool. This has been organized and unified in the book of Cartan–Eilenberg, which became the state-of-the-art of the subject. The spectacular impact to commutative algebra followed suit in the work of M. Auslander, D. Buchsbaum, D. Northcott, D. Rees and J. P. Serre, to mention the first mentors.

6.1 Regular local rings

Although the terminology "regular local ring" has a deep entrenchment in the theory of smooth algebraic varieties and in homology in the 1950s, it is surprising how one can travel quite a bit in shallower waters to grasp its preliminaries. The purpose of the first part is to explore as much as possible the natural position of this concept amidst the basic notions of commutative ring theory.

6.1.1 Relation to basic invariants

For the sake of the present discussion, $(R, \mathfrak{m})$ is a Noetherian local ring. Recall that $\mu(I)$ denotes the minimal number of generators of an ideal $I \subset \mathfrak{m}$. One knows that $\operatorname{depth} R \leq \dim R \leq \mu(\mathfrak{m})$, where the rightmost inequality follows from Krull's prime ideal theorem.

The leftmost inequality being an equality means that R is Cohen–Macaulay. On the other hand, equality throughout means that $\mathfrak{m}$ can be generated by an R-sequence. Indeed, far more generally, one can show: let R be a Noetherian ring, M a finitely generated R-module and $I \subset R$ an ideal generated by n elements such that $IM \neq M$. If $\operatorname{depth}_I M = n$, then I can be generated by an M-sequence of length n. For the proof, one applies iteratively prime avoidance (Lemma 2.5.22). Say, $I = (a_1, \dots, a_n)$. Then one gets a set of generators in triangular shape as follows:

$$\begin{aligned} a_1 \ &+ \ \lambda_{1,2}a_2 + \cdots + \lambda_{1,n}a_n = a_1 + u_1 \\ a_2 \ &+ \ \lambda_{2,3}a_3 + \cdots + \lambda_{2,n}a_n = a_2 + u_2 \\ &\cdots \end{aligned}$$

forming an R-sequence, where $u_i \in I$ is picked such that $a_i + u_i$ does not belong to any associated prime of $M/(a_{i-1} + u_{i-1})M$, for $i = 1, \dots, n$.

It remains to analyze the impact of the equality $\dim R = \mu(\mathfrak{m})$.

Lemma 6.1.1. *Let $(R, \mathfrak{m})$ denote a local ring. If $\dim R = \mu(\mathfrak{m})$, then R is a domain.*

https://doi.org/10.1515/9783110616989-006

Proof. Induct on $\dim R$. If $\dim R = 0$, then R must be a field. If $\dim R \geq 1$, pick $a \in \mathfrak{m} \setminus \mathfrak{m}^2$.

Claim: $\mu(\mathfrak{m}/(a)) = \mu(\mathfrak{m}) - 1$.

Indeed, by Nakayama, with $k = R/\mathfrak{m}$, one has $\mu(\mathfrak{m}) = \dim_k \mathfrak{m}/\mathfrak{m}^2$ and $\mu(\mathfrak{m}/(a)) = \dim_k \mathfrak{m}/(\mathfrak{m}^2, a)$. One has an exact sequence of k-vector spaces

$$0 \to (\mathfrak{m}^2, a)/\mathfrak{m}^2 \longrightarrow \mathfrak{m}/\mathfrak{m}^2 \longrightarrow \mathfrak{m}/(\mathfrak{m}^2, a),$$

where $(\mathfrak{m}^2, a)/\mathfrak{m}^2 \simeq (a)/(a) \cap \mathfrak{m}^2$ is a one-dimensional vector space.

At the other end, one has $\dim R/(a) \geq \dim R - 1$ (Proposition 5.1.12(i)). Therefore, $\dim R/(a) \geq \mu(\mathfrak{m}/(a))$ and since $\dim R/(a) \leq \mu(\mathfrak{m}/(a))$ always holds, one gets the equality $\dim R/(a) = \mu(\mathfrak{m}/(a))$. By the inductive hypothesis, $R/(a)$ is a domain. In particular, (a) is a prime ideal of R. One claims that if R is not a domain then necessarily (a) is a minimal prime of R. In fact, let $P \subsetneq (a)$ denote a prime ideal. Any element of P has the form ab_1, with $b_1 \in P$ since $a \notin P$. Repeating ad nauseam, one gets that $P \subset \bigcap_{l \geq 0} (a)^l$. But the latter intersection is zero by Theorem 5.2.18. Then $\{0\}$ is a prime ideal, *i. e.*, R is a domain.

Thus, if R is not a domain every element $a \in \mathfrak{m} \setminus \mathfrak{m}^2$ generates a minimal prime of R. Since these are finitely many, one gets that $\mathfrak{m}$ is contained in the union of $\mathfrak{m}^2$ and the finitely many minimal primes of R. Therefore, $\mathfrak{m}$ is contained in one of these primes, which is a contradiction since $\dim R \geq 1$. □

Proposition 6.1.2. *Let $(R, \mathfrak{m})$ denote a local ring. If $\dim R = \mu(\mathfrak{m})$, then $\mathfrak{m}$ is generated by an R-sequence.*

Proof. As in the proof of the previous lemma, one inducts on $n := \dim R = \mu(\mathfrak{m})$. If $n = 0$, then R is a field and on can accept that the empty set is an R-sequence of length zero. If $n \geq 1$, pick $a \in \mathfrak{m} \setminus \mathfrak{m}^2$. By the previous lemma, R is a domain, hence a is a nonzero divisor on R. But, as in the proof of the lemma, $\dim R/(a) = \mu(\mathfrak{m}/(a))$. By the inductive hypothesis, $\mathfrak{m}/(a)$ is generated by an $R/(a)$-sequence $\{\overline{a_2}, \ldots, \overline{a_n}\}$. Clearly, then $\{a, a_2, \ldots, a_n\}$ is an R-sequence generating $\mathfrak{m}$. □

This motivates the following.

Definition 6.1.3. A local ring $(R, \mathfrak{m})$ is *regular* if, equivalently:
(1) $\dim R = \mu(\mathfrak{m})$.
(2) $\dim R = \dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$.
(3) $\mathfrak{m}$ is generated by an R-sequence.

An R-sequence generating the maximal ideal of a regular local ring is called a *regular system of parameters* of R.

Remark 6.1.4. A curious extension of Proposition 6.1.2 is due to E. Davis ([41, Remark, p. 203]): any prime ideal P in a Noetherian ring generated by $\operatorname{ht} P$ elements is generated

by an R-sequence. This is clearly false for arbitrary ideals, *e. g.*, let $I := (a)$, where a is a zero divisor not contained in the finitely many primes of R of height 0.

6.1.2 Properties

The class of regular local rings is fairly restricted. While for most other classes of rings it is fairly immediate to prove their preservation by localization, not so for regular local rings.

Some of the basic properties are as follows:

($\mathfrak{R}_1$) A regular local ring is a domain.
This is the content of Lemma 6.1.1.

($\mathfrak{R}_2$) A regular local ring is Cohen–Macaulay.
This is clear from the definition.

($\mathfrak{R}_3$) A regular local ring is normal.
To see this, the shortest is to use Serre's criterion of normality, encapsulated in the usual conditions (S_2) and (R_1). The first is automatic since R is Cohen–Macaulay, hence satisfies even (S_n) with $n = \dim R$. The second condition says that R is locally regular at primes of height one. Unfortunately, this is a harder piece and will be tackled a little later by homological methods.

($\mathfrak{R}_4$) (Chevalley) If $(R, \mathfrak{m})$ is regular and $I \subset \mathfrak{m}$ is an ideal, then $(R/I, \mathfrak{m}/I)$ is regular if and only if I is generated by a subset of a regular system of parameters of R.
The "if" implication is immediate. Conversely, by $(\mathfrak{R}_1)$ the ideal I is prime. Say, $\operatorname{ht} I = d$. Then $\dim R/I = n - d$ by $(\mathfrak{R}_2)$ and Proposition 5.4.5. By hypothesis, $\mathfrak{m}/I$ is generated by an R/I-sequence, say, $\{\overline{a_{d+1}}, \dots, \overline{a_n}\}$. Lift the respective preimages and complete to a full set $\{a_1, \dots, a_d, a_{d+1}, \dots, a_n\}$ of minimal generators of $\mathfrak{m}$, where $\{a_1, \dots, a_d\} \subset I$. By Proposition 6.1.2, this set of generators is an R-sequence; in particular, $\{a_1, \dots, a_d\}$ is a subset of a regular system of parameters, hence $P := (a_1, \dots, a_d)$ is a prime ideal by the "if" assertion and $(\mathfrak{R}_1)$. Since $P \subset I$, one must have $I = P$, hence I is generated by a subset of a regular system of parameters.

($\mathfrak{R}_5$) Let A denote a Noetherian ring and let $R := A[X_1, \dots, X_m]$ stand for a polynomial ring over it. If every prime localization of A is regular, then so is every prime localization of R.
The proof is basically the same as that of Example 5.4.13 (2) with the obvious adaptation.

Remark 6.1.5. In particular, if k is a field, every prime localization of $k[X_1, \dots, X_m]$ is regular. This result is sometimes referred to as Hilbert theorem, but of course what Hilbert actually proved was the celebrated syzygy theorem for homogeneous ideals of $k[X_1, \dots, X_m]$ ([72, Theorem III]). The precise relation between the two results will be made clear in subsequent sections.

It should be noted that, from the early half of the last century, the theory of regular local rings acquired a strong homological contour, culminating with Serre's theorem to be considered in the subsequent parts. The required homological tool will be developed in the next section.

6.2 The homological tool for Noetherian rings

The purpose of this section is to develop enough of the basic material needed for the homological approach to regular local rings. Fatally, by so doing one is led to introducing sufficiently many details to make the section self-contained. The theme has been treated in many excellent sources, starting with the celebrated book by H. Cartan and S. Eilenberg. By going through the section, the reader will recognize the original work of the classical sources, and made explicit as much as possible.

6.2.1 Projective modules

The basic notion is encapsulated in the following conditions.

Proposition 6.2.1. *Let R denote a ring and let M stand for an R-module. The following conditions are equivalent:*

(i) (Lifting) *Given R-modules N, L, a homorphism $\varphi : M \to L$ and a surjective homomorphism $\psi : N \twoheadrightarrow L$, there is a homomorphism $\chi : M \to N$ such that $\varphi = \psi \circ \chi$; in other words, for any surjective homomorphism $\psi : N \twoheadrightarrow L$ the induced homomorphism $\mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(M,L)$ is also surjective.*

(ii) (Splitting) *Every surjective homomorphism $\varphi : N \twoheadrightarrow M$ splits, i. e., there exists a homomorphism backwards $\psi : M \to N$ such that the composite $\Phi \circ \psi$ is the identity map of M.*

(iii) (Direct summand) *M is a direct summand of a free R-module.*

Proof. (i) $\Rightarrow$ (ii) Apply (i) with $L = M$ and φ the identity map.

(ii) $\Rightarrow$ (iii) By selecting a set o generators of M, there is a surjective map $F \to M$, with F free. The assumed splitting map makes M into a direct summand of F.

(iii) $\Rightarrow$ (i) Write $F = M \oplus M'$, with F free. Add M' as a direct summand to all modules in sight and set

$$\widetilde{\varphi} := (\varphi, 1_{M'}) : F = M \oplus M' \to L \oplus M', \quad \widetilde{\psi} := (\psi, 1_{M'}) : N \oplus M' \to L \oplus M',$$

where $1_{M'}$ denotes the identity map of M'.

Suppose for a minute that (i) holds when M is a free module. Then, applying to $F = F = M \oplus M'$ one gets a homomorphism $\widetilde{\chi} : F \to N \oplus M'$ such that $\widetilde{\varphi} = \widetilde{\psi} \circ \widetilde{\chi}$. Set $\chi : M \to N \oplus M'$ for the restriction of $\widetilde{\chi}$ to M, where an element $x \in M$ is identified

with $(x,0) \in F$. Say, $\chi(x) = \widetilde{\chi}(x,0) = (y,y') \in N \oplus M'$. Then $(\psi(y),y')\widetilde{\psi}(\chi(x)) = \widetilde{\varphi}(x,0) = (\varphi(x),0)$, from which one gets $y' = 0$, hence $\chi(x) = y \in N$, and $\psi(y) = \varphi(x)$. This proves (i) for M, with χ as chosen.

Finally, to see that the statement of (i) holds when M is a free module, take a free basis $\{x_\alpha\}$ of M and for every α lift $\varphi(x_\alpha)$ to a preimage $y_\alpha \in N$. Then define $\chi : x_\alpha \mapsto y_\alpha$. □

Definition 6.2.2. A module satisfying the equivalent conditions of Proposition 6.2.1 is called *projective*.

For quite some time in this section, one denotes a projective module by the letter P, thus momentarily leaving the habit by which P denotes a prime ideal.

The first question is whether any ring admits projective modules which are not free. The answer is easily answered in the negative if one restricts the question to the consideration of finitely generated modules. Thus, *e. g.*, over a PID every finitely generated projective module is free. In arbitrary dimension, one can file the following basic result.

Proposition 6.2.3. *Let $(R,\mathfrak{m})$ be a local ring. Then every finitely generated projective module P is free.*

Proof. Let $\mu(P) = n$. Map a free R-module F of rank n onto P. By Proposition 6.2.1(ii), one has a direct sum decomposition $F \simeq Z \oplus P$, where Z denotes the kernel of the map $F \twoheadrightarrow P$. Tensoring with $k := R/\mathfrak{m}$ yields an isomorphism $F/\mathfrak{m}F \simeq Z/\mathfrak{m}Z \oplus P/\mathfrak{m}P$ of vector spaces over k. By Nakayama, $\dim_k P/\mathfrak{m}P = n = \dim_k F/\mathfrak{m}F$. Therefore, $Z/\mathfrak{m}Z = 0$, and hence, again by Nakayama, $Z = 0$. □

By a result of Kaplansky ([92]), over a quasilocal ring every projective module is free—here, *quasilocal ring* means one having a unique maximal ideal, but not necessarily Noetherian. The proof depends on two results of independent interest: the first is particular to projective modules over quasilocal rings and the second is a piece of universal algebra. Although no use of this generalization is foreseen in this book, for the reader's convenience here are the corresponding statements.

Proposition 6.2.4. *If P is a projective module over a quasilocal ring, then every element of P is contained in some free direct summand of P.*

Proposition 6.2.5. *Let M be a module over an arbitrary ring. If M is an arbitrary direct sum of countably generated submodules, then any direct summand of M is likewise a direct sum of countably generated submodules.*

It may be observed that the proof of Proposition 6.2.4 is overall finitistic, while that of Proposition 6.2.5 requires an inductive argument involving ordinal numbers.

For finitely generated modules over Noetherian rings, one has the following useful characterization.

Corollary 6.2.6. *Let R denote a Noetherian ring and let M stand for a finitely generated R-module. Then M is projective if and only if $M_{\wp}$ is $R_{\wp}$-free for every $\wp \in \operatorname{Spec} R$.*

Proof. The "only if" direction follows from Proposition 6.2.3 (and holds true without any hypothesis on either R or M, by the previous contents).

Alas, simple as it sounds, the converse statement has no known proof that does not essentially use some functorial argument. The result is a consequence of the more general statement that a short exact sequence $0 \to L \longrightarrow N \longrightarrow M \to 0$ of finitely generated modules over a Noetherian ring R splits if and only if it splits locally everywhere. One applies the functor $\operatorname{Hom}_R(M, \_)$ to this sequence yielding a left exact sequence

$$0 \to \operatorname{Hom}_R(M, L) \longrightarrow \operatorname{Hom}_R(M, N) \longrightarrow \operatorname{Hom}_R(M, M).$$

By assumption, the last sequence splits locally everywhere since $\operatorname{Hom}(,)$ commutes with localizations under the present finiteness hypotheses; in particular, the rightmost map $\operatorname{Hom}_R(M, N) \longrightarrow \operatorname{Hom}_R(M, M)$ is locally surjective everywhere, hence surjective because the cokernel vanishes locally everywhere (hence is zero). Now, any element of $\operatorname{Hom}_R(M, N)$ in the preimage of the identity map of M is a splitting map for the original exact sequence. □

Remark 6.2.7.

(a) In the previous corollary, one can replace "locally free everywhere" by "locally free at every maximal ideal." In fact, the only required checking in the above argument is that a module is zero if it is so in every localization at a maximal ideal.

(b) A similar argument to the one above appears in [15, Lemma 1.9]. There one uses the characterization of $\operatorname{Ext}^1(M, L)$ as being the set of classes of the extensions of M by L. Then the given exact sequence splits if and only if its corresponding element in $\operatorname{Ext}^1(M, L)$ is zero. But, under the present finiteness conditions, one has $\operatorname{Ext}^1(M, L)_{\wp} = \operatorname{Ext}^1_{R_{\wp}}(M_{\wp}, L_{\wp})$ for any $\wp \in \operatorname{Spec} R$. Thus, one is bound to prove that an element of an R-module is zero if it is zero in all localizations of the module. This is the same argument as for a module.

6.2.2 Homological dimension

6.2.2.1 Projective resolutions

This part is the technical core of the section. It is possible to introduce the material in abstract (general nonsensical manner) by appealing to category theory, as is carried in many textbooks in homological algebra. Here, one brings up the material in the exact required proportion for the homological commutative setup.

One has met before free presentations of modules. One similarly speaks of a *projective presentation* of an R-module M as a short exact sequence $0 \to Z \longrightarrow P \longrightarrow M \to 0$, with P projective. By iteration, one finds the following basic notion.

Definition 6.2.8. A *projective resolution* of a module M is a long (possibly countably infinite) exact sequence

$$\cdots \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow M \to 0,$$

where P_i is projective for every $i = 0, 1, \ldots$.

The resolution is said to be *finite* if at some finite step the kernel is projective, *i. e.*, if one has an exact sequence

$$0 \to P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow M \to 0.$$

If this is the case, n is called the length of the resolution.

The *homological dimension* (or *projective dimension*) of the R-module M is the length of a projective resolution of finite length of minimal possible length; if no such resolution of finite length exists, one say that M has infinite homological dimension.

One denotes the homological dimension of M by $\mathrm{hd}_R M$.

Obviously, $\mathrm{hd}_R M = 0$ if and only if P is projective.

If the modules P_i turn in fact to be free one talks about a *free resolution*.

Clearly, every module admits a free resolution by starting with some set of generators of M and iterating the procedure of getting a free presentation. So why bother introducing projective resolutions? Part of the justification comes from the following result.

Proposition 6.2.9. *Let* $0 \to Z \longrightarrow P \xrightarrow{\varphi} M \to 0$, $0 \to Z' \longrightarrow P' \xrightarrow{\varphi'} M' \to 0$ *denote module projective presentations. If* $M \simeq M'$, *then there is an isomorphism* $Z \oplus P' \simeq Z' \oplus P$.

Proof. By composing φ with an isomorphism $\iota : M \simeq M'$, one can assume that $M = M'$.

Consider the "coincidence" submodule

$$C := \{(p, p') \in P \oplus P' \mid \varphi(p) = \varphi'(p')\}$$

and the restrictions $\pi : C \to P$ and $\pi' : C \to P'$ of the respective coordinate projections $P \oplus P' \twoheadrightarrow P$ and $P \oplus P' \twoheadrightarrow P'$. Since φ' surjects onto M then π surjects onto P and, by a symmetrical argument, π' surjects onto P'.

A straightforward calculation shows that $\ker \pi = \{(0, p') \mid \varphi'(p') = 0\} \simeq \ker \varphi' = Z'$, thus yielding a short exact sequence $0 \to Z' \longrightarrow C \longrightarrow P \to 0$. By a symmetrical argument, one gets a short exact sequence $0 \to Z \longrightarrow C \longrightarrow P' \to 0$. But since P, P' are projective, the two sequences split. □

The proposition is often called *Schanuel's lemma*, ever since it has so been dubbed by Kaplansky, honoring the intervention of Stephen Schanuel in one of his Chicago

lectures. The result itself has been known to others (see [58]), but the above beautiful proof is the original one based on Shanuel's intervention.

One now derives the following extension for truncated projective resolutions.

Proposition 6.2.10 (Long Schanuel's lemma). *Let*

$$0 \to Z_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \xrightarrow{\varphi} M \to 0$$

and

$$0 \to Z'_n \longrightarrow P'_{n-1} \longrightarrow \cdots \longrightarrow P'_0 \xrightarrow{\varphi'} M' \to 0$$

denote two long (exact) module presentations. If $M \simeq M'$, then there is an isomorphism

$$Z_n \oplus P'_{n-1} \oplus P_{n-2} \oplus \cdots \simeq Z'_n \oplus P_{n-1} \oplus P'_{n-2} \oplus \cdots.$$

In particular, Z_n is projective if and only if Z'_n is projective.

Proof. One inducts on n. For $n = 1$, it is Proposition 6.2.9. Thus, assume $n \geq 2$.

Setting $Z_1 := \ker \varphi_0$ and $Z'_1 := \ker \varphi'_0$, one gets the following pair of truncated resolutions:

$$0 \to Z_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \xrightarrow{\varphi_1} Z_1 \to 0$$

and

$$0 \to Z'_n \longrightarrow P'_{n-1} \longrightarrow \cdots \longrightarrow P'_1 \xrightarrow{\varphi'_1} Z'_1 \to 0.$$

From these, one gets the following pair of truncated resolutions:

$$0 \to Z_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \oplus P'_0 \xrightarrow{(\varphi_1, 1_{P'_0})} Z_1 \oplus P'_0$$

and

$$0 \to Z'_n \longrightarrow P'_{n-1} \longrightarrow \cdots \longrightarrow P'_1 \oplus P_0 \xrightarrow{(\varphi_1, 1_{P_0})} Z'_1 \oplus P_0.$$

By Proposition 6.2.9, one has $Z_1 \oplus P'_0 \simeq Z'_1 \oplus P_0$. Therefore, the result follows from the inductive hypothesis as applied to the last pair of truncated resolutions of $Z_1 \oplus P'_0$ and $Z'_1 \oplus P_0$. □

Remark 6.2.11. A neat consequence of the above is the following observation: if M has finite homological dimension, say, $\mathrm{hd}_R M = n$, then *any* projective resolution of M affords by truncation a finite projective resolution of length n. This is where one sees for the first time the advantage of considering homological dimension by means of projective resolutions instead of free resolutions. Indeed, for finite free resolutions the Schanuel lemma would only allow to conclude that the truncation is a *stably free module*, in the sense that it is a direct summand of a free module with free complement. Now, rings satisfying the property that their stably free modules are in fact free have been studied, but final classification is so far unheard of.

The following elementary result is recurrently used in many passages.

Proposition 6.2.12. *Let M denote an R-module and let*

$$\cdots \to P_n \longrightarrow \cdots \longrightarrow P_0 \xrightarrow{\varphi} M \to 0 \quad \text{and} \quad \cdots \to P'_n \longrightarrow \cdots \longrightarrow P'_0 \xrightarrow{\varphi'} M \to 0$$

denote two projective resolutions of M. Then there are homomorphisms $P_i \to P'_i$, for every $i \geq 0$, such that the following diagram is commutative:

$$\begin{array}{ccccccccc} \cdots & \to & P_n & \longrightarrow & \cdots & \xrightarrow{\varphi_1} & P_0 & \xrightarrow{\varphi} & M & \to & 0 \\ & & \downarrow & & & & \downarrow & & \| & & \\ \cdots & \to & P'_n & \longrightarrow & \cdots & \xrightarrow{\varphi'_1} & P'_0 & \xrightarrow{\varphi'} & M & \to & 0 \end{array} \tag{6.2.12.1}$$

Proof. For the first map $P_0 \to P'_0$, one uses Proposition 6.2.1(i): since φ is surjective its composite with the identity of M can be lifted to such a map and then the resulting square diagram is commutative. Next, compose φ_1 and the map $P_0 \to P'_0$. Clearly, this composite maps P_1 to $\ker(\varphi') = \mathrm{Im}(\varphi'_1)$, so it lifts to a map $P_1 \to P'_1$. By construction, the diagram obtained so far is commutative. A formal induction completes the argument. □

Remark 6.2.13. The collection of maps $P_i \to P'_i$, for $i \geq 0$, is an example of a chain map to be studied in Section 6.2.3. One says informally that, as such, this chain map is a *lifting* of the identity map of M. By the same token, there are maps $P'_i \to P_i$ making the similar diagram commutative. The obvious question is whether the two chain maps are totally unrelated. The answer is that in fact they are closely connected by means of *homotopy*, but this will have to wait until Section 6.2.3. The importance is to show that certain properties of a module M defined in terms of a chosen projective resolution are in fact independent of the choice.

6.2.2.2 Homological dimension along short exact sequences

Lemma 6.2.14. *Over any ring R if two of the three modules in a short exact sequence $0 \to N \longrightarrow M \longrightarrow K \to 0$ have finite homological dimension, then so does the third module. In particular, in a projective presentation $0 \to Z \longrightarrow P \longrightarrow M \to 0$ of a module M, one has $\mathrm{hd}_R M < \infty$ if and only if $\mathrm{hd}_R Z < \infty$.*

Proof. Let $0 \to Z' \longrightarrow P' \xrightarrow{\varphi'} N \to 0$ and $0 \to Z'' \longrightarrow P'' \xrightarrow{\varphi''} K \to 0$ stand for projective presentations of N and K, respectively. Let $P' \oplus P'' \twoheadrightarrow K$ denote the composite of the coordinate projection $P' \oplus P'' \twoheadrightarrow P''$ and $\varphi'' : P'' \twoheadrightarrow K$. Since $P' \oplus P''$ is projective, there is a lifting map $P' \oplus P'' \xrightarrow{\varphi} M$ whose composite with φ'' is $P' \oplus P'' \twoheadrightarrow K$. Clearly, φ surjects onto M, too. Let $Z := \ker \varphi$. This provides a projective presentation $0 \to Z \longrightarrow P' \oplus P'' \xrightarrow{\varphi} M \to 0$.

Identifying Z' with a submodule of $P' \oplus P''$ via $Z' \hookrightarrow P' = P' \oplus \{0\} \subset P' \oplus P''$, it follows that φ maps Z' to zero, hence there is a map $Z' \to Z$ which is clearly injective by construction. By a similar token, there is a surjective map $Z \twoheadrightarrow Z''$. Assembling the information, one gets a commutative diagram with exact rows and columns as follows:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & Z' & \longrightarrow & Z & \longrightarrow & Z'' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & P' & \longrightarrow & P' \oplus P'' & \longrightarrow & P'' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & N & \longrightarrow & M & \longrightarrow & K & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array} \tag{6.2.14.1}$$

By iterating, one finds a similar diagram of "simultaneous" projective resolutions of N, M and K. By using Remark 6.2.11, it follows that if two among N, M, K have finite homological dimension then so does the third module. □

The precise intertwining of the three homological dimensions by looking at the above diagram of simultaneous projective resolutions does not come out immediately. For that, one has to work harder. A first precision is obtained in the following.

Corollary 6.2.15. *Given a projective presentation* $0 \to Z \longrightarrow P \longrightarrow M \to 0$, *where* $0 < \mathrm{hd}_R M < \infty$, *then* $\mathrm{hd}_R M = \mathrm{hd}_R Z + 1$.

Proof. By Lemma 6.2.14, $\mathrm{hd}_R Z < \infty$. Let

$$0 \to P_n \longrightarrow \cdots \longrightarrow P_0 \longrightarrow Z \to 0$$

stand for a projective resolution of Z with $n = \mathrm{hd}_R Z$. Then, letting $P_0 \longrightarrow P$ denote the composite of the map $P_0 \longrightarrow Z$ and the injection $Z \hookrightarrow P$, one gets a projective resolution of M

$$0 \to P_n \longrightarrow \cdots \longrightarrow P_0 \longrightarrow P \longrightarrow M \to 0, \tag{6.2.15.1}$$

which tells that $\mathrm{hd}_R M \leq n+1$. But (6.2.15.1) can be truncated to a projective resolution of M of length $\mathrm{hd}_R M$ (see Remark 6.2.11). Therefore, $\mathrm{hd}_R M = n + 1$; otherwise, one would get $\mathrm{hd}_R Z < n$, which is a contradiction. □

Proposition 6.2.16. *Let* $0 \to N \longrightarrow M \longrightarrow K \to 0$ *stand for an exact sequence of R-modules over a ring R, such that two of the modules have finite homological dimension. Then one of the following takes place:*

(1) *If* $\mathrm{hd}_R M < \mathrm{hd}_R N$, *then* $\mathrm{hd}_R K = \mathrm{hd}_R N + 1$.
(2) *If* $\mathrm{hd}_R M > \mathrm{hd}_R N$, *then* $\mathrm{hd}_R K = \mathrm{hd}_R M$.
(3) *If* $\mathrm{hd}_R M = \mathrm{hd}_R N$, *then* $\mathrm{hd}_R K \leq \mathrm{hd}_R M + 1$ (*"indetermination"*).

Proof. (1) By Lemma 6.2.14, one can assume that all three modules have finite homological dimension.

First, assume that M is projective. Then K is not projective under the standing hypothesis that $\mathrm{hd}_R M < \mathrm{hd}_R N$. In this case, the statement has been proved in Corollary 6.2.15.

Thus, assume that M is not projective. One inducts on the sum $\mathrm{hd}_R N + \mathrm{hd}_R M + \mathrm{hd}_R K$, the initial step being subsumed in the case where M is projective, already taken care of.

One considers two cases:

(a) K is not projective.
Then $\mathrm{hd}_R Z'' = \mathrm{hd}_R K - 1 < \mathrm{hd}_R K$ again by Corollary 6.2.15. Therefore, $\mathrm{hd}_R Z' + \mathrm{hd}_R Z + \mathrm{hd}_R Z'' < \mathrm{hd}_R N + \mathrm{hd}_R M + \mathrm{hd}_R K$, hence the inductive hypothesis is applicable provided one shows that the exact sequence $0 \to Z' \longrightarrow Z \longrightarrow Z'' \to 0$ satisfies the hypothesis of (1), too. For this, one has $\mathrm{hd}_R Z = \mathrm{hd}_R M - 1$ by an encore of Corollary 6.2.15, by noting that Z is not projective since M is not projective. By a similar token, $\mathrm{hd}_R Z' = \mathrm{hd}_R N - 1$ since Z' is not projective as nor is N. Since $\mathrm{hd}_R M < \mathrm{hd}_R N$, then $\mathrm{hd}_R Z < \mathrm{hd}_R Z'$, as required. Applying the inductive step, one gets

$$\mathrm{hd}_R K = \mathrm{hd}_R Z'' + 1 = \mathrm{hd}_R Z' + 2 = \mathrm{hd}_R N - 1 + 2 = \mathrm{hd}_R N + 1,$$

as was to be shown.

(b) K is projective.
This a virtual possibility. Indeed, in this case, since M is not projective then $\mathrm{hd}_R M < \mathrm{hd}_R N$ implies by a similar token as above that $\mathrm{hd}_R Z < \mathrm{hd}_R Z'$. Therefore, applying the inductive hypothesis yields $\mathrm{hd}_R Z'' = \mathrm{hd}_R Z' + 1$ which is nonsense as K projective implies Z'' projective.

(2) Since $\mathrm{hd}_R M > \mathrm{hd}_R N$, then M is not projective. Thus, by Corollary 6.2.15 $\mathrm{hd}_R M = \mathrm{hd}_R Z + 1$.

Suppose first that N is not projective either, so similarly $\mathrm{hd}_R N = \mathrm{hd}_R Z' + 1$. In this case, one has $\mathrm{hd}_R Z > \mathrm{hd}_R Z'$ and one can apply the inductive assumption on $\mathrm{hd}_R N + \mathrm{hd}_R M + \mathrm{hd}_R K$ to conclude that $\mathrm{hd}_R Z'' = \mathrm{hd}_R Z$. On the other hand, K is not projective. Indeed, otherwise one would get $M \simeq N \oplus P$, where $P \simeq K$. In this case, any projective resolution of N yields one for M by simply adding P as a direct summand to all terms of the resolution. This would say that $\mathrm{hd}_R M \leq \mathrm{hd}_R N$, contradicting the main assumption of the item. Therefore, once more by Corollary 6.2.15, $\mathrm{hd}_R K = \mathrm{hd}_R Z'' + 1$; assembling yields $\mathrm{hd}_R K = \mathrm{hd}_R Z + 1 = \mathrm{hd}_R M$, as required.

Next, suppose that N is projective. Then Z' is projective and one has two alternatives. If Z is not projective, one can apply the inductive hypothesis to deduce that $\mathrm{hd}_R Z'' = \mathrm{hd}_R Z$. Now, K is not projective as otherwise M would be projective, contradicting $\mathrm{hd}_R M > 0$. Then, as before $\mathrm{hd}_R K = \mathrm{hd}_R Z'' + 1$. Therefore, $\mathrm{hd}_R K = \mathrm{hd}_R M$, as required.

It remains to analyze the case where, besides N and Z', also Z is projective. In this case, since $\mathrm{hd}_R M > 0$, then $\mathrm{hd}_R M = 1$. Since now $\mathrm{hd}_R K = \mathrm{hd}_R Z'' + 1 \leq 1 + 1 = 2$ and also $\mathrm{hd}_R K > 0$, one must show that $\mathrm{hd}_R K \leq 1$ is the case. This is left to the reader.

(3) A similar discussion takes care of this case as well. □

6.2.2.3 Homological behavior over local rings

The most distinguished basic feature of projective resolutions over a Noetherian local ring $(R, \mathfrak{m})$ is the notion of a *minimal free presentation* of a finitely generated R-module M, defined to be a free presentation $0 \to Z \longrightarrow F \longrightarrow M \to 0$ such that $Z \subset \mathfrak{m}F$. Letting $\mu(M)$ denote the cardinality of one (hence, all) minimal set of generators of M, such a presentation is obtained by mapping a free basis of a free R-module F of rank $\mu(M)$ to this set of generators, an easy reading of Nakayama's lemma.

Iterating, one has the notion of a (not necessarily finite) minimal free resolution of a finitely generated R-module M. By Remark 6.2.11, if $\mathrm{hd}_R M = n < \infty$ then any free resolution of M of length n is minimal, and conversely, any minimal free resolution of M has length n.

In this part, one proves a couple of results about as how the homological dimension of a finitely generated module over a local ring $(R, \mathfrak{m})$ behaves under the residue map $R \to R/(a)$, where $a \in \mathfrak{m}$ is a regular element.

Lemma 6.2.17. *Let $(R, \mathfrak{m})$ denote a local ring and let M stand for a finitely generated R-module. If $a \in \mathfrak{m}$ is a regular element on M such that M/aM is $R/(a)$-free, then M is free.*

Proof. Consider a minimal free presentation $0 \to Z \longrightarrow F \longrightarrow M \to 0$, *i. e.*, F is a free module with a basis mapping onto a set of minimal generators of M, so that $Z \subset \mathfrak{m}F$. Tensoring with $R/(a)$ over R, one finds the exact sequence of $R/(a)$-modules:

$$0 \to Z/Z \cap aF \longrightarrow F/aF \longrightarrow M/aM \to 0.$$

By assumption and construction, the map $F/aF \longrightarrow M/aM$ is a surjective map of free $R/(a)$-modules of the same rank, hence is an isomorphism. This implies that $Z = Z \cap aF$, hence $Z \subset aF$. Then $a \notin \mathcal{Z}(M)$ implies that $Z \subset aZ$—indeed, writing an arbitrary $z \in Z$ as $z = af$, for some $f \in F$, and going modulo Z, gives $f \in Z$. Now, apply Nakayama lemma to conclude that $Z = \{0\}$. □

Proposition 6.2.18. *Let $(R, \mathfrak{m})$ denote a local ring and let M stand for a finitely generated R-module. If $a \in \mathfrak{m}$ is a regular element on both R and M, then*

$$\mathrm{hd}_{R/(a)} M/aM = \mathrm{hd}_R M.$$

Proof. Let a be as in the statement. The base of the argument is the following.

Claim. If

$$\cdots \longrightarrow F_n \longrightarrow \cdots \longrightarrow F_0 \longrightarrow M \to 0 \tag{6.2.18.1}$$

is a free resolution of M then

$$\cdots \longrightarrow F_n/aF_n \longrightarrow \cdots \longrightarrow F_0/aF_0 \longrightarrow M/aM \to 0 \tag{6.2.18.2}$$

is a free resolution of M/aM.

In fact, let $0 \to Z_{i+1} \longrightarrow F_i \longrightarrow Z_i \to 0$, with $i = 0, 1, \ldots$ and $Z_0 = M$, stand for the induced short exact sequences from (6.2.18.1). Since a is a regular element on M, tensoring $0 \to Z_1 \longrightarrow F_0 \longrightarrow M \to 0$ with $R/(a)$ over R yields an exact sequence

$$0 \to Z_1/aZ_1 \longrightarrow F_0/aF_0 \longrightarrow M/aM \to 0.$$

Since a is regular on R, then it is so on every Z_i, for $i \geq 1$. Therefore, by the same token, one has exact sequences

$$0 \to Z_{i+1}/aZ_{i+1} \longrightarrow F_i/aF_i \longrightarrow Z_i/aZ_i \to 0 \quad (i \geq 1).$$

Pasting together one finds the free resolution (6.2.18.2).

Proceeding on, suppose that $\mathrm{hd}_{R/(a)} M/aM = n < \infty$. Then Z_n/aZ_n is a free $R/(a)$-module by Remark 6.2.11. Then Lemma 6.2.17 implies that Z_n is R-free, hence $\mathrm{hd}_R M \leq n$.

Conversely, if $\mathrm{hd}_R M = m < \infty$, then the above claim as applied to a finite free resolution of M of length m implies that $\mathrm{hd}_{R/(a)} M/aM \leq m$. □

6.2.2.4 The theorem of Auslander–Buchsbaum

In this part, one discusses a theorem of fundamental importance for the rest of the theory.

Theorem 6.2.19 (Auslander–Buchsbaum formula). *Let $(R, \mathfrak{m})$ denote a local ring and let M stand for a finitely generated R-module of finite homological dimension. Then*

$$\mathrm{hd}_R M + \mathrm{depth}\, M = \mathrm{depth}\, R.$$

Proof. One proceeds by induction on $\mathrm{depth}\, R$.

(1) $\mathrm{depth}\, R = 0$.

One claims that any finitely generated R-module of finite homological dimension is free. Supposing otherwise, let $\mathrm{hd}_R M = n > 0$. Letting $Z := \mathrm{coker}(F_n \to F_{n-1})$ along a free resolution of M of length n, one has $\mathrm{hd}_R Z = 1$. Rename Z to M and take a minimal free resolution $0 \to F_1 \longrightarrow F_0 \longrightarrow M \to 0$, with $F_1 \subset \mathfrak{m}F_0$. By assumption, $\mathfrak{m}$ is an associated prime of R, say, $\mathfrak{m} = 0 : r$, with $0 \neq r \in R$. Multiplying by r through $F_1 \subset \mathfrak{m}F_0$ yields $rF_1 = \{0\}$, hence $F_1 = \{0\}$ and M is free; this is a contradiction.

(2) $\mathrm{depth}\, R > 0$.

First, let $\mathrm{depth}\, M = 0$. In particular, M is not projective, hence in a finite free presentation $0 \to Z \longrightarrow F \longrightarrow M \to 0$ one has $\mathrm{hd}_R Z = \mathrm{hd}_R M - 1$ by Corollary 6.2.15,

while $\operatorname{depth} Z = \operatorname{depth} M + 1 = 1$ by Proposition 5.3.20(1). On the other hand, picking a regular element $a \in \mathfrak{m}$ gives $\operatorname{depth} R/(a) = \operatorname{depth} R - 1$ and, since a is also regular on F, hence on Z as well, one has $\operatorname{depth} Z/aZ = \operatorname{depth} Z - 1 = 1 - 1 = 0$. By the inductive hypothesis as applied to the ring $R/(a)$ and the $R/(a)$-module Z/aZ of depth zero, and drawing upon Proposition 6.2.18, one gets

$$\begin{aligned}\operatorname{hd}_R M &= \operatorname{hd}_R Z + 1 = \operatorname{hd}_{R/(a)} Z/aZ + 1 = \operatorname{depth} R/(a) - \operatorname{depth} Z/aZ + 1 \\ &= \operatorname{depth} R - 1 + 0 + 1 = \operatorname{depth} R + 0 = \operatorname{depth} R + \operatorname{depth} M.\end{aligned}$$

Finally, let $\operatorname{depth} M > 0$. This time around, one selects an element $a \in \mathfrak{m}$ which is regular both on R and on M. Then $\operatorname{hd}_{R/(a)} M/aM = \operatorname{hd}_R M$ by Proposition 6.2.18, while $\operatorname{depth}_{\mathfrak{m}/(a)} M/aM = \operatorname{depth}_{\mathfrak{m}} M/aM = \operatorname{depth}_{\mathfrak{m}} M - 1$. Since $\operatorname{depth} R/(a) = \operatorname{depth} R - 1$ one can apply the inductive hypothesis (for all modules over $R/(a)$ of finite homological dimension), thus getting

$$\operatorname{depth} R = \operatorname{depth} R/(a) + 1 = \operatorname{hd}_{R/(a)} M/aM + \operatorname{depth}_{\mathfrak{m}/(a)} M/aM + 1 = \operatorname{hd}_R M + \operatorname{depth} M,$$

as was to be shown. □

Next are some important consequences of the theorem. One makes use of the following lemma which is a special case of a result in [32].

Lemma 6.2.20. *Let $R \to S$ denote a homomorphism of local rings, with S finitely generated as R-module. If N is finitely generated S-module, one has*

$$\operatorname{hd}_R N \leq \operatorname{hd}_S N + \operatorname{hd}_R S.$$

Proof. One may clearly assume that $\operatorname{hd}_S N < \infty$ and $\operatorname{hd}_R S < \infty$.

One inducts on the first of these integers. If $\operatorname{hd}_S N = 0$, then N is S-free, say, $N \simeq S^d$, for some $d \geq 1$. Then $\operatorname{hd}_R N = \operatorname{hd}_R S^d = \operatorname{hd}_R S$, so one is done in this case.

Now, suppose that $\operatorname{hd}_S N \geq 1$. Letting

$$0 \to Z \longrightarrow G \longrightarrow N \to 0 \tag{6.2.20.1}$$

stand for a finite free presentation as S-modules, one has $\operatorname{hd}_S Z = \operatorname{hd}_S N - 1$ by Corollary 6.2.15. Applying the inductive hypothesis, one gets

$$\operatorname{hd}_R Z \leq \operatorname{hd}_S N + \operatorname{hd}_R S - 1. \tag{6.2.20.2}$$

Now consider the behavior of hd_R along (6.2.20.1), which is also an exact sequence of R-modules. If $\operatorname{hd}_R G \leq \operatorname{hd}_R Z$, then one is in either case (1) or (3) of Proposition 6.2.14, hence $\operatorname{hd}_R N \leq \operatorname{hd}_R Z + 1$. In this case, using (6.2.20.2) yields the required inequality. If $\operatorname{hd}_R G > \operatorname{hd}_R Z$, then one is in case (2) of Proposition 6.2.14, hence $\operatorname{hd}_R N = \operatorname{hd}_R G = \operatorname{hd}_R(S^d) = \operatorname{hd}_R S$, where $G \simeq S^d$ as S-module. In this case, the required inequality is obvious. □

Corollary 6.2.21. *Let* $(R, \mathfrak{m}) \to (S, \mathfrak{n})$ *denote a homomorphism of local rings, with* S *finitely generated as* R*-module and let* N *stand for a finitely generated* S*-module. If* $\operatorname{hd}_S N < \infty$ *and* $\operatorname{hd}_R S < \infty$*, then*

$$\operatorname{hd}_R N = \operatorname{hd}_S N + \operatorname{hd}_R S.$$

Proof. By Proposition 5.4.9, one has

$$\operatorname{depth}_{\mathfrak{n}} S = \operatorname{depth}_{\mathfrak{m}} S, \quad \operatorname{depth}_{\mathfrak{n}} N = \operatorname{depth}_{\mathfrak{m}} N.$$

Theorem 6.2.19 gives the following equalities:

$$\operatorname{hd}_R S = \operatorname{depth}_{\mathfrak{m}} R - \operatorname{depth}_{\mathfrak{m}} S$$

and

$$\operatorname{hd}_R N = \operatorname{depth}_{\mathfrak{m}} R - \operatorname{depth}_{\mathfrak{m}} N.$$

Assembling yields the required equality. □

An even more special case is very useful.

Corollary 6.2.22. *Let* $(R, \mathfrak{m})$ *denote a local ring and* $a \in \mathfrak{m}$ *a regular element of* R*. If* N *is a finitely generated* $R/(a)$*-module such that* $\operatorname{hd}_{R/(a)} N < \infty$*, then*

$$\operatorname{hd}_R N = \operatorname{hd}_{R/(a)} N + 1.$$

Proof. Since a is a regular element, one has an exact sequence

$$0 \to R \xrightarrow{\cdot a} R \longrightarrow R/(a) \to 0 \tag{6.2.22.1}$$

of R-modules. Clearly, this is a minimal free R-resolution of $R/(a)$, hence $\operatorname{hd}_R R/(a) = 1$. Now apply the previous corollary with $S = R/(a)$. □

Corollary 6.2.23. *Let* $(R, \mathfrak{m}) \to (S, \mathfrak{n})$ *denote an injective homomorphism of local rings, with* S *finitely generated as* R*-module. Then the following conditions are equivalent:*
(i) *R is Cohen–Macaulay and S is R-free.*
(ii) *S is Cohen–Macaulay and* $\operatorname{hd}_R S < \infty$.

Proof. (i) ⇒ (ii). This is easy—note that S is Cohen–Macaulay as an R-module if and only if it is Cohen–Macaulay as a ring (Proposition 5.4.9(b)).

(ii) ⇒ (i). One has

$$\begin{aligned}
\operatorname{depth}_{\mathfrak{m}} S + \operatorname{hd}_R S &= \operatorname{depth} R, && \text{by Theorem 6.2.19} \\
&\leq \dim R = \dim S, && \text{“dimension under finite extensions”} \\
&= \operatorname{depth}_{\mathfrak{n}} S, && \text{since } S \text{ is Cohen–Macaulay} \\
&= \operatorname{depth}_{\mathfrak{m}} S, && \text{by Proposition 5.4.9(a)}
\end{aligned}$$

It follows that $\operatorname{hd}_R S = 0$, hence S is R-free, and $\operatorname{depth} R = \dim R$, hence R is Cohen–Macaulay. □

Corollary 6.2.24. *Let R denote a Noetherian ring and let M stand for a finitely generated R-module admitting a finite free resolution. The following conditions are equivalent:*
(i) $0 : M$ *has a regular element.*
(ii) $0 : M \neq \{0\}$.

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

(ii) $\Rightarrow$ (i) First, note that $\operatorname{depth}_{\mathfrak{q}_\mathfrak{q}} R_\mathfrak{q}$ for every $\mathfrak{q} \in \operatorname{Ass} R$, hence $M_\mathfrak{q}$ is $R_\mathfrak{q}$-free for every such $\mathfrak{q}$ by a special case of Theorem 6.2.19.

Supposing that $0 : M$ is nonzero and has no regular elements, $0 : M$ is contained in some $\wp \in \operatorname{Ass} R$. Then $\wp \in \operatorname{supp} M$, *i. e.*, $M_\wp \neq \{0\}$. Therefore, $M_\wp \neq \{0\}$ is $R_\wp$-free of positive rank.

Localizing a finite free resolution $0 \to F_n \longrightarrow \cdots \longrightarrow F_0 \longrightarrow M \to 0$ at a prime $\mathfrak{q} \in \operatorname{Ass} R$, it is easy to see the following relation between the ranks of the various free modules over $R_\mathfrak{q}$:

$$\operatorname{rank} M_\mathfrak{q} = \sum_{i=0}^{n} (-1)^i \operatorname{rank}(F_i)_\mathfrak{q}.$$

Since the rank of a free module does not change under localization it follows that the rank of the localizations of M at primes of $\operatorname{Ass} R$ is constant. But $R_\wp$ has positive rank, hence all such localizations have positive rank as well. This implies that $(0 : M)_\mathfrak{q} = 0 : M_\mathfrak{q} = \{0\}$ for every $\mathfrak{q} \in \operatorname{Ass} R$. Clearly, then $(0 : M) = \{0\}$; a contradiction. □

Corollary 6.2.25. *Let R denote a Noetherian ring and let*

$$0 \to F_n \xrightarrow{\Phi_n} \cdots \xrightarrow{\Phi_2} F_1 \xrightarrow{\Phi_1} F_0 \longrightarrow M \to 0$$

denote a finite free resolution of a finitely generated R-module M. Then, for each $i = 1, \ldots, n$, the map Φ_i has well-defined rank r_i and $\operatorname{depth}_{I_{r_i}(\Phi_i)} R \geq i$.

Proof. It suffices to show that $Z_i := \operatorname{coker} \Phi_i$ has well-defined rank, for $i = 1, \ldots, n$. The argument is similar to the one in the proof of the previous corollary. Namely, for every $\wp \in \operatorname{Ass} R$, $(Z_i)_\wp$ is free (see the proof of Theorem 6.2.19, case (1)). Since the rank of a free module is constant under localizations, then Z_i is locally free at the primes of $\operatorname{Ass} R$ of constant rank.

Now, let $Z := \operatorname{coker} \Phi_i$. Pick a prime ideal $\wp \subset R$ containing $I_{r_i}(\Phi_i)$ and associated to a maximal R-sequence in $I_{r_i}(\Phi_i)$. Thus, $\operatorname{depth}_{I_{r_i}(\Phi_i)} R = \operatorname{depth}_\wp R = \operatorname{depth}_{\wp_\wp} R_\wp$. Localizing the given free resolution at $\wp$ one obtains a minimal free presentation

$$(F_i)_\wp \xrightarrow{\Phi_{i_\wp}} (F_{i-1})_\wp \longrightarrow Z_\wp \to 0$$

and an exact sequence

$$0 \to Z_\wp \longrightarrow (F_{i-2})_\wp \longrightarrow \cdots \longrightarrow (F_0)_\wp \longrightarrow M_\wp \to 0.$$

From the first of these sequences, one sees that $Z_{\wp}$ is not $R_{\wp}$-free, otherwise it would split, which would contradict $I_r(\Phi) \subset \wp$. Therefore, from the second sequence one deduces that $\operatorname{hd}_{R_{\wp}} M_{\wp} \geq i - 2 + 2 = i$. Now apply Theorem 6.2.19 to get $\operatorname{depth}_{\wp_{\wp}} R_{\wp} = \operatorname{hd}_{R_{\wp}} M_{\wp} + \operatorname{depth}_{\wp_{\wp}} M_{\wp} \geq i$, as was to be shown. □

Corollary 6.2.26 (Rees). *Let R denote a Noetherian ring and let M stand for a finitely generated R-module. Then* $\operatorname{depth}_{\wp} R \leq \operatorname{hd}_R M$ *for every* $\wp \in \operatorname{Ass} M$.

Proof. Assume that $\operatorname{hd}_R M < \infty$ as otherwise there is nothing to prove.

Since $\operatorname{depth}_{\wp_{\wp}} M_{\wp} = 0$ for $\wp \in \operatorname{Ass} M$, then by Theorem 6.2.19 gives

$$\operatorname{depth}_{\wp} R \leq \operatorname{depth}_{\wp_{\wp}} R_{\wp} = \operatorname{hd}_{R_{\wp}} M_{\wp} \leq \operatorname{hd}_R M,$$

where the last inequality is obvious by a localization argument. □

Since $0 : M \subset \wp$ for $\wp \in \operatorname{Ass} M$, one has $\operatorname{depth}_{0:M} R \leq \operatorname{hd}_R M$. This motivates the following notion.

Definition 6.2.27. A finitely generated module M over a Noetherian ring R is called *perfect* if $\operatorname{depth}_{0:M} R = \operatorname{hd}_R M$.

This definition is nearly superfluous due to the following

Corollary 6.2.28. *Let R denote a Cohen–Macaulay local ring and let M stand for a finitely generated R-module of finite homological dimension. Then M is perfect if and only if it is Cohen–Macaulay.*

Proof. Set $I := 0 : M$ for lighter reading. Suppose that M is perfect. Then:

$$\begin{aligned}
\operatorname{depth} M &= \operatorname{depth} R - \operatorname{hd}_R M, && \text{by Theorem 6.2.19}\\
&= \operatorname{depth} R - \operatorname{depth}_I R, && \text{since } M \text{ is perfect}\\
&= \dim R - \operatorname{ht} I = \dim R/I, && \text{since } R \text{ is Cohen–Macaulay}\\
&= \dim M.
\end{aligned}$$

The converse implication is proved in a totally similar way. □

In the footsteps of Corollary 6.2.28, one may quite justifiably ask what is the purpose of introducing perfect modules. One reason is that Cohen–Macaulay modules typically depend on the ambient, while many perfect modules exist "generically" in the sense that they are quite always ambient free.

Example 6.2.29. Most familiar examples of perfect modules are cyclic ones.

(a) Complete intersections.

Let $(R, \mathfrak{m})$ stand for a local ring and $\mathbf{a} := \{a_1, \ldots, a_n\} \subset \mathfrak{m}$ an R-sequence. Then an iterated application of Corollary 6.2.22 yields $\operatorname{hd}_R R/\mathbf{a} = n$. Moreover, the exact sequence (6.2.22.1) is truthful for a nonzero divisor a in any ring. A sort of tensor construction

based on this sequence defines a free complex that always resolves $R/\mathbf{a}$ over R for arbitrary R—this is the celebrated Koszul complex associated to $\mathbf{a}$, to be introduced in a later part. Thus, this a first example of a perfect module over an arbitrary ring.

(b) Determinantal rings.

This is a venerable subject, where on considers a ring R and an $m \times n$ matrix $\mathfrak{M}$ with entries in R. For any integer $\leq \min m, n$ one takes the ideal $I_t(\mathfrak{M}) \subset R$ generated by the $t \times t$ minors of $\mathfrak{M}$. The basic result concerning this setup says that if $I_t(\mathfrak{M}) \neq R$ and $\operatorname{depth}_{I_t(\mathfrak{M})} R \geq (m-t+1)(n-t+1)$ then $R/I_t(\mathfrak{M})$ is a perfect module and $\operatorname{depth}_{I_t(\mathfrak{M})} R = (m-t+1)(n-t+1)$.

One proof of this result consists in two fundamental steps. The first is to argue that in the generic case the determinantal ring is perfect, where by "generic" one means selecting $R := \mathbb{Z}[X_{i,j} \mid 1 \leq i \leq m, 1 \leq j \leq n]$, a polynomial ring over the integers of dimension mn, and $\mathfrak{M} = (X_{i,j})$. The second step consists in showing that perfect modules specialize. Both steps require some additional development, parts of which will be seen in a later section (Section 6.4).

A natural question arises as to when an ideal is a determinantal ideal. Of course, the question may in the very least impose certain a priori dimension restrictions. Curiously enough, over a Noetherian domain R every ideal I such that $\operatorname{depth}_I R \geq 2$ is nearly the ideal of maximal minors of an $(m+1) \times m$ matrix over R. More precisely, we have the following.

Proposition 6.2.30. *Let R denote a Noetherian domain and let $I \subsetneq R$ stand for an ideal such that $\operatorname{depth}_I R \geq 2$. Then there exists an $n \times (n-1)$ matrix φ of rank $n-1$, and a nonzero element $a \in R$ such that $aI = I_n(\varphi)$.*

Proof. Let $I = (a_1, \ldots, a_n)$. Consider a finite free presentation of I based on this set of generators:

$$F_1 \xrightarrow{\Phi} F_0 \longrightarrow I \to 0,$$

with F_0 of rank n; clearly, F_1 has rank at least $n-1$, while Φ has rank $n-1$. Applying $\_^* := \operatorname{Hom}_R(\_, R)$ yields an exact sequence of R-modules

$$0 \to I^* \xrightarrow{\delta} F_0^* \simeq R^n \xrightarrow{\Phi^*} F_1^*.$$

Since $\operatorname{depth}_I R \geq 2$, the natural inclusion $R^* \subset I^*$ is an equality. Up to such identification, one has $\delta(1) = (a_1 \ldots a_n)^t$, where ^{t} denotes transpose. Now, choose an $n \times (n-1)$ submatrix φ of rank $n-1$ of a matrix representing Φ and let $\Delta_1, \ldots, \Delta_n$ denote the signed ordered list of its $(n-1)$-minors.

Claim. $\varphi^t((\Delta_1 \ldots \Delta_n)^t) = (0 \ldots 0)^t$.

Indeed, every $n \times n$ subdeterminant of Φ vanishes. Hence, for any row $(b_{i,1} \ldots b_{i,n})$ of φ^t one has $\sum_{j=1}^n b_{i,j}\Delta_j = 0$, as claimed.

Finally, since $\operatorname{Im}\delta$ is the kernel of Φ^*, it follows that $(\Delta_1 \dots \Delta_n)^t \in \operatorname{Im}\delta$, *i. e.*, $(\Delta_1 \dots \Delta_n)^t = a(a_1 \dots a_n)$, for some $a \in R$, as required. □

Remark 6.2.31.

(a) If R is not a domain, the result has to be modified. Since $\operatorname{depth}_I R \geq 1$ then Φ still has well-defined rank $n-1$, which means that $\operatorname{depth}_{I_{n-1}(\Phi)} R \geq 1$. However, a regular element therein may not be an $(n-1)$-minor, hence the result would change to a more complicated statement involving minors from various submatrices.

(b) If R is a unique factorization domain (*e. g.*, a regular local ring) then the same result holds by assuming only that $I \neq 0$. Indeed, then one has $I = bJ$ for some ideal J such that $\operatorname{depth}_J R \geq 2$. Clearly, I and J have the same free presentation with respect to respective sets of generators $\{ba_1, \dots, ba_n\}$ and $\{a_1, \dots, a_n\}$, where $b = \gcd(a_1, \dots, a_n)$.

A consequence of the proposition is that over a Noetherian domain R any ideal of depth at least 2 is isomorphic as a module to the ideal of maximal minors of some $(n-1) \times n$ matrix over R. In a particular situation, this result has a strengthened form.

Theorem 6.2.32 (Hilbert–Burch). *Let $I \subset R$ denote an ideal over the Noetherian ring having a free resolution*

$$0 \to R^{n-1} \xrightarrow{\Phi} R^n \longrightarrow I \to 0. \tag{6.2.32.1}$$

Then there exists a regular element $b \in R$ such that $I = bI_{n-1}(\Phi)$.

Proof. Fix a free basis $\{e_1, \dots, e_n\}$ of R^n such that Φ also denotes the matrix with respect to the map $e_i \mapsto a_i$, with $I = (a_1, \dots, a_n)$.

One can trace through the proof of Proposition 6.2.30, with the notation there, where now $\varphi = \Phi$. Clearly, $I \neq 0$, hence Corollary 6.2.24 with $M = R/I$ yields that I has a regular element. This means that Φ has well-defined rank $n-1$, *i. e.*, $\operatorname{depth}_{I_{n-1}(\Phi)} R \geq 1$ and one has no need to assume that R is a domain. If actually $\operatorname{depth}_R I \geq 2$, one could apply Proposition 6.2.30 to deduce that I and $I_{n-1}(\Phi)$ are isomorphic as modules. Instead, one has $\operatorname{depth}_{I_{n-1}(\Phi)} R \geq 2$ by Corollary 6.2.25 and this will do as well.

In fact, the complex

$$0 \to R^{n-1} \xrightarrow{\Phi} R^n \xrightarrow{\pi} I_{n-1}(\Phi) \to 0$$

is also exact, where $\pi : e_i \mapsto \Delta_i$. Applying $\_^* := \operatorname{Hom}_R(\_, R)$ to the latter complex and exchanging roles between the two exact complexes yields an isomorphism of modules $\eta : I_{n-1}(\Phi) \simeq I \subset R$ and the induced homomorphism $I_{n-1}(\Phi) \to R$ must be multiplication by an element $b \in R$ since $R \simeq R^*$ and the natural inclusion $R^* \subset I_{n-1}(\Phi)^*$ is an equality.

This shows that $I = bI_{n-1}(\Phi)$ for some $b \in R$. Clearly, b is a regular element since $\operatorname{depth}_I R \geq 1$. □

6.2.2.5 The theorem of Vasconcelos

A second fundamental theorem is as follows.

Theorem 6.2.33 (Vasconcelos). *Let $(R, \mathfrak{m})$ denote a local ring and let $I \subset \mathfrak{m}$ stand for an ideal. The following conditions are equivalent:*
(i) *I is generated by an R-sequence.*
(ii) *$\mathrm{hd}_R\, R/I < \infty$ and I/I^2 is a free R/I-module.*

Proof. (i) $\Rightarrow$ (ii) Let $\mathbf{a} = \{a_1, \ldots, a_n\}$ denote an R-sequence generating I. The issue of the finite homological dimension has been treated in Example 6.2.29 (a). As to the stated freeness, the fastest is to use the fact to be established independently in Subsection 6.3 to the effect that the module of syzygies of I is generated by the so-called trivial syzygies of $\mathbf{a}$, namely, those of the form $a_j \cdot a_i - a_i \cdot a_j = 0$, for $1 \leq i \leq j \leq n$. This implies that I admits a free presentation $0 \to Z \longrightarrow F \longrightarrow I \to 0$, with $Z \subset IF$. Tensoring with R/I over R yields immediately $F/IF \simeq I/I^2$.

(A direct proof of the freeness of I/I^2 is available by applying the definition of R-sequence to argue that the residues of $\{a_1, \ldots, a_n\}$ as elements of the R-module I/I^2 form a free basis.)

(ii) $\Rightarrow$ (i) This is of course the hard direction.

To avoid confusion, the residue in I/I^2 of an element $a \in I$ will be denoted $\widetilde{a}$.

Claim 1. I/I^2 admits a free basis $\{\widetilde{a}_1, \ldots, \widetilde{a}_n\}$, with a_1 is a regular element of R.

To argue for the claim, first note that since I/I^2 is a free R/I-module then any minimal set of generators of I/I^2 is a free basis as this much holds for any free module M of finite rank over a local ring S. To see this, take a minimal free presentation $0 \to Z \longrightarrow F \longrightarrow M \to 0$ corresponding to the given set of minimal generators of M, so $Z \subset \mathfrak{m}F$; since M is free, the sequence splits, hence Z is a direct summand of F. But this forbids $Z \subset \mathfrak{m}F$ unless $Z = \{0\}$. Then the original map $F \longrightarrow M$ is an isomorphism, in particular the image of a free basis has to be a free basis.

Next, to get a minimal set of generators of I/I^2 with the required proviso, note that $I/I^2 \otimes_R R/\mathfrak{m} \simeq I/\mathfrak{m}I$. This implies by Nakayama that any choice $a_1 \in I \setminus \mathfrak{m}I$ is such that $\widetilde{a_1}$ belongs to a minimal set of generators of I/I^2. But even more is within reach: by Corollary 6.2.24, with $M = R/I$, the ideal I admits regular elements. Therefore, $I \not\subset \mathfrak{m}I \cup (\bigcup_{\wp \in \mathrm{Ass}\, R} \wp)$. By prime avoidance, one can pick a regular element $a_1 \in I \setminus \mathfrak{m}I$. This proves the claim.

To proceed, one inducts on the cardinality of a free basis of I/I^2.

Let $\{\widetilde{a}_1, \ldots, \widetilde{a}_n\}$ stand for such a basis with $a_1 \in I$ a regular element. Set $\overline{R} = R/(a_1)$ and $\overline{I} = I/(a_1)$.

Claim 2. $\overline{I}/\overline{I}^2$ is $\overline{R}/\overline{I}$-free of rank $n-1$.

As a preliminary, note that $\overline{R}/\overline{I} \simeq R/I$ and that $\overline{I}/\overline{I}^2 \simeq I/(I^2, a_1)$. Thus, one has an exact sequence of R/I-modules

$$0 \to (I^2, a_1)/I^2 \longrightarrow I/I^2 \longrightarrow \overline{I}/\overline{I}^2 \to 0. \tag{6.2.33.1}$$

But one has the following isomorphisms of R/I-modules:

$$\begin{aligned}(I^2, a_1)/I^2 \simeq (a_1)/(a_1) \cap I^2 \simeq (a_1)/a_1 I, &\quad \text{since } \widetilde{a_1} \text{ is a free element in } I/I^2\\ \simeq R/I \otimes_R (a_1) \simeq (R/I)\widetilde{a}_1, &\quad \text{since } Ra_1 \text{ is } R\text{-free.}\end{aligned}$$

Back to (6.2.33.1), the kernel is isomorphic to the free direct summand $(R/I)\widetilde{a}_1$ of I/I^2 of rank one, hence the cokernel $\overline{I}/\overline{I}^2$ is a free R/I-module of rank $n-1$. This takes care of Claim 2.

Claim 3. $\mathrm{hd}_{\overline{R}}(\overline{R}/\overline{I}) < \infty$.

Of course, $\overline{R}/\overline{I} \simeq R/I$, but one needs to show that the homological dimension of R/I over $\overline{R} = R/(a_1)$ is still finite.

Introduce the ideal $J := (a_1 I, a_2, \ldots, a_n)$. Clearly, $I = (a_1, J)$. Moreover, one has $(a_1) \cap J = a_1 I$. Indeed, let $y \in (a_1) \cap J$, say, $y = r_1 a_1 = a_1 a + \sum_{i>1} r_i a_i$, with $r_i \in R$, $a \in I$. Then $r_1 a_1 - \sum_{i>1} r_i a_i \in I^2$ and since $\{\widetilde{a}_1, \ldots, \widetilde{a}_n\}$ is a free basis of I/I^2 one derives $r_1 \in I$, hence $y \in a_1 I$, as was to be shown.

It follows that $I/a_1 I = (a_1, J)/(a_1) \cap J \simeq (a_1)/a_1 I \oplus J/a_1 I$ as $R/(a_1)$-modules. Now, $\mathrm{hd}_{R/(a_1)} I/a_1 I = \mathrm{hd}_R I$ by Proposition 6.2.18 with $M = I$, since a_1 is regular on R, hence on I as well. Therefore, $I/a_1 I$ has finite homological dimension over $R/(a_1)$ and so does its direct summand $(a_1)/a_1 I$. But $(a_1)/a_1 I \simeq (R/I)\widetilde{a}_1 \simeq R/I$ as $R/(a_1)$-modules, hence one is through. □

Corollary 6.2.34 (Serre's theorem). *A local ring* $(R, \mathfrak{m})$ *is regular if and only if* $\mathrm{hd}_R R/\mathfrak{m} < \infty$.

Of course, Vasconcelos' theorem is later to Serre's by 10 years. One will come back to Serre's methods in subsequent subsections.

The following question remains open.

Conjecture 6.2.35 (Vasconcelos). *Let* $(R, \mathfrak{m})$ *denote a local ring and let* $I \subset \mathfrak{m}$ *stand for an ideal with* $\mathrm{hd}_R R/I < \infty$. *Then* $\mathrm{hd}_{R/I} I/I^2$ *is either* 0 *or* ∞.

Only a few cases have been touched upon: Vasconcelos has proved that $\mathrm{hd}_{R/I} I/I^2 = 1$ is not possible. The conjecture is part of a more encompassing conjecture as stated in [157].

Remark 6.2.36. Note that the hypothesis that I/I^2 is a free R/I-module by itself does not imply much, as one already knows from the case where $\mathfrak{m}$ is the maximal ideal of a local ring. Even the stronger condition that all higher conormal modules I^t/I^{t+1} are free R/I-modules over a nonregular ring just implies that all relations of I have coefficients in I—like when the associated graded ring of Section 7.3 is a free R/I-module. Typically, an ideal generated by a system of parameters in a Cohen–Macaulay local ring will be of this kind (see Proposition 7.4.32).

6.2.3 Chain complexes

The basic object of this part has been introduced in various particular situations before. Here, one intends to consider its abstract shape that will make possible to work with the so-called chain homology.

Some authors may believe that one can disregard this general theory in favor of a more concrete one by taking free modules (*cf.*, *e. g.*, [112]).

Let R be a ring. One is given a sequence of R-modules and R-homomorphisms

$$\cdots \to C_{i+1} \xrightarrow{d_{i+1}} C_i \xrightarrow{d_i} C_{i-1} \to \cdots \quad (i \in \mathbb{Z}) \tag{6.2.36.1}$$

satisfying the condition $d_i \circ d_{i+1} = 0$, for every i.

One calls (6.2.36.1) a *complex* or *chain complex* (of modules). The maps d_i are called the *differentials* (*boundary maps* is often used as to keep the topological ancestrality) of the complex, while the modules C_i are the *components* or *terms* or *chains* of the complex. One adheres to the notation $C_\bullet$ for the complex (6.2.36.1)—sometimes even $(C_\bullet, \mathbf{d}_\bullet)$ to emphasize its structural differentials.

Remark 6.2.37. In this book, complexes will typically be right-bounded, *i. e.*, $C_i = \{0\}$ for $i < 0$. A structure like (6.2.36.1) where the differentials follow the increasing ordering of the indices is called *co-complex*, denoted $C^\bullet$. The theory of complexes to follow can be easily adapted to the case of co-complexes and, in fact, many authors prefer to deal with the latter instead. One leaves to the reader the details of the required adaptation.

The essential information carried by a complex is expressed by the following modules:

$$\begin{aligned} Z_i(C_\bullet) &:= \ker \mathrm{d}_i && (\textit{cycles} \text{ of degree } i) \\ B_i(C_\bullet) &:= \operatorname{Im} \mathrm{d}_{i+1} && (\textit{boundary cycles} \text{ of degree } i) \\ H_i(C_\bullet) &:= \ker \mathrm{d}_i / \operatorname{Im} \mathrm{d}_{i+1} && (\textit{homology} \text{ in degree } i) \end{aligned} \tag{6.2.37.1}$$

(The *cocycles, coboundaries, cohomology* of degree i are defined similarly as $Z^i(C^\bullet) := \ker \mathrm{d}_{i+1}$, $B^i(C^\bullet) := \operatorname{Im} \mathrm{d}_i$, $H^i(C^\bullet) := \ker \mathrm{d}_{i+1} / \operatorname{Im} \mathrm{d}_i$, respectively.)

One says that $C_\bullet$ is exact in degree i if $H_i(C_\bullet) = \{0\}$, while $C_\bullet$ is *exact* (or *acyclic*) if it is exact in degree i for every $i \geq 1$.

It is customary to append a zero at the right end of the complex, namely, writing $\cdots \longrightarrow C_1 \longrightarrow C_0 \to 0$. In this way, one always has $H_0(C_\bullet) = C_0 / \operatorname{Im} \mathrm{d}_1$ and the rest of the homology of the complex is supposed to give some insight into the structure of the 'augmentation module' $H_0(C_\bullet)$. For example, a projective resolution of a module M is an exact complex of projective modules whose augmentation is M.

6.2.3.1 Functorial properties

Complexes of modules can be made into a category. Here, one will restrict the discussion to some routine constructions involving complexes.

Given two complexes $C_\bullet$ and $C'_\bullet$, a *morphism* (or *chain map*) $\mathbf{f} : C_\bullet \to C'_\bullet$ is a collection $\mathbf{f} = \{f_i\}_{i\geq 0}$ of module homomorphisms $f_i : C_i \to C'_i$ such that the following diagram of maps is commutative:

$$\begin{array}{ccccccccc} \cdots & \to & C_{i+1} & \xrightarrow{d_{i+1}} & C_i & \xrightarrow{d_i} & C_{i-1} & \to & \cdots \\ & & f_{i+1}\downarrow & & f_i\downarrow & & f_{i-1}\downarrow & & \\ \cdots & \to & C'_{i+1} & \xrightarrow{d_{i+1}} & C'_i & \xrightarrow{d_i} & C'_{i-1} & \to & \cdots \end{array} \tag{6.2.37.2}$$

The morphism $\mathbf{f}$ is said to be an isomorphism if f_i is an isomorphism for every $i \geq 0$.

More precisely, (6.2.37.2) is a morphism of degree 0.

One could analogously define a morphism of degree r, for any fixed integer r, by requiring homomorphisms $f_i : C_i \to C'_{r+i}$ instead. This extended notion is nearly superfluous as it is equivalent to having a morphism $\mathbf{f} : C_\bullet \to C'_\bullet(-r)$ of degree 0, where $C'_\bullet(-r)$ is the *r-shifted* complex defined by setting $C'_\bullet(-r)_i = (C'_\bullet)_{r-i}$.

Note that taking homology is a functorial step in the sense that the chain map (6.2.37.2) induces a collection $H_\bullet(\mathbf{f}) := \{H_i(\mathbf{f})\}_{i\geq 0}$, where $H_i(\mathbf{f}) : H_i(C_\bullet) \to H_i(C'_\bullet)$ is a module homomorphism.

One can further introduce the notion of an exact sequence of chain maps. To wit, this consists of a pair of chain maps $\mathbf{f} : C'_\bullet \to C_\bullet$ and $\mathbf{g} : C_\bullet \to C''_\bullet$ such that, for every $i \geq 0$, the sequence of module homomorphisms

$$0 \to C'_i \xrightarrow{f_i} C_i \xrightarrow{g_i} C''_i \to 0$$

are exact. Such an exact sequence will be denoted

$$0 \to C'_\bullet \xrightarrow{\mathbf{f}} C_\bullet \xrightarrow{\mathbf{g}} C''_\bullet \to 0 \tag{6.2.37.3}$$

(Note that, for printing convenience, one is in this definition writing the complexes as vertical sequences of maps, so one can see the ith slices as horizontal sequences of module homomorphisms.)

By functoriality, (6.2.37.3) induces a collection of homomorphisms at the level of homology:

$$0 \to H_i(C'_\bullet) \xrightarrow{H_i(\mathbf{f})} H_i(C_\bullet) \xrightarrow{H_i(\mathbf{g})} H_i(C''_\bullet) \to 0.$$

A question arises as to whether this is a disconnected bunch of maps. The answer is the following.

Proposition 6.2.38 (Long exact sequence in homology). *Let there be given an exact sequence* $0 \to C'_\bullet \xrightarrow{\mathbf{f}} C_\bullet \xrightarrow{\mathbf{g}} C''_\bullet \to 0$ *of complexes. Then, for every* $i \geq 0$*, there exists a homomorphism* $\delta_i : H_i(C''_\bullet) \to H_i(C'_\bullet)$ *such that the following sequence of homomorphisms:*

$$\begin{aligned} \cdots \to H_i(C'_\bullet) &\xrightarrow{H_i(\mathbf{f})} H_i(C_\bullet) \xrightarrow{H_i(\mathbf{g})} H_i(C''_\bullet) \\ &\xrightarrow{\delta_i} H_{i-1}(C'_\bullet) \xrightarrow{H_{i-1}(\mathbf{f})} H_{i-1}(C_\bullet) \xrightarrow{H_{i-1}(\mathbf{g})} H_{i-1}(C''_\bullet) \\ &\xrightarrow{\delta_{i-1}} \cdots \end{aligned} \tag{6.2.38.1}$$

is an exact complex.

Proof. Consider a slice of the given short exact sequence:

$$\begin{array}{ccccccccc} 0 & \to & C'_i & \xrightarrow{f_i} & C_i & \xrightarrow{g_i} & C''_i & \to & 0 \\ & & d'_i \downarrow & & d_i \downarrow & & d''_i \downarrow & & \\ 0 & \to & C'_{i-1} & \xrightarrow{f_{i-1}} & C_{i-1} & \xrightarrow{g_{i-1}} & C''_{i-1} & \to & 0 \end{array} \tag{6.2.38.2}$$

By the snake lemma, one has a connecting homomorphism

$$\widetilde{\delta}_i : Z_i(C''_\bullet) = \ker d''_i \to \operatorname{coker} d'_i = C'_{i-1}/\operatorname{Im} d'_i = C'_{i-1}/B_i(C'_\bullet).$$

Claim. The image of $\widetilde{\delta}_i$ is contained in $Z_i(C'_\bullet)/B_i(C'_\bullet)$ and $\widetilde{\delta}_i(B_i(C''_\bullet)) = \{0\}$.

For the first assertion, let $\mathfrak{z}'' \in Z_i(C''_\bullet)$ and let $c'_{i-1} \in C'_{i-1}$ denote a preimage of $\widetilde{\delta}_i(\mathfrak{z}'')$. In addition, let $c_i \in C_i$ denote a preimage of $\mathfrak{z}''$ by g_i. Then

$$f_{i-2}(d'_{i-1}(c'_{i-1})) = d_{i-1}(f_{i-1}(c'_{i-1})) = (d_{i-1} \circ d_i)(c_i) = 0.$$

Since f_{i-2} is injective, $d'_{i-1}(c'_{i-1}) = 0$, as claimed.

For the second assertion, suppose that $\mathfrak{z}'' = d''_{i+1}(c''_{i+1})$, for some $c''_{i+1} \in C''_{i+1}$. Let $c_{i+1} \in C_{i+1}$ denote a preimage of c''_{i+1} by g_{i+1}. Then $(d_i \circ d_{i+1})(c_{i+1}) = 0$. By the definition of $\widetilde{\delta}_i$ via the snake lemma and by the fact that f_{i-1} is injective, one must have $\widetilde{\delta}_i(\mathfrak{z}'')$, as asserted.

As a consequence of the discussion so far, one has an induced homomorphism

$$\delta_i : H_i(C''_\bullet) = Z_i(C''_\bullet)/B_i(Z_i(C''_\bullet)) \longrightarrow Z_i(C'_\bullet)/B_i(C'_\bullet) = H_i(C'_\bullet).$$

It remains to show that

(1) $\operatorname{Im}(H_i(\mathbf{g})) = \ker \delta_i$, and
(2) $\operatorname{Im}(\delta_i) = \ker H_{i-1}(\mathbf{f})$.

After sufficient manipulation as above, both are consequences of the remaining maps in the snake lemma. □

Definition 6.2.39. The sequence (6.2.38) is called the *long exact sequence in homology* associated to the given short exact sequence of complexes. The reader will easily deduce a similar long exact sequence in cohomology associated to a short exact sequence of cocomplexes.

6.2.3.2 New complexes from old ones

Tensor product

The operation of tensor product of modules extends to complexes.

Definition 6.2.40. Let $(C_\bullet, d_\bullet)$ and $(C'_\bullet, d'_\bullet)$ stand for complexes. The *tensor product* of these two complexes is the complex $(C_\bullet \otimes_R C'_\bullet, \partial_\bullet)$, with terms

$$(C_\bullet \otimes_R C'_\bullet)_n := \bigoplus_{i=0}^{n} C_i \otimes_R C'_{n-i} \tag{6.2.40.1}$$

and differentials

$$\partial_n(c_i \otimes_R c'_{n-i}) := (0, \dots, 0, d_i(c_i) \otimes_R c'_{n-i}, (-1)^i c_i \otimes_R \mathrm{d}'_{n-i}(c'_{n-i}), 0, \dots, 0). \tag{6.2.40.2}$$

Note that the image of $c_i \otimes_R c'_{n-i}$ has null terms in all summands of $(C_\bullet \otimes_R C'_\bullet)_{n-1}$ except possibly in $C_{i-1} \otimes_R C'_{n-i}$ and $C_i \otimes_R C'_{n-i-1}$.

It is easily verified that indeed $\partial_{n-1} \circ \partial_n = 0$ for every $n \geq 0$.

Equally easy, though tedious, is the verification that this operation is commutative in the sense that the two complexes $(C_\bullet \otimes_R C'_\bullet, \partial_\bullet)$ and $(C'_\bullet \otimes_R C_\bullet, \partial'_\bullet)$ are naturally isomorphic, where ∂' is similarly defined. By iterative associativity, one defines the tensor product of a finite collection of complexes.

Mapping cone

This construction comes from algebraic topology and it often gives a hint about free resolutions of certain modules.

Given a chain map $\mathbf{f} : (C_\bullet, \mathbf{d}_\bullet) \to (C'_\bullet, \mathbf{d}'_\bullet)$, one introduces for each $i \geq 0$ the module $\mathbb{M}(\mathbf{f})_i := C'_i \oplus C_{i-1}$ and a homomorphism $\partial_i : \mathbb{M}(\mathbf{f})_i \to \mathbb{M}(\mathbf{f})_{i-1}$ defined (in suggestive matrix form) as

$$\partial_i = \begin{pmatrix} d'_i & (-1)^i f_{i-1} \\ 0 & d_{i-1} \end{pmatrix}. \tag{6.2.40.3}$$

Proposition 6.2.41 (Mapping cone). *In the above notation, one has:*

(i) $\mathbb{M}(\mathbf{f})_\bullet = (\mathbb{M}(\mathbf{f})_\bullet, \partial_\bullet)$ *is a complex.*

(ii) $\mathbb{M}(\mathbf{f})_\bullet$ *is acyclic if and only if the induced map* $H_i(\mathbf{f}) : H_i(C_\bullet) \to H_i(C'_\bullet)$ *is an isomorphism for every* $i \geq 1$.

Proof. (i) is straightforward. Since one wrote δ_i in the above matrix form, then it applies on the right to an element of $\mathbb{M}(\mathbf{f})_i$ written as a column vector:

$$
\begin{aligned}
(\delta_{i-1}\circ\delta_i)\begin{pmatrix} c_i' \\ c_{i-1}\end{pmatrix} &= \delta_{i-1}\begin{pmatrix} d_i'(c_i') + (-1)^i f_{i-1}(c_{i-1}) \\ d_{i-1}(c_{i-1})\end{pmatrix} \\
&= \begin{pmatrix} (d_{i-1}'\circ d_i')(c_i') - (d_{i-1}'\circ f_{i-1})(c_{i-1}) + (f_{i-2}\circ d_{i-1})(c_{i-1} \\ (d_{i-2}\circ d_{i-1})(c_{i-1})\end{pmatrix} \\
&= \begin{pmatrix} (d_{i-1}'\circ d_i')(c_i') - (f_{i-2}\circ d_{i-1})(c_{i-1}) + (f_{i-2}\circ d_{i-1})(c_{i-1} \\ (d_{i-2}\circ d_{i-1})(c_{i-1})\end{pmatrix} \\
&= \begin{pmatrix} 0 \\ 0\end{pmatrix}.
\end{aligned}
$$

To prove (ii), one considers the exact sequence of chain maps

$$0 \to C_\bullet' \longrightarrow \mathbb{M}(\mathbf{f}) \longrightarrow C_\bullet(-1) \to 0, \tag{6.2.41.1}$$

induced by the natural split exact sequences $0 \to C_i' \longrightarrow \mathbb{M}(\mathbf{f})_i \longrightarrow C_{i-1} \to 0$, for $i \geq 0$. Then take the associated long exact sequence of chain maps

$$
\begin{aligned}
\cdots \to\ & H_i(C_\bullet') \longrightarrow H_i(\mathbb{M}(\mathbf{f})) \longrightarrow H_i(C_\bullet(-1)) = H_{i-1}(C_\bullet) \\
& \xrightarrow{\delta_i} H_{i-1}(C_\bullet') \longrightarrow H_{i-1}(\mathbb{M}(\mathbf{f})) \longrightarrow H_{i-1}(C_\bullet(-1)) = H_{i-2}(C_\bullet) \\
& \xrightarrow{\delta_{i-1}} \cdots
\end{aligned}
$$

Now, because of the splitting character of (6.2.41.1) and the naturality of the maps in the long exact sequence, one can check that δ_i is the induced map in homology $H_i(\mathbf{f}) : H_i(C_\bullet) \to H_i(C_\bullet')$. This proves the required statement. □

Definition 6.2.42. The above construction is known as the *mapping cone* or *the mapping cylinder* of the chain map $\mathbf{f}$.

One of its applications is the construction of the Koszul complex (Section 6.3). A typical application is to the case where $(C_\bullet, \mathbf{d}_\bullet)$ and $(C_\bullet', \mathbf{d}_\bullet')$ are acyclic.

Double chain complexes

The idea of a double complex generalizes the previous notions. It is visually convenient to think of a chain complex as a dimension-one diagram, while a double complex as a dimension-two diagram, extending throughout the entire plane as a grid of chain complexes with commutative squares.

A *double (chain) complex* has the usual nature of any double mathematical structure. Namely, it is a grid $C_{\bullet,\bullet} = \{C_{r,s}\}_{(r,s)\in\mathbb{Z}\times\mathbb{Z}}$ of R-modules such that:

(i) For every fixed $r \in \mathbb{Z}$ (resp., $s \in \mathbb{Z}$), the family $C_{r,\bullet}$ (resp., $C_{\bullet,s}$) is a "vertical" (resp., "horizontal") chain complex; let $d_{\mathbf{r},s} : C_{r,s} \to C_{r,s-1}$ (resp., $d_{r,\mathbf{s}} : C_{r,s} \to C_{r-1,s}$) denote its sth differential (respectively, its rth differential)

(ii) For every pair $(r,s) \in \mathbb{Z}\times\mathbb{Z}$, one has $d_{\mathbf{r}-1,s}\circ d_{\mathbf{r},s} = d_{r,\mathbf{s}-1}\circ d_{\mathbf{r},s-1}$.

Note that to comply with the definition of a chain complex, the "vertical" differential $d_{r,\mathbf{s}-1}$ of $C_{r,\bullet}$ maps $C_{r,s}$ to $C_{r,s-1}$ (sliding along $\mathbb{Z}$ in the decreasing direction). A simi-

lar remark goes for the "horizontal" differentials as well. The following commutative square illustrates the definition:

$$\begin{array}{ccc} C_{r,s} & \xrightarrow{d_{\mathbf{r}-1,s}} & C_{r-1,s} \\ {\scriptstyle d_{r,\mathbf{s}-1}}\downarrow & & {\scriptstyle d_{\mathbf{r},s}}\downarrow \\ C_{r,s-1} & \xrightarrow{d_{\mathbf{r},s-1}} & C_{r-1,s-1} \end{array} \tag{6.2.42.1}$$

A foremost example comes from the tensor product of two complexes $(C_\bullet, d_\bullet)$ and $(C'_\bullet, d'_\bullet)$ that induces a double complex $C_{\bullet,\bullet} = C_\bullet \otimes_R C'_\bullet$ with terms $(C_\bullet \otimes_R C'_\bullet)_{r,s} = C_r \otimes_R C'_s$ and differentials as in (6.2.40.2).

The *total (chain) complex* associated to a double complex $C_{\bullet,\bullet}$ is the single chain complex $\mathrm{Tot}(C_{\bullet,\bullet})$ with terms

$$\big(\mathrm{Tot}(C_{\bullet,\bullet})\big)_n := \bigoplus_{r+s=n} (C_{\bullet,\bullet})_{r,s} \tag{6.2.42.2}$$

and differentials defined like in (6.2.40.2).

Note that the terms of the total complex are nothing more than the direct sums of the terms of the original double complex taken along the antidiagonals of the grid squares (visualize it in (6.2.42.1)). As to the differentials, they are as complicated as in (6.2.40.2), but no more.

Remark 6.2.43. The notion of total complex is a basic technique in the realm of the so-called *spectral sequences*. Although the latter is beyond the objective of the book, it is good to keep in mind that it leads to alternative ways of showing increasingly involved properties of the derived functors $\mathrm{Tor}_i(M,N)$.

One often says that the homology of the original double complex $C_{\bullet,\bullet}$ is the homology of its associated total complex and writes by abuse $H_i(C_{\bullet,\bullet}) := H_i(\mathrm{Tot}(C_{\bullet,\bullet}))$.

Homotopy equivalence

The next notion, also inspired from topology, establishes a way of detecting isomorphisms of homologies.

Definition 6.2.44. Let $\mathbf{f}, \mathbf{g} : (C_\bullet, \mathbf{d}_\bullet) \to (C'_\bullet, \mathbf{d}'_\bullet)$ denote two chain maps. One says that $\mathbf{f}$ is *homotopic* to $\mathbf{g}$ if there is a collection of module homomorphisms $\mathbf{h} := \{h_i : C_i \to C'(1)\}_{i\geq 0}$ such that $f_i - g_i = d'_{i+1} \circ h_i + h_{i-1} \circ d_i$, for every $i \geq 0$.

One can depict the idea through the following diagram:

$$\begin{array}{ccccccccc} \cdots & \to & C_{i+1} & \xrightarrow{d_{i+1}} & C_i & \xrightarrow{d_i} & C_{i-1} & \to & \cdots \\ & & \downarrow\downarrow & {\scriptstyle h_i}\swarrow & \downarrow\downarrow & {\scriptstyle h_{i-1}}\swarrow & \downarrow\downarrow & & \\ \cdots & \to & C'_{i+1} & \xrightarrow{d'_{i+1}} & C'_i & \xrightarrow{d'_i} & C'_{i-1} & \to & \cdots \end{array} \tag{6.2.44.1}$$

where the vertical down-arrows represent f_i, g_i, for $i \geq 0$.

Proposition 6.2.45. *Let* $\mathbf{f}, \mathbf{g} : (C_\bullet, \mathbf{d}_\bullet) \to (C'_\bullet, \mathbf{d}'_\bullet)$ *denote two chain maps. If* $\mathbf{f}$ *is homotopic to* $\mathbf{g}$*, then* $H_i(\mathbf{f}) : H_i(C_\bullet) \to H_i(C'_\bullet)$ *and* $H_i(\mathbf{g}) : H_i(C_\bullet) \to H_i(C'_\bullet)$ *are the same map for every* $i \geq 0$.

Proof. Obviously, $\mathbf{f}$ is homotopic to $\mathbf{g}$ if and only if $\mathbf{f} - \mathbf{g}$ is homotopic to the zero map. Thus, one can assume that the hypothesis is that $\mathbf{f}$ is a chain map homotopic to the zero map and the goal is to show that $\mathbf{f}$ induces the zero map in homology, that is to say, that for every $i \geq 0$ and every $\mathfrak{z} \in Z_i(C_\bullet)$, one has $f_i(\mathfrak{z}) \in B_i(C'_\bullet)$.

But the hypothesis says that $f_i = d'_{i+1} \circ h_i + h_{i-1} \circ d_i$, for some homotopy $\mathbf{h}$. Applying to $\mathfrak{z}$ gives $f_i(\mathfrak{z}) = d'_{i+1}(h_i(\mathfrak{z})) + h_{i-1}(0) = d'_{i+1}(h_i(\mathfrak{z})) \in B_i(C'_\bullet)$. □

6.2.4 Basics on derived functors

Derived functors are an invention of Cartan–Eilenberg ([32]), and so are the terminologies "Tor" and "Ext." Alas, the introduction of these objects is not always easy to grasp in their source, perhaps due to its aiming at great generality. Since the goal here is quite narrower, envisaging exclusively the homology of Noetherian rings and modules, likewise will be the material developed in the section.

A full treatment would perhaps require introducing elements of category theory, but this would hardly make sense when the applications are circumscribed to only two examples. The only category to be considered here is that of modules over a fixed ring R, well known to have the usual good properties. The only functors of this category to be envisaged are the tensor product and the "hom" functor.

For the definitions, one is given a functor $\mathcal{F}$ of modules, which can be *covariant* (respectively, *contravariant*) in the sense that it maps a homomorphism $M \to M'$ to a homomorphism $\mathcal{F}(M) \to \mathcal{F}(M')$ (resp., $\mathcal{F}(M') \to \mathcal{F}(M)$). Here, one deals with the covariant case, leaving to the reader the required adjustments for the contravariant case.

Basically, the derived functors of a given functor $\mathcal{F}$ of modules appear as a family of functors indexed over the natural integers. However, for this to happen, the given functor $\mathcal{F}$ is required to fulfill a strong condition in relation to short exact sequences of modules. Namely, one says that a (covariant) functor $\mathcal{F}$ is *right-exact* if, for every short exact sequence of R-modules $0 \to M' \longrightarrow M \longrightarrow M'' \to 0$, the resulting sequence

$$\mathcal{F}(M') \longrightarrow \mathcal{F}(M) \longrightarrow \mathcal{F}(M'') \to 0$$

is exact.

The reader will as easily introduce the notion of a (covariant or contravariant) left-exact functor.

Definition 6.2.46. Let $\mathcal{F}$ denote a (covariant) right-exact functor of R-modules and let M stand for an R-module. Consider a projective resolution $P_\bullet$ of M and apply $\mathcal{F}$ to it to

get the complex $\mathcal{F}(P_\bullet)$, where $\mathcal{F}(P_\bullet)_i = \mathcal{F}(P_i)$ for $i \geq 0$. The *ith left-derived functor* of $\mathcal{F}$ is the functor that associates to M the homology module $H_i(\mathcal{F}(P_\bullet))$.

The *ith right-derived functor* of a (covariant or contravariant) left-exact functor is similarly defined and is left to the reader.

For this definition to make sense, one has to prove that it is independent of the choice of the projective resolution of M. At this point, one realizes that, for the proof, one needs an additional property of $\mathcal{F}$. First, recall that as a functor $\mathcal{F}$ acts on homomorphisms as well. One says that $\mathcal{F}$ is *additive* if it preserves sums in the sense that if $\varphi, \psi : M \to N$ are module homomorphism, then $\mathcal{F}(\varphi + \psi) = \mathcal{F}(\varphi) + \mathcal{F}(\psi) : \mathcal{F}(M) \to \mathcal{F}(N)$.

At first sight, it is hardly believable that for any given functor with those properties, the above definition is well posed. The gist of this fact is that the independence of the chosen projective resolution can be taken as one of the items of an axiomatic approach to derived functors. Although no such approach will be followed here, one now argues on this independence. The following result is at the core of this problem.

Lemma 6.2.47. *Let $P_\bullet$ and $P'_\bullet$ stand for projective resolutions of an R-module M. Any two chain maps $\mathbf{f} : P_\bullet \to P'_\bullet$ and $\mathbf{g} : P_\bullet \to P'_\bullet$ lifting the identity map on M are homotopic.*

Proof. Clearly, the difference chain map $\mathbf{f} - \mathbf{g}$ lifts the zero map of M. Therefore, it suffices to show that if a chain map $\mathbf{z} : P_\bullet \to P'_\bullet$ lifts the zero map on M then it is homotopic to the zero chain map.

One inducts on $i \geq 0$. By hypothesis, $z_0 : P_0 \to P'_0$ lifts the zero map

$$M = \operatorname{coker}(P_1 \xrightarrow{\varphi_1} P_0) \longrightarrow N = \operatorname{coker}(P'_1 \xrightarrow{\varphi'_1} P'_0),$$

hence $z_0(P_0) \subset \operatorname{Im}(\varphi'_1)$. Then there is a lifting $h_0 : P_0 \to P'_1$ such that $z_0 = \varphi'_1 \circ h_0$. This gives the zeroth step of the required homotopy $\mathbf{h}$ such that $z_i = h_{i-1} \circ \varphi_i + \varphi'_{i+1} \circ h_i$ for every $i \geq 0$. Suppose that $h_i : P_i \to P'_{i+1}$ has been determined so that $z_j = h_{j-1} \circ \varphi_j + \varphi'_{j+1} \circ h_j$, for every $j \leq i$:

$$\begin{array}{ccccccc} & & P_{i+1} & \xrightarrow{\varphi_{i+1}} & P_i & \xrightarrow{\varphi_i} & P_{i-1} \\ & \overset{?}{\swarrow} & \downarrow{\scriptstyle z_{i+1}} & \overset{h_i}{\swarrow} & \downarrow{\scriptstyle z_i} & \overset{h_{i-1}}{\swarrow} & \\ P'_{i+2} & \xrightarrow{\varphi'_{i+2}} & P'_{i+1} & \xrightarrow{\varphi'_{i+1}} & P'_i & & \end{array} \tag{6.2.47.1}$$

Consider the map $h_i \circ \varphi_{i+1} - z_{i+1} : P_{i+1} \to P'_{i+1}$. One has

$$\begin{aligned} \varphi'_{i+1} \circ (h_i \circ \varphi_{i+1} - z_{i+1}) &= (z_i - h_{i-1} \circ \varphi_i) \circ \varphi_{i+1} - \varphi'_{i+1} \circ z_{i+1} \\ &= -h_{i-1} \circ \varphi_i \circ \varphi_{i+1} + (z_i \circ \varphi_{i+1} - \varphi'_{i+1} \circ z_{i+1}) \\ &= 0 + 0 = 0. \end{aligned}$$

This shows that $h_i \circ \varphi_{i+1} - z_{i+1}$ maps P_{i+1} into $\ker \varphi'_{i+1} = \mathrm{Im}(\varphi'_{i+2})$. Since P_{i+1} is projective, this map lifts to a map $l : P_{i+1} \to P'_{i+2}$ such that $\varphi'_{i+2} \circ l = h_i \circ \varphi_{i+1} - z_{i+1}$. Now take $h_{i+1} = -l$ to establish the structural equation of homotopy in step $i+1$. □

Proposition 6.2.48. *Let $\mathcal{F}$ denote a covariant additive right-exact functor of R-modules and let M stand for an R-module. Let $P_\bullet$ and $P'_\bullet$ stand for projective resolutions of M. Then for every $i \geq 0$ there is a natural isomorphism $H_i(\mathcal{F}(P_\bullet)) \simeq H_i(\mathcal{F}(P'_\bullet))$.*

Proof. Any chain map $\mathbf{f} : P_\bullet \to P'_\bullet$ induces a chain map $\mathcal{F}(\mathbf{f}) : \mathcal{F}(P_\bullet) \to \mathcal{F}(P'_\bullet)$, and hence there are module homomorphisms $H_i(\mathcal{F}(\mathbf{f})) : H_i(\mathcal{F}(P_\bullet)) \to H_i(\mathcal{F}(P'_\bullet))$ at the level of homology. The goal is to show that these maps are isomorphisms and, in addition, they are independent of the choice of $\mathbf{f}$ to get them.

Claim 1 (Isomorphism). For any choice of $\mathbf{f}$ lifting the identity map of M, the map $H_i(\mathcal{F}(\mathbf{f}))$ is an isomorphism.

For this, choose any chain map $\mathbf{f}' : P'_\bullet \to P_\bullet$ in the reverse direction lifting the identity map of M. Take the composite chain map $\mathbf{f}' \circ \mathbf{f} : P_\bullet \to P_\bullet$ and compare with the identity chain map $\mathbb{I}$ of $P_\bullet$. By Lemma 6.2.47, they are homotopic to each other, hence $H_i(\mathbf{f}' \circ \mathbf{f})$ and $H_i(\mathbb{I})$ are the same map by Proposition 6.2.45. But $H_i(\mathbf{f}' \circ \mathbf{f}) = H_i(\mathbf{f}') \circ H_i(\mathbf{f})$, hence $H_i(\mathbf{f})$ is an isomorphism.

Claim 2 (Naturality). For every $i \geq 0$, the map $H_i(\mathcal{F}(\mathbf{f}))$ is independent of the choice of $\mathbf{f}$, *i. e.*, the maps $H_i(\mathcal{F}(\mathbf{f}))$ and $H_i(\mathcal{F}(\mathbf{g}))$ coincide for any two chain maps $\mathbf{f} : P_\bullet \to P'_\bullet$ and $\mathbf{g} : P_\bullet \to P'_\bullet$.

By Claim 1, $\mathbf{f}$ and $\mathbf{g}$ are homotopic. Let us write this fact in the following symbolic way $\mathbf{f} - \mathbf{g} = \mathbf{h} \circ \boldsymbol{\varphi} + \boldsymbol{\varphi}' \circ \mathbf{h}$. Applying the additive functor $\mathcal{F}$, one gets $\mathcal{F}(\mathbf{f}) - \mathcal{F}(\mathbf{g}) = \mathcal{F}(\mathbf{h}) \circ \mathcal{F}(\boldsymbol{\varphi}) + \mathcal{F}(\boldsymbol{\varphi}') \circ \mathcal{F}(\mathbf{h})$, thus yielding a homotopy between the chain maps $\mathcal{F}(\mathbf{f})$ and $\mathcal{F}(\mathbf{g})$. Now apply Proposition 6.2.45 to derive that they are the same at the homology level. □

As a matter of notation, since the definition of the ith left-derived functor is independent of the choice of a projective resolution, one might for simplicity denote it by $L\mathcal{F}_i := H_i(\mathcal{F}(P_\bullet))$, where L stands for "left."

Remark 6.2.49. An entirely similar result such as the last proposition holds for a (contravariant) additive left-exact functor, with cohomology instead of homology. In this case, the notation would be $R\mathcal{F}^i := H^i(\mathcal{F}(P_\bullet))$.

The last topic of these general preliminaries explains the relation between short exact sequences of modules and derived functors.

Proposition 6.2.50 (Long exact sequence of derived functors). *Let there be given an exact sequence $0 \to M' \xrightarrow{\iota} M \xrightarrow{\pi} M'' \to 0$ of R-modules and a covariant additive right-exact functor of modules $\mathcal{F}$. Then there is an induced long exact sequence of left*

derived functors

$$\begin{aligned}\cdots \to L\mathcal{F}_i(M') &\xrightarrow{L\mathcal{F}_i(\iota)} L\mathcal{F}_i(M) \xrightarrow{L\mathcal{F}_i(\pi)} L\mathcal{F}_i(M'')\\ &\xrightarrow{\delta_i} L\mathcal{F}_{i-1}(M') \xrightarrow{L\mathcal{F}_{i-1}(\iota)} L\mathcal{F}_{i-1}(M) \xrightarrow{L\mathcal{F}_{i-1}(\pi)} L\mathcal{F}_{i-1}(M'')\\ &\xrightarrow{\delta_{i-1}} \cdots \xrightarrow{\delta_1} L\mathcal{F}_1(M'') \longrightarrow \mathcal{F}(M') \xrightarrow{\mathcal{F}(\iota)} \mathcal{F}(M) \xrightarrow{\mathcal{F}(\pi)} \mathcal{F}(M'') \to 0.\end{aligned}$$

Proof. Take "simultaneous" (vertical) projective resolutions of M', M, M'' as done in the proof of Lemma 6.2.14:

$$\begin{array}{ccccccccc} 0 & \to & P'_\bullet & \longrightarrow & P_\bullet & \longrightarrow & P''_\bullet & \to & 0\\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & M' & \xrightarrow{\iota} & M & \xrightarrow{\pi} & M'' & \to & 0\\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array} \tag{6.2.50.1}$$

Note that the top row is a split exact sequence of complexes. Therefore, applying $\mathcal{F}$ to all of its terms gives an exact sequence of (vertical) complexes. Then the long exact sequence follows from Proposition 6.2.38 and the fact that $L\mathcal{F}_0 = \mathcal{F}$. □

Corollary 6.2.51 ("Décalage"). *Let $0 \to Z \longrightarrow P \longrightarrow M \to 0$ denote an exact sequence of R-modules, with P projective, and let $\mathcal{F}$ denote an additive right-exact functor of modules. Then there is an exact sequence*

$$0 \to L\mathcal{F}_1(N) \longrightarrow \mathcal{F}(Z) \longrightarrow \mathcal{F}(P) \longrightarrow \mathcal{F}(M) \to 0$$

and, moreover, $L\mathcal{F}_i(Z) = L\mathcal{F}_{i+1}(M)$, for $i \geq 1$.

Proof. Since P is projective, $L\mathcal{F}_i(P) = 0$, for $i \geq 1$. Then the result is a straightforward consequence of the above proposition. □

Entirely similar results to Proposition 6.2.50 and its corollary are established for right-derived functors of additive contravariant left-exact functors.

This is as much as will be devoted to the preliminaries of left-derived functors.

The subsequent parts will deal with the details of two fundamental examples, informally known as the Tor and the Ext functors.

6.2.4.1 Tor

For a fixed R-module N the (right) tensor functor $\mathcal{T}_N = \_ \otimes_R N$ is a covariant additive functor of R-modules and it is easy to verify that it is right-exact.

One sets $\mathrm{Tor}_i^R(M,N) := (L\mathcal{T}_N)_i(M)$, for $i \geq 0$. Often the superscript will be omitted if the ground ring is clear from the context.

The notation was introduced in [32], but is not an acronym for "tensor on (the) right," having to do more with the idea of torsion. The following elementary situation suggests this: let $a \in R$ denote a regular element and let N stand for an R-module. Then

$$\operatorname{Tor}_i^R(R/(a), N) = \begin{cases} N/aN & \text{if } i = 0 \\ 0 :_N a & \text{if } i = 1 \\ 0 & \text{if } i \geq 2, \end{cases} \tag{6.2.51.1}$$

as one easily verifies. Since $\operatorname{hd}_R R/(a) = 1$, one may naturally ask if this is related to having $\operatorname{Tor}_i^R(R/(a), N) = 0$, for every $i \geq 1$ and every R-module N. Indeed, this is the case in a pretty general situation, as one will soon see.

Similarly, fixing an R-module M, the (left) tensor functor ${}_M\mathcal{T} = M \otimes_R \_$ is a covariant additive right exact functor and one defines $\operatorname{Tor}_i^R(N, M) := (L_M\mathcal{T})_i(N)$.

The notation is slightly cumbersome to distinguish the two versions. It is natural to ask if one can get rid of this inconvenience. Note that the first version is defined by taking a projective resolution of the left "variable" M, while the second version is defined by taking a projective resolution of the right "variable" N.

The answer is the most spectacular basic property of Tor, its "commutativity," in the following sense.

Proposition 6.2.52. *For any two R-modules M, N, one has an isomorphism*

$$\operatorname{Tor}_i^R(M, N) \simeq \operatorname{Tor}_i^R(N, M).$$

Proof. Let $P_\bullet \xrightarrow{\boldsymbol{\varphi}} M \to 0$ and $Q_\bullet \xrightarrow{\boldsymbol{\psi}} N \to 0$ stand for projective resolutions of M and N, respectively. For any $r \geq 0$, P_r is projective, hence the complex $P_r \otimes_R Q_\bullet$ is acyclic, *i. e.*, $H_s(P_r \otimes_R Q_\bullet) = 0$ for $s \geq 1$, while $H_0(P_r \otimes_R Q_\bullet) = P_r \otimes_R N$.

Similarly, for any $s \geq 0$, $H_r(P_\bullet \otimes_R Q_s) = 0$ for $r \geq 1$ and $H_0(P_\bullet \otimes_R Q_s) = M \otimes_R Q_s$.

Now consider the full double complex $P_\bullet \otimes_R Q_\bullet$ and, for $n \geq 0$, define a homomorphism of modules $\pi_n : \operatorname{Tot}(P_\bullet \otimes_R Q_\bullet)_n \to (P_\bullet \otimes_R N)_n$ by setting

$$\pi_n(p_0 \otimes q_n, p_1 \otimes q_{n-1}, \ldots, p_n \otimes q_0) := (1_{P_n} \otimes \psi_0)(p_n \otimes q_0) = p_n \otimes \psi_0(q_0),$$

where $p_i \in P_i$, $q_{n-i} \in Q_{n-i}$. This is well-defined by the universal property of the tensor product of modules. It is routine to check that the following square is a commutative diagram of maps

$$\begin{array}{ccc} \operatorname{Tot}(P_\bullet \otimes_R Q_\bullet)_n & \xrightarrow{\tau_n} & \operatorname{Tot}(P_\bullet \otimes_R Q_\bullet)_{n-1} \\ \pi_n \downarrow & & \pi_{n-1} \downarrow \\ (P_\bullet \otimes_R N)_n & \xrightarrow{\varphi_n \otimes 1_N} & (P_\bullet \otimes_R N)_{n-1} \end{array} \tag{6.2.52.1}$$

where τ_n is the differential of the total complex as derived from the corresponding double complex, thus yielding a morphism of complexes $\boldsymbol{\pi} : \operatorname{Tot}(P_\bullet \otimes_R Q_\bullet) \to P_\bullet \otimes_R N$.

Claim. For each $n \geq 0$, the map π_n induces an isomorphism in homology

$$H_n(\boldsymbol{\pi}) : H_n(\mathrm{Tot}(P_\bullet \otimes_R Q_\bullet)) \simeq H_n(P_\bullet \otimes_R N).$$

For surjectivity, given $\mathfrak{z}_n \in \ker(\varphi_n \otimes 1_N) \subset (P_\bullet \otimes_R N)_n = P_n \otimes N$ lift to $\mathfrak{p}_{n,0} \in P_n \otimes Q_0$ such that $(1_{P_n} \otimes \psi_0)(\mathfrak{p}_{n,0}) = \mathfrak{z}_n$. Now, $(1_{P_n} \otimes \psi_0)((\varphi_n \otimes 1_N)(\mathfrak{z}_n)) = (1_{P_n} \otimes \psi_0)(0) = 0 \in P_{n-1} \otimes Q_0$. Since $P_n \otimes Q_\bullet$ is acyclic, there exists an element $\mathfrak{p}_{n-1,1} \in P_{n-1} \otimes Q_1$ such that $(1_{P_{n-1}} \otimes \psi_1)(\mathfrak{p}_{n-1,1}) = (\varphi_n \otimes 1_N)(\mathfrak{z}_n) = 0 \in P_{n-1} \otimes Q_0$. Then, using the commutative squares in the double complex $P_\bullet \otimes Q_\bullet$, one gets

$$(1_{P_{n-2}} \otimes \psi_1) \circ (\varphi_{n-1} \otimes 1_{Q_1})(\mathfrak{p}_{n-1,1}) = (\varphi_{n-1} \otimes Q_0) \circ (1_{P_{n-1}} \otimes \psi_1)(\mathfrak{p}_{n-1,1}) = 0.$$

Therefore, there exists $\mathfrak{p}_{n-2,2} \in P_{n-2} \otimes Q_2$ such that

$$(1_{P_{n-2}} \otimes \psi_2)(\mathfrak{p}_{n-2,2}) = (\varphi_{n-1} \otimes 1_{Q_1})(\mathfrak{p}_{n-1,1}).$$

Iterating, one finds $\mathfrak{p}_{n-i,i} \in P_{n-i} \otimes Q_i$, for all $0 \leq i \leq n$, such that

$$(1_{P_{n-(i+1)}} \otimes \psi_{i+1})(\mathfrak{p}_{n-(i+1),i+1}) = (\varphi_{n-i} \otimes 1_{Q_i})(\mathfrak{p}_{n-i,i}).$$

It follows that $\tau_n(\mathfrak{p}) = 0$, where

$$\mathfrak{p} = (\pm\mathfrak{p}_{0,n}, \ldots, \pm\mathfrak{p}_{n,0}) \in \mathrm{Tot}(P_\bullet \otimes_R Q_\bullet)_n,$$

with suitable signs to comply with the definition of τ_n, and by construction, the residue class of $\mathfrak{p}$ in $H_n(\mathrm{Tot}(P_\bullet \otimes_R Q_\bullet))$ maps to the residue class of $\mathfrak{z}_n$ in $H_n(P_\bullet \otimes_R N)$.

Injectivity is shown similarly by conveniently reversing the above argument, and is left to the reader.

So much for the claim. By an obvious symmetry, one deduces an isomorphism $H_n(P_\bullet \otimes_R N) \simeq H_n(M \otimes_R Q_\bullet)$. This proves the statement. □

Remark 6.2.53. It is not entirely trivial to make explicit the isomorphism in the above proposition in a concrete case, even in simple situations. For example, take (6.2.51.1). There one computed $\mathrm{Tor}_1^R(R/(a), N) \simeq 0 :_N a$ by taking the free resolution $0 \to R \xrightarrow{\cdot a} R \longrightarrow R/(a) \to 0$. If one takes a projective resolution of N instead, then one finds that $\mathrm{Tor}_1^R(R/(a), N) \simeq Z \cap aP/aZ$, where $0 \to Z \longrightarrow P \longrightarrow N \to 0$ is a projective presentation of N. Unraveling the isomorphism in the above proposition might lead one to the following map $\iota : 0 :_N a \to Z \cap aP/aZ$ that sends an element $x \in 0 :_N a$ to the residue class of $a\mathfrak{p}$, where $\mathfrak{p} \in P$ is any preimage of x. One can show directly that ι is a (well-defined) isomorphism.

For the reader's convenience, one repeats the contents of Corollary 6.2.51 in the case of Tor.

Proposition 6.2.54 (Décalage of Tor). *Let* $0 \to Z \longrightarrow P \longrightarrow M \to 0$ *stand for an exact sequence of R-modules, with P projective and let N denote an R-module. Then there is an exact sequence*

$$0 \to \operatorname{Tor}_1^R(M,N) \longrightarrow Z \otimes_R N \longrightarrow P \otimes_R N \longrightarrow M \otimes_R N \to 0$$

and, moreover, $\operatorname{Tor}_i^R(Z,N) \simeq \operatorname{Tor}_{i+1}^R(M,N)$*, for* $i \geq 1$.

Example 6.2.55. A good concrete case to have in mind is the double information that stems out of taking an ideal $N = I \subset R$ and $M = R/I$. One has $\operatorname{Tor}_1^R(R/I,I) \simeq \ker(I \otimes_R I \twoheadrightarrow I^2) \simeq Z \cap IF/IF$, where $0 \to Z \longrightarrow F \longrightarrow I \to 0$ is a free presentation of I. One will come back to this example in a later section.

Vanishing properties of Tor

By definition, if M is a projective module over a ring R, then $\operatorname{Tor}_i^R(M,N) = 0$ for every $i \geq 1$ and every R-module N. A natural question arises as to whether the converse holds. The answer is negative in full generality, so one takes the easy way out by introducing the following notion.

Definition 6.2.56. An R-module M is *flat* if for any R-module M' and any submodule $M'' \subset M'$, the induced map $M'' \otimes_R M \to M' \otimes_R M$ is injective.

Equivalently, M is flat if the tensor functor $\mathcal{T}_M = \_ \otimes_R M$ is left-exact. The simplest example of a flat module is a projective module, as one can reduce to the case of a free module (also by Proposition 6.2.57 below).

This module-theoretic notion turns out to be unexpectedly useful in the following form: an R-algebra S is said to be an *R-flat algebra* if it is R-flat as an R-module.

This concept and its terminology are due to Serre ([137, Annexe, 21]). Bringing them up at this point is a little premature, but is convenient to formalize some properties related to Tor. The concept has become an essential tool to deal with families of varieties in algebraic geometry. In commutative algebra it plays a stricter role controlled by the query as to when certain R-algebras S are flat. The interest herein lies in the case where S is finitely generated as an algebra, but not as a module; for a thorough discussion, see [160, Section 2.6].

Of course, one has the following easy result as "la raison d'être" of flat modules.

Proposition 6.2.57. *The following conditions are equivalent for an R-module N:*

(i) *M is flat.*

(ii) $\operatorname{Tor}_i^R(M,N) = 0$ *for every* $i \geq 1$ *and every R-module N.*

(iii) $\operatorname{Tor}_1^R(M,N) = 0$ *for every R-module N.*

Proof. (i) ⇒ (ii) Given a projective resolution $(P_\bullet, \boldsymbol{\varphi}_\bullet)$ of N, break it up into its short exact sequences $0 \to \ker \varphi_i \longrightarrow P_i \longrightarrow \operatorname{Im}(\varphi_i) \to 0$, for $i \geq 1$. Tensoring with M on the

left, since M is flat, one gets short exact sequences

$$0 \to M \otimes_R \ker \varphi_i \longrightarrow M \otimes_R P_i \longrightarrow M \otimes_R \operatorname{Im} \varphi_i \to 0$$

for every $i \geq 1$. Thus, $M \otimes_R \operatorname{Im} \varphi_j = \operatorname{Im}(1_M \otimes \varphi_j)$ and $M \otimes_R \ker \varphi_j = \ker(1_M \otimes \varphi_j)$, for all $j \geq 1$. Since $(P_\bullet, \boldsymbol{\varphi}_\bullet)$ is acyclic, then

$$\ker(1_M \otimes \varphi_i) = M \otimes_R \ker \varphi_i = M \otimes_R \operatorname{Im} \varphi_{i+1} = \operatorname{Im}(1_M \otimes \varphi_{i+1}),$$

for every $i \geq 1$.

(ii) $\Rightarrow$ (iii) Obvious.

(iii) $\Rightarrow$ (i) An exact sequence $0 \to M'' \longrightarrow M' \longrightarrow M'/M'' \to 0$, yields the following part of the long exact sequence of Tor:

$$0 = \operatorname{Tor}_1^R(M, M'/M'') \longrightarrow M \otimes_R M'' \longrightarrow M \otimes M' \longrightarrow M \otimes_R (M'/M'') \to 0. \qquad \square$$

Flat modules have many interesting properties. A general source is the book of H. Matsumura ([108]) and the references there. Although the subject will not be pursued at this point, it may be worth listing some of its properties:

F1. (Local criterion) An R-module M is flat if and only if $M_{\mathfrak{m}}$ is flat over $R_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$ of R.

F2. (Ideal criterion) An R-module M is flat if and only if $\operatorname{Tor}_1^R(R/I, M) = 0$ for every finitely generated ideal $I \subset R$. If $(R, \mathfrak{m})$ is a (Noetherian) local ring then an R-module M is flat if and only if $\operatorname{Tor}_1^R(R/\mathfrak{m}, M) = 0$.

F3. (Flat versus projective) If R is Noetherian or a domain, every finitely generated flat R-module is projective; in particular, finitely generated flat modules over a (Noetherian) local ring are free.

There are more precise statements in terms of certain rings of fractions and invariant factors (see, *e. g.*, [56], [158]); however, there is as yet not an exact characterization of a ring R for which all finitely generated flat R-modules are projective.

F4. (Regular sequence criterion) If $(R, \mathfrak{m})$ is a regular local ring and M is an R-module such that a regular system of parameters of R is an M-sequence, then M is flat.

This result admits many generalizations.

F5. (Flat base change of Tor) Let S denote a flat R-algebra and let M, N stand for R-modules. Then

$$\operatorname{Tor}_i^S(M \otimes_R S, N \otimes_R S) \simeq \operatorname{Tor}_i^R(M, N) \otimes_R S,$$

for every $i \geq 0$.

F6. (Fiber criterion for flat algebras (see Proposition 5.1.14)) Let $(R, \mathfrak{m}) \to (S, \mathfrak{n})$ denote a local homomorphism of local rings, with R regular and S Cohen–Macaulay. Then S is R-flat if (and only if) $\dim B = \dim A + \dim B/\mathfrak{m}B$.

This is a typical assumption in the environment of a family in algebraic geometry.

Away from flat world, there are a couple of useful vanishing-like properties of Tor.

Proposition 6.2.58 (Criterion of homological dimension). *Let R denote a Noetherian ring and let M stand for a finitely generated R-module. The following conditions are equivalent for a given integer $n \geq 0$:*

(i) $\mathrm{hd}_R M \leq n$.

(ii) $\mathrm{Tor}_i^R(M, N) = 0$ *for all $i > n$ and for every R-module N.*

(iii) $\mathrm{Tor}_{n+1}^R(M, R/\wp) = 0$ *for every prime ideal $\wp \subset R$.*

(iv) $\mathrm{Tor}_{n+1}^R(M, R/\mathfrak{m}) = 0$ *for every maximal ideal $\mathfrak{m} \subset R$.*

Proof. By localizing (drawing upon property F5 above), one can reduce to the local case after proving the following formula.

Claim. $\mathrm{hd}_R M = \sup\{\mathrm{hd}_{R_\mathfrak{m}} M_\mathfrak{m} \mid \mathfrak{m} \subset R \text{ maximal}\}$.

To prove the claim, the inequality $\mathrm{hd}_R M \geq \mathrm{hd}_{R_\mathfrak{m}} M_\mathfrak{m}$ is obvious from the definitions, so it suffices to show that $\mathrm{hd}_R M \leq \sup\{\mathrm{hd}_{R_\mathfrak{m}} M_\mathfrak{m} \mid \mathfrak{m} \subset R \text{ maximal}\}$. For that, one may assume that the right side is finite, otherwise there is nothing to prove. Thus, let the supremum be attained at a maximal ideal $\mathfrak{m} \subset R$, say, $\mathrm{hd}_{R_\mathfrak{m}} M_\mathfrak{m} = n < \infty$. Since M is finitely generated and R is Noetherian, M admits a projective (even free) resolution $P_\bullet$ whose terms are finitely generated. Consider the syzygy module $Z := \ker(P_n \to P_{n-1})$. By the principle observed in Remark 6.2.11, $Z_\mathfrak{m}$ is projective over $R_\mathfrak{m}$ (actually, free). For any other maximal ideal $\mathfrak{n} \subset R$, one has $\mathrm{hd}_{R_\mathfrak{n}} M_\mathfrak{n} \leq \mathrm{hd}_{R_\mathfrak{m}} M_\mathfrak{m}$, hence for even more reason $Z_\mathfrak{n}$ is projective over $R_\mathfrak{n}$. Therefore, Z is locally everywhere free at maximal ideals, hence is projective over R by Corollary 6.2.6. Therefore, $\mathrm{hd}_R M \leq n$, as required.

So much for the claim. Thus, one can and will now assume that $(R, \mathfrak{m})$ is a local ring.

The implication (i) $\Rightarrow$ (ii) is clear by taking a free resolution of M of length n.

The implications (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) are obvious, so it remains to show that (iv) $\Rightarrow$ (i). For that, take a free resolution $F_\bullet$ of M with finitely generated terms. By Proposition 6.2.54, one has $\mathrm{Tor}_{n+1}^R(M, R/\mathfrak{m}) = \mathrm{Tor}_1^R(Z_n, R/\mathfrak{m})$, where $Z_n := \ker(F_n \to F_{n-1})$. Let $0 \to Z \longrightarrow F \longrightarrow Z_n \to 0$ stand for a minimal free presentation of Z_n. Applying the second statement of Proposition 6.2.54 to this exact sequence yields an exact sequence

$$0 \to \mathrm{Tor}_1(Z_n, R/\mathfrak{m}) \longrightarrow Z/\mathfrak{m}Z \longrightarrow F/\mathfrak{m}F \longrightarrow Z_n/\mathfrak{m}Z_n \to 0.$$

Since the map $Z/\mathfrak{m}Z \longrightarrow F/\mathfrak{m}F$ is the zero map (because $Z \subset \mathfrak{m}F$ by construction) and $\operatorname{Tor}_1^R(Z_n, R/\mathfrak{m}) = 0$, one has $Z/\mathfrak{m}Z = 0$. By Nakayama, $Z = 0$, and hence $Z_n \simeq F$ is free. □

Note that in the local case the above criterion depends on checking only at the maximal ideal. One can emphasize the local case once more in the following.

Corollary 6.2.59. *Let $(R, \mathfrak{m})$ denote a local ring and let M stand for a finitely generated R-module. Then*
(a) *For any minimal free R-resolution $F_\bullet$ of M, one has*

$$\operatorname{rank} F_i = \dim_{R/\mathfrak{m}} \operatorname{Tor}_i^R(M, R/\mathfrak{m}),$$

for all $i \geq 0$.
(b) $\operatorname{hd}_R M = \sup_i\{\operatorname{Tor}_i^R(M, R/\mathfrak{m}) \neq 0\}$.

Proof. (a) This is evident since tensoring $F_\bullet$ with $R/\mathfrak{m}$ over R yields a complex with zero maps.

(b) This follows from (a) or from the previous proposition. □

Definition 6.2.60. Let $(R, \mathfrak{m})$ denote a local ring and let M stand for a finitely generated R-module with minimal free R-resolution $F_\bullet$. The ith *Betti number* of M is the integer $\operatorname{rank} F_i$. Note that by the above corollary this is an invariant of M.

Perfection and grade sensitivity

For the next result, one needs the following concept.

Definition 6.2.61. Let M stand for an R-module. Given an R-module N, one defines the *Tor N-dimension* of M, denoted $\operatorname{Tor\,dim}_N M$, to be the largest integer $i \geq 0$ such that $\operatorname{Tor}_i^R(M, N) \neq 0$; if no such integer exists, one sets $\operatorname{Tor\,dim}_N M = -1$. Clearly, $\operatorname{Tor\,dim}_N M = \operatorname{Tor\,dim}_M N$, so in order to get an invariant of M one defines the *Tor dimension* of M to be

$$\operatorname{Tor\,dim} M := \sup_N\{\operatorname{Tor\,dim}_N M\},$$

where N runs through all R-modules.

The notation $\operatorname{Tor\,dim}_N M$ chosen here is not usually found in the literature; since the first time it has been brought up in [47] it has been given different (unrelated) forms. The object itself is a delicate invariant of the modules M, N. Even if R is Noetherian, if one of these modules is not finitely generated, this invariant may have a bizarre behavior. As an example, let $(R, \mathfrak{m})$ denote a regular local ring of dimension 1, say, $\mathfrak{m} = (a)$ and let $M = R/\mathfrak{m}$ and $N = K/R$, where K is the fraction field of R. Then $\operatorname{Tor}_0^R(M, N) = R/\mathfrak{m} \otimes_R (K/R) = 0$, while $\operatorname{Tor}_1^R(M, N) = 0 :_N a = M \neq 0$ (here N is the so-called injective envelope of M). If R is Noetherian, both M, N are finitely generated

and $\operatorname{hd}_R M < \infty$, the *rigidity conjecture* says that such a phenomenon is impossible. A propos of this setup, one has the following curious interpretation of $\operatorname{Tor}\dim_N M$.

Proposition 6.2.62 ([87]). *Let $(R, \mathfrak{m})$ denote a Noetherian local ring and let M, N stand for finitely generated R-modules with $\operatorname{hd}_R M < \infty$. Then*

$$\operatorname{Tor}\dim_N M = \sup\{\operatorname{hd}_{R_\wp} M_\wp - \operatorname{depth}_{\wp_\wp} N_\wp \mid \wp \in \operatorname{supp} M_\wp \cap \operatorname{supp} N_\wp\}.$$

Note that this generalizes the Auslander–Buchsbaum formula in Theorem 6.2.19, which is the case where $N = R/\mathfrak{m}$ by using Proposition 6.2.58. The proof of the above proposition will not be given as it extrapolates the objectives of the book. In any case, one will not have occasion to use it throughout.

On the other hand, $\operatorname{Tor}\dim M$ is a more pliable invariant. Thus, *e. g.*, if R is Noetherian and M is finitely generated, and if in addition $\operatorname{hd}_R M < \infty$ then Proposition 6.2.58 implies that $\operatorname{Tor}\dim M = \operatorname{hd}_R M$.

One sees that juggling between finite generation and nonfinite generation is a rather complicated matter (for more on this, see History below).

The following result is a facilitated version of a theorem of Eagon–Northcott ([47, Theorem 3]) and M. Hochster ([74, Theorem 1]).

Proposition 6.2.63. *Let $R \to S$ be a homomorphism of Noetherian rings, let M denote a finitely generated R-module and let N stand for any S-module. Then*

$$\operatorname{Tor}\dim_N M + \operatorname{depth}_{(0:M)S} N \leq \operatorname{hd}_R M,$$

where N is considered as an R-module via $R \to S$.

Proof. It suffices to show that if $\{a_1, \ldots, a_n\} \subset (0 : M)S$ is an N-sequence then

$$\operatorname{Tor}\dim_N M + n \leq \operatorname{hd}_R M.$$

One inducts on n.

For $n = 0$, the result follows from Proposition 6.2.58.

If $n > 0$, consider the exact sequence $0 \to N \xrightarrow{\cdot a} N \longrightarrow N/aN \to 0$, where $a := a_1$ and look at the associated long exact sequence of Tor:

$$\begin{aligned}\cdots \longrightarrow \operatorname{Tor}_i^R(M,N) \longrightarrow \operatorname{Tor}_i^R(M,N) \longrightarrow \operatorname{Tor}_i^R(M,N/aN) \longrightarrow \\ \longrightarrow \operatorname{Tor}_{i-1}^R(M,N) \longrightarrow \operatorname{Tor}_{i-1}^R(M,N) \longrightarrow \operatorname{Tor}_{i-1}^R(M,N/aN) \longrightarrow \cdots\end{aligned}$$

One claims that $\operatorname{Tor}_i^R(M,N) \longrightarrow \operatorname{Tor}_i^R(M,N)$ is the null map for every i. Let h denote the structural homomorphism $R \to S$. Since $a \in (0 :_R M)S$ is a sum of elements of the form $h(b)s$, with $b \in 0 :_R M$, $s \in S$, then it suffices to show that for any $a \in 0 :_R M$, one has $h(a) \in 0 :_S \operatorname{Tor}_i^R(M,N)$, for every $i \geq 0$, where $\operatorname{Tor}_i^R(M,N)$ is considered as S-module by the natural structure induced by the fact that N is an S-module. In other words, one needs to prove that, for every $i \geq 0$, the localization

$$\operatorname{Tor}_i^R(M,N)_{h(a)} = H_i(P_\bullet \otimes_R N) \otimes_S S_{h(a)} = H_i(P_\bullet \otimes_R N \otimes_S S_{h(a)})$$

vanishes, where $P_\bullet$ denotes a projective resolution of M over R.

But $P_\bullet \otimes_R N \otimes_S S_{h(a)} = P_\bullet \otimes_R N \otimes_S (R_a \otimes_R S) = (P_\bullet \otimes_R R_a) \otimes_R N$, hence $\operatorname{Tor}_i^R(M,N)_{h(a)} = H_i((P_\bullet \otimes_R R_a) \otimes_R N)$. On the other hand, $P_\bullet \otimes_R R_a$ is a projective resolution of $M_a = 0$. Therefore, $\operatorname{Tor}_i^R(M,N)_{h(a)} = 0$.

As a consequence, one has short exact sequences

$$0 \to \operatorname{Tor}_i^R(M,N) \longrightarrow \operatorname{Tor}_i^R(M,N/aN) \longrightarrow \operatorname{Tor}_{i-1}^R(M,N) \to 0,$$

for all i. In particular, setting $d := \operatorname{Tor\,dim}_N M$, one has $\operatorname{Tor}_{d+1}^R(M,N) = 0$, and hence

$$\operatorname{Tor}_{d+1}^R(M,N/aN) = \operatorname{Tor}_d^R(M,N) \neq 0.$$

By the same token, one sees that $\operatorname{Tor}_i^R(M,N/aN) = 0$ for every $i > d+1$. Applying the inductive hypothesis with N replaced by N/aN, gives $d - n = d + 1 - (n-1) \leq \operatorname{hd}_R M$, as required. □

A special case of the above is important enough: N is an R-algebra S and $M = R/I$, for some ideal $I \subset R$. In this setup, one has the following consequence.

Proposition 6.2.64 (Stability of perfection). *Let $R \longrightarrow S$ be a homomorphism of Noetherian rings and let $I \subset R$ denote an ideal such that $IS \neq S$. If R/I is perfect and $\operatorname{depth}_{IS} S \geq \operatorname{depth}_I R$, then S/IS is perfect and $\operatorname{hd}_S S/IS = \operatorname{hd}_R I$.*

Proof. By Proposition 6.2.63, $\operatorname{Tor\,dim}_S R/I + \operatorname{depth}_{IS} S \leq \operatorname{hd}_R R/I$, while by assumption $\operatorname{depth}_{IS} S \geq \operatorname{depth}_I R = \operatorname{hd}_R I$. This forces $\operatorname{Tor\,dim}_S R/I = 0$, hence any projective R-resolution $P_\bullet \to R/I \to 0$ induces a projective S-resolution $P_\bullet \otimes_R S \to S/IS \to 0$. This gives $\operatorname{hd}_S S/IS \leq \operatorname{hd}_R I \leq \operatorname{depth}_{IS} S$. On the other hand, one always has $\operatorname{depth}_{IS} S \leq \operatorname{hd}_S S/IS$ by Corollary 6.2.26. Therefore, $\operatorname{depth}_{IS} S = \operatorname{hd}_S S/IS = \operatorname{hd}_R I$, as was to be shown. □

More properties of perfect modules will be given in Section 6.2.5.

6.2.4.2 Ext

This functor can be introduced in (at least) three apparently different ways. Eventually, any of these alternatives turns out to be equivalent to each other, but none of these equivalences is trivially verified.

In this book, one will settle for the details of one among these alternatives. Alas, all three are useful. Thus, one may possibly be lead to draw upon some of the properties which may be easier to establish via the other two alternatives.

Ext via projective resolutions

This choice here is coherent with the guideline so far of obtaining derived functors using projective resolutions. Consider the homomorphism functor $\operatorname{Hom}_R(\_, N)$ associated to a fixed R-module N. By definition, $\operatorname{Hom}_R(\_, N)(M) = \operatorname{Hom}_R(M,N)$ for any R-module N, while for any homomorphisms $\varphi : M \to M'$ and $f : M' \to N$ one has

$\mathrm{Hom}_R(\_, N)(\varphi) = f \circ \varphi$. It is easy to see that $\mathrm{Hom}_R(\_, N)$ is an additive left-exact contravariant functor. As mentioned before, in a fashion entirely similar to the definition of a left-derived functor of a right-exact covariant functor, one establishes the notion of a right-derived functor of a left-exact contravariant functor.

Definition 6.2.65. The "Ext" functor is the right-derived functor of the "Hom" functor. Precisely, on sets

$$\mathrm{Ext}^i_R(\_, N)(M) := H^i(\mathrm{Hom}(P_\bullet, N)),$$

for $i \geq 0$, where $P_\bullet$ is a projective resolution of M.

Observe the notation H^i with upper index, indicating (co)homology of the (right) complex $0 \to \mathrm{Hom}_R(P_0, N) \to \mathrm{Hom}_R(P_0, N) \to \cdots$.

Throughout, one sets $\mathrm{Ext}^i_R(M, N) := \mathrm{Ext}^i_R(\_, N)(M)$. By Remark 6.2.49, the definition is independent of the chosen projective resolution.

For the reader's convenience, one states the analogues of the long exact sequence in cohomology and of décalage in the case of Ext.

Proposition 6.2.66. *Let $0 \to M' \longrightarrow M \longrightarrow M'' \to 0$ stand for an exact sequence of R-modules and let N denote an R-module. Then there is an induced long exact sequence*

$$\begin{aligned} 0 \;\to\; & \mathrm{Hom}_R(M'', N) \longrightarrow \mathrm{Hom}_R(M, N) \longrightarrow \mathrm{Hom}_R(M', N) \\ \longrightarrow\; & \mathrm{Ext}^1_R(M'', N) \longrightarrow \mathrm{Ext}^1_R(M, N) \longrightarrow \mathrm{Ext}^1_R(M', N) \\ \cdots \longrightarrow\; & \mathrm{Ext}^i_R(M'', N) \longrightarrow \mathrm{Ext}^i_R(M, N) \longrightarrow \mathrm{Ext}^i_R(M', N) \longrightarrow \cdots \end{aligned}$$

In order to state the décalage property of Ext as defined, one needs a characterization of a projective module in terms of Ext.

Lemma 6.2.67. *Let R denote a ring and let M stand for an R-module. The following conditions are equivalent:*
(i) *M is projective.*
(ii) *$\mathrm{Ext}^1_R(M, N) = 0$ for every R-module N.*

Proof. (i) $\Rightarrow$ (ii) This is clear from the definitions since $\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow M$ is a projective resolution of M, and in fact one has $\mathrm{Ext}^i_R(M, N) = 0$ for every $i \geq 1$.

(ii) $\Rightarrow$ (i) The proof is a consequence of the long exact sequence in Proposition 6.2.66. Namely, let $0 \longrightarrow Z \longrightarrow P \longrightarrow M \to 0$ stand for a projective presentation of M. Since in particular $\mathrm{Ext}^1_R(M, Z) = 0$ taking $N := Z$, the map $\mathrm{Hom}(P, Z) \to \mathrm{Hom}(Z, Z)$ is surjective, hence the identity map of Z lifts to a map $P \to Z$, which is then a splitting of the inclusion $Z \subset P$. It follows that the surjective map $P \to M$ splits as well, hence M is projective. □

Corollary 6.2.68 (Décalage of Ext). *Let $0 \longrightarrow Z \longrightarrow P \longrightarrow M \to 0$ stand for a projective presentation of an R-module M and let N denote an R-module. Then there is an exact*

sequence

$$0 \to \mathrm{Hom}(M,N) \longrightarrow \mathrm{Hom}(P,N) \longrightarrow \mathrm{Hom}(Z,N) \longrightarrow \mathrm{Ext}^1_R(M,N) \to 0$$

and $\mathrm{Ext}^i_R(M,N) \simeq \mathrm{Ext}^{i+1}_R(M,N)$, *for all* $i \geq 1$.

The following analogue of Proposition 6.2.58 holds as well.

Proposition 6.2.69. *Let R denote a Noetherian ring and let M stand for a finitely generated R-module. The following conditions are equivalent for a given integer $n \geq 0$:*

(i) $\mathrm{hd}_R M \leq n$.

(ii) $\mathrm{Ext}^i_R(M,N) = 0$ *for all* $i > n$ *and for every finitely generated R-module N.*

(iii) $\mathrm{Ext}^{n+1}_R(M, R/\wp) = 0$ *for every prime ideal* $\wp \subset R$.

Proof. (i) $\Rightarrow$ (ii) follows from the definitions.

Conversely, (ii) $\Rightarrow$ (i) as one now shows. Namely, consider a projective resolution $P_\bullet$ of M, which one breaks into the short exact sequences

$$0 \to \mathrm{Im}(P_{i+1} \to P_i) \longrightarrow P_i \longrightarrow \mathrm{Im}(P_i \to P_{i-1}) \to 0.$$

Applying the second statement of décalage (Corollary 6.2.68) to each one of these short sequences with second variable N, and splicing the results together, one finds that $\mathrm{Ext}^{n+1}_R(M,N) = \mathrm{Ext}^1_R(Z_n,N)$, where $Z_n = \mathrm{Im}(P_n \to P_{n-1})$. Then $\mathrm{Ext}^1_R(Z_n,N) = 0$, hence Z_n is projective by Lemma 6.2.67. □

Obviously, (ii) $\Rightarrow$ (iii). The proof of the reverse implication is not difficult as soon as the alternative definition of Ext in terms of injective resolutions is assumed. The argument is described in Remark 6.2.74. □

As done for Tor regarding finitely generated modules in the local case, one can check projectivity (*i. e.*, freeness) in terms of Ext.

Lemma 6.2.70. *Let $(R,\mathfrak{m})$ denote a Noetherian local ring and let M stand for a finitely generated R-module. Then M is free if and only* $\mathrm{Ext}^1_R(M, R/\mathfrak{m}) = 0$.

Proof. One implication is obvious.

For the other one, set $R/\mathfrak{m} = k$ for emphasis. For any R-module N, there is a natural bijection between R-maps of N to k and k-maps of $N/\mathfrak{m}N$ to k (*i. e.*, the dual k-vector space of the k-vector space $N/\mathfrak{m}N$). This bijection endows $\mathrm{Hom}_R(N,k)$ with a structure of k-vector space and, considering $\mathrm{Hom}_R(N/\mathfrak{m}N,k)$ as an R-module via the residual map $R \twoheadrightarrow k$, yields an R-isomorphism $\mathrm{Hom}_R(N,k) \simeq \mathrm{Hom}_R(N/\mathfrak{m}N,k)$.

Now, let $0 \to Z \longrightarrow F \longrightarrow M \to 0$ stand for a minimal free presentation of M. By Corollary 6.2.68 and the assumption, one has an exact sequence

$$0 \to \mathrm{Hom}_R(M,k) \longrightarrow \mathrm{Hom}_R(F,k) \longrightarrow \mathrm{Hom}_R(Z,k) \to 0.$$

Since the rank of F coincides with $\mu(M)$, the map $\mathrm{Hom}_R(M,k) \longrightarrow \mathrm{Hom}_R(F,k)$ of $\mathfrak{m}$-vector spaces is an isomorphism. Therefore, $\mathrm{Hom}_R(Z,k) = 0$. But since $\mathrm{Hom}_R(Z,k) \simeq \mathrm{Hom}_R(Z/\mathfrak{m}Z,k)$, then clearly $Z/\mathfrak{m}Z = 0$. By the Nakayama lemma, it follows that $Z = 0$, hence $M \simeq F$. □

In the local case, one has the following souped-up version of Proposition 6.2.69.

Proposition 6.2.71. *Let $(R,\mathfrak{m})$ denote a Noetherian local ring and let M stand for a finitely generated R-module. The following conditions are equivalent for a given integer $n \geq 0$:*
(i) $\mathrm{hd}_R M \leq n$.
(iii) $\mathrm{Ext}^{n+1}_R(M, R/\mathfrak{m}) = 0$.

Proof. Induct on n. For $n = 0$, this is the previous lemma.

Assume that $n \geq 1$.

Consider a free resolution $F_\bullet$ of M and set $Z := \ker(F_{n-1} \to F_{n-2})$. By the assumption and decalage as applied to the short exact sequences stemming out of $F_\bullet$, one gets

$$\mathrm{Ext}^1_R(Z, R/\mathfrak{m}) \simeq \mathrm{Ext}^{n+1}_R(M, R/\mathfrak{m}) = 0,$$

hence Z is free by the previous corollary. □

Ext via injective resolutions

One now considers the functor $\mathrm{Hom}(M,\_)$, where M is a fixed R-module. Thus, this is a functor of the "second variable" and, as such it is a covariant functor. Moreover, it is also left-exact. The theory comes in through the notion of injective resolutions (of the second variable for the case on the agenda). Naturally, this presupposes the notion of an injective module. The theory has a high degree of sophistication, so it would be required to dedicate a substantial part of the chapter to fill in all details that are expected in a textbook. Therefore, one will give the main definitions and a few properties enough to follow the contents with no detriment to a full understanding. A reader interested in the full disclosure of the theory is referred to the more specialized literature ([107], [25] and, for the noncommutative case, [49]); see History 6.5.3.

Definition 6.2.72. An R-module N is *injective* if the functor $\mathrm{Hom}(\_,N)$ is right-exact; in other words, if for any injective map $M' \hookrightarrow M$ the induced map $\mathrm{Hom}(M,N) \to \mathrm{Hom}(M',N)$ is surjective.

Next are the most basic properties of injective modules:

$\mathfrak{I}1$. The following assertions are equivalent for an R-module N:
(i_1) N is injective.
(i_2) (Direct summand) Any inclusion $N \subset M$ splits.
(i_3) (Ideal Ext-criterion) $\mathrm{Ext}^1_R(R/J,N) = 0$ for any ideal $J \subset R$.
(i_3) (Module Ext-criterion) $\mathrm{Ext}^1_R(M,N) = 0$ for any R-module M.

ℑ2. (Injective resolutions) Every R-module N admits an *injective resolution*, *i. e.*, a cocomplex

$$I^\bullet : 0 \to I^0 \longrightarrow I^1 \longrightarrow \cdots,$$

whose terms are injective modules, such that $H^0(I^\bullet) = N$ and $H^i(I^\bullet) = 0$ for all $i \geq 1$.

ℑ3. (Minimal injective resolutions) The previous result can be strengthened as follows: every R-module N is contained in an injective module $E(N)$ such that any nonzero submodule of $E(N)$ intersects N properly—such a module is called an *injective hull* of N. One sets $I^0 := E(N)$. Next, one takes $I^1 := E(E(N)/N)$, and so forth thus producing an injective resolution of N of a minimal nature. (This phenomenon is often described by the loose expression saying that "the category of R-modules has enough injectives.") An example is the minimal injective resolution $\mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ of $R = \mathbb{Z}$. Quite often, minimal injective resolutions are infinite.

ℑ4. (Ext by injective resolutions) Let M, N denote R-modules. Then one defines

$$\mathrm{IExt}^i_R(M,N) := H^i(\mathrm{Hom}(M, I^\bullet))$$

for every $i \geq 0$, where $I^\bullet$ stands for an injective resolution of N. These derived functors as applied to short exact sequences $0 \to N' \longrightarrow N \longrightarrow N'' \to 0$ produce analogues of Proposition 6.2.66 and Corollary 6.2.68.

ℑ5. Let M, N denote R-modules. Then $0 : M \subset 0 : \mathrm{IExt}^i_R(M,N)$.

This result is of medium difficulty, depending on properties of the injective hulls used in building up an injective resolution of N.

ℑ6. There are natural module isomorphisms $\mathrm{IExt}^i_R(M,N) \simeq \mathrm{Ext}^i_R(M,N)$, for any R-modules M, N and every $i \geq 0$.

The proof of this result is a lot more difficult than the contents of the previous properties. It became quite standard to prove this important fact using spectral sequences. However, a proof similar to the one in Proposition 6.2.52 is available, namely one takes a projective resolution $P_\bullet$ of M and an injective resolution $I^\bullet$ of N and introduces the double cocomplex of general term $\mathrm{Hom}(P_i, I^j)$ with the obvious maps induced by the differentials of the two resolutions (since homing out each of these resolutions is a cocomplex, so is the result a double cocomplex); then a similar procedure shows that the cohomology of the total cocomplex of this double cocomplex is isomorphic to both versions of Ext. A third proof exists by showing that both alternatives (projectives or injectives) are equivalent to the so-called extension theory of Baer–Yoneda. The latter is beyond the scope of the book; once more, an interested reader is referred to the specialized source literature ([11], [165], [22]); see also History 6.5.3.

ℑ7. (Injective dimension) The *injective dimension* of an R-module M is the minimum length of an injective resolution of M (if there exits one such; otherwise M has infinite injective dimension). There is no universally agreed notation: Serre uses $\mathrm{di}_R M$, while the English version would have $\mathrm{id}_R M$; in [108] and [25] the longer nota-

tion $\operatorname{inj.dim}_R M$ is employed throughout. Another alternative, in the spirit of $\operatorname{hd}_R M$ (homological dimension) would be $\operatorname{cd}_R M$ (cohomological dimension) but, unfortunately, this one has been used in many other contexts.

Here is its characterization in terms of Ext.

Proposition 6.2.73. *The following are equivalent for an R-module N and an integer $n \geq 0$:*

(i) $\operatorname{inj.dim}_R N \leq n$.

(ii) $\operatorname{Ext}_R^{n+1}(M, N) = 0$ *for every R-module M.*

(iii) $\operatorname{Ext}_R^{n+1}(R/J, N) = 0$ *for every ideal $J \subset R$.*

Moreover, if R is Noetherian, one can replace (ii) *by* (ii)$'$*, where an arbitrary R-module M is trade by an arbitrary finitely generated R-module and, in addition, include to the list a fourth equivalent condition:*

(iv) $\operatorname{Ext}_R^{n+1}(R/\wp, N) = 0$ *for every prime ideal $\wp \subset R$.*

Proof. The implications (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) are evident. The proof of the implication (iii) $\Rightarrow$ (i) follows the same pattern as that of (ii) $\Rightarrow$ (i) in Proposition 6.2.69. Finally, to see that (iv) $\Rightarrow$ (ii)$'$ one takes a finite filtration of M by submodules with successive quotients of the form $R/\wp$, $\wp \subset R$ a prime ideal (*cf.* Proposition 5.2.8) and apply the long exact sequence of $\operatorname{Ext}_R(\_, N)$ of (Proposition 6.2.66) upon the resulting short exact sequences of this filtration. □

Remark 6.2.74. By the same token, one can prove the implication (iii) $\Rightarrow$ (ii) of Proposition 6.2.69, using instead the long exact sequence of $\operatorname{Ext}_R(M, \_)$ as mentioned in property $\mathfrak{J}4$.

This result admits the following souped-up version in the local case—a sort of dual characterization of projective dimension in the local case (Corollary 6.2.59 (b)).

Corollary 6.2.75. *Let $(R, \mathfrak{m})$ denote a Noetherian local ring and let N stand for a finitely generated R-module. Then*

$$\operatorname{inj.dim}_R N = \sup_i \{\operatorname{Ext}_R^i(R/\mathfrak{m}, N) \neq 0\}.$$

The proof is more involved than that in the case of projective dimension and Tor because one still has to call upon all prime ideals of R in order to use Proposition 6.2.73. The precise argument is left as a challenging exercise calling upon the Nakayama lemma once and again.

6.2.5 Rees theorem and perfect ideals

Another important use of the long exact sequence of $\operatorname{Ext}_R(M, \_)$ is the next result, used in the characterization of depth in terms of Ext (Corollary 5.3.6).

Proposition 6.2.76 (Rees "décalage" to Hom). *Given R-modules M, N and an N-sequence $\{a_1, \dots, a_n\} \subset R$ contained in the annihilator of M, one has*

$$\begin{cases} \operatorname{Ext}^n_R(M,N) \simeq \operatorname{Hom}_R(M, N/(a_1,\dots,a_n)N) \\ \operatorname{Ext}^i_R(M,N) = \{0\}, \quad 0 \le i \le n-1 \end{cases}$$

Proof. Induct on n. Consider the exact sequence

$$0 \to N \xrightarrow{.a_1} N \to N/a_1N \to 0. \tag{6.2.76.1}$$

By property $\mathfrak{I}5$ above, a_1 annihilates $\operatorname{Ext}^i_R(M,N)$ for all $i \ge 0$. On the other hand, $\operatorname{Ext}^0_R(M,N) = \operatorname{Hom}_R(M,N) = \{0\}$ since a_1 annihilates M and is N-regular. Therefore, from the long exact sequence of $\operatorname{Ext}_R(M,\_)$ induced by (6.2.76.1), there is an isomorphism

$$\operatorname{Hom}_R(M, N/a_1N) \simeq \operatorname{Ext}^1_R(M,N) \tag{6.2.76.2}$$

This shows the contention for $n = 1$. Thus, let $n \ge 2$ and assume that

$$\begin{cases} \operatorname{Ext}^{n-1}_R(M,N) \simeq \operatorname{Hom}_R(M, N/(a_1,\dots,a_{n-1})N) \\ \operatorname{Ext}^i_R(M,N) = \{0\}, \quad 0 \le i \le n-2 \end{cases}$$

By a similar token, a_n annihilates M and is regular on $N/(a_1,\dots,a_{n-1})N$, hence $\operatorname{Hom}_R(M, N/(a_1,\dots,a_{n-1})N) = \{0\}$. Therefore, $\operatorname{Ext}^i_R(M,N) = \{0\}$, $0 \le i \le n-1$. It remains to show that $\operatorname{Ext}^n_R(M,N) \simeq \operatorname{Hom}_R(M, N/(a_1,\dots,a_n)N)$. For this, applying iteratively the long exact sequences induced by each of the exact sequences

$$0 \to N/(a_1,\dots,a_{i-1})N \xrightarrow{.a_i} N/(a_1,\dots,a_{i-1})N \to N/(a_1,\dots,a_i)N \to 0$$

for $i = 0, \dots, n$, and having in account that a_i annihilates all $\operatorname{Ext}_R(M,\_)$, one finds isomorphisms

$$\begin{aligned} \operatorname{Hom}_R(M, N/(a_1,\dots,a_n)N) &\simeq \operatorname{Ext}^1_R(M, N/(a_1,\dots,a_{n-1})N) \\ &\simeq \operatorname{Ext}^2_R(M, N/(a_1,\dots,a_{n-2})N) \\ &\simeq \cdots \simeq \operatorname{Ext}^n_R(M,N), \end{aligned}$$

as was to be shown. □

The following terminology has been introduced for ideals as an alternative to depth (Section 3.3).

Definition 6.2.77. The *grade* of an R-module is the grade of its annihilator.

Note that this is a set theoretic invariant, since the grade of a module and that of the radical of its annihilator coincide.

Drawing upon the above proposition, one sees that the grade of an R-module M is the least integer g such that $\operatorname{Ext}^g_R(M,R) \neq 0$.

Lemma 6.2.78. *Let R be a Noetherian ring and let M denote a finitely generated perfect module of grade g. Then* $\operatorname{Ass}(M) \subset \operatorname{Ass}(\operatorname{Ext}^g_R(M,R))$.

Proof. Let $\mathbf{a} := \{a_1,\dots,a_g\} \subset R$ denote a maximal R-sequence contained in $I := \operatorname{ann}(M)$. Then $\operatorname{Ext}^g_R(M,R) \simeq \operatorname{Hom}(M, R/(\mathbf{a}))$ by Proposition 6.2.76, hence

$$\operatorname{Ass}\big(\operatorname{Ext}^g_R(M,R)\big) = \operatorname{supp} M \cap \operatorname{Ass}\big(R/(\mathbf{a})\big) = \operatorname{Spec} R/I \cap \operatorname{Ass}\big(R/(\mathbf{a})\big)$$

by Proposition 5.2.6(vii).

Let $P \in \operatorname{Ass}(M)$. Since M is perfect, $\operatorname{grade}(P) = \operatorname{grade}(I)$. Therefore, $\mathbf{a}$ is a maximal R-sequence inside P, and hence $P \subset Q$ for some $Q \in \operatorname{Ass}(R/(\mathbf{a})$. Now, for such a prime Q one has

$$g = \operatorname{grade}(Q) = \operatorname{grade}(Q_Q) \geq \operatorname{hd}_{R_Q} M_Q \geq \operatorname{hd}_{R_P} M_P = \operatorname{grade}(P_P).$$

But, since at any rate $\operatorname{hd}_{R_P} R_P/(\mathbf{a})_P = g$, one gets $\operatorname{depth}_{P_P}(R_P/(\mathbf{a})_P) = 0$. Therefore, $P_P \in \operatorname{Ass}(R_P/(\mathbf{a})_P)$, hence $P \in \operatorname{Ass}(R/(\mathbf{a}))$, as required. □

Corollary 6.2.79. *Let R be a Noetherian ring and let M denote a finitely generated perfect R-module of grade g. Then* $\operatorname{Ass}(M) = \operatorname{Ass}(\operatorname{Ext}^g_R(M,R))$.

Proof. By perfectness of M, dualizing a projective resolution of length g of M yields that $\operatorname{Ext}^g_R(M,R)$ is a perfect R-module of grade g and

$$\operatorname{Ext}^g_R\big(\operatorname{Ext}^g_R(M,R),R\big) \simeq M.$$

Then the reverse inclusion $\operatorname{Ass}(\operatorname{Ext}^g_R(M,R)) \subset \operatorname{Ass}(M)$ follows from Lemma 6.2.78 as applied to $\operatorname{Ext}^g_R(M,R)$. □

Theorem 6.2.80 (Rees hypersurface grade theorem). *Let R be a Noetherian ring, let M denote a finitely generated perfect module of grade g. If $a \in R$ is such that* $\operatorname{grade} M/aM \geq g+1$, *then M/aM is a perfect R-module of grade exactly $g+1$.*

Proof. **Claim.** a is a regular element on M.

To see this, let $x \in 0 :_M (a)$ and set $J := \ker(R \xrightarrow{\varphi} M)$, where $\varphi(1) = x$. Then $(0 : M, a) \subset J$. By Proposition 5.1.1, $\operatorname{grade}(0 : M, a) = \operatorname{grade} 0 : M/aM$. But $\operatorname{grade} 0 : M/aM = \operatorname{grade} M/aM \geq g+1$. Therefore, $\operatorname{grade} J \geq g+1 = \operatorname{hd}_R(M)+1$. Thus, Proposition 6.2.76 implies that $\operatorname{Ext}^r_R(R/J,R) = 0$ for every $r \leq g$. Clearly, then $\operatorname{Ext}^r_R(R/J,F) = 0$ for every $r \leq g$ and every free R-module F, and hence, also $\operatorname{Ext}^r_R(R/J,P) = 0$ for every $r \leq g$ and every projective R-module P.

Pick a projective resolution of M of length g:

$$0 \to P_g \longrightarrow P_{g-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow M \to 0. \tag{6.2.80.1}$$

Applying general décalage to the short exact sequences

$$0 \to Z_1 \longrightarrow P_0 \longrightarrow M \to 0 \quad \text{and} \quad 0 \to Z_{i+1} \longrightarrow P_i \longrightarrow Z_i \to 0,$$

with $1 \leq i \leq g-1$, $Z_g = P_g$, extracted from this resolution (see Corollary 6.2.68) will give $\operatorname{Hom}(R/J, M) = 0$. Therefore, $Rx \simeq R/J = \{0\}$, hence $x = 0$, thus proving the claim.

In order to prove that M/aM is perfect, one draws on the mapping cone process, as follows. Write $P_\bullet$ for the acyclic complex of projective modules as in (6.2.80.1). Let $\mathfrak{a} : P_\bullet \to P_\bullet$ denote the chain map induced by multiplication by a. Since $P_\bullet$ is acyclic, this map in an isomorphism at the homology level. Therefore, by Proposition 6.2.41 the resulting mapping cone is acyclic. Moreover, by construction, since a is regular on M, it has M/aM as augmentation. Therefore, it is a projective resolution of M/aM of length $g+1$.

Now, since always $\operatorname{grade} M/aM \leq \operatorname{hd}_R(M/aM)$, then from the assumption it follows that M/aM is perfect of grade $g+1$. □

Corollary 6.2.81 (Vasconcelos). *Let R be a Noetherian ring, $I \subset R$ an ideal and $a \in R$ a regular element modulo I. Then:*
(i) *If* $\operatorname{hd}_R(R/I) < \infty$, *then* $\operatorname{grade}(I, a) \geq \operatorname{grade}(I) + 1$.
(ii) *If I is perfect and* $(I, a) \neq R$, *then* $\operatorname{grade}(I, a) = \operatorname{grade}(I) + 1$.

Proof. Note that, quite naturally, as a consequence of Theorem 6.2.80 with $M = R/I$, (i) implies (ii). Then it would suffice to prove (i). One chooses instead to first prove (ii) and obtain (i) as a consequence.

Thus, by Theorem 6.2.80 with $M = R/I$, hence, $M/aM = R/(I, a)$—it suffices to show the inequality $\operatorname{grade}(I, a) \geq \operatorname{grade}(I) + 1$. Let $\operatorname{grade}(I) = g$. By the assumption on a, one has an exact sequence of R-modules

$$0 \to R/I \xrightarrow{.a} R/I \longrightarrow R/(I, a) \to 0.$$

Since $\operatorname{Ext}^r_R(R/I, R) = 0$ for $r \leq g-1$, one gets an exact sequence

$$0 \to \operatorname{Ext}^g_R(R/(I, a), R) \longrightarrow \operatorname{Ext}^g_R(R/I, R) \xrightarrow{.a} \operatorname{Ext}^g_R(R/I, R). \tag{6.2.81.1}$$

Suppose that $\operatorname{Ext}^g_R(R/(I, a), R) \neq 0$ and let P be an associated prime thereof. By (6.2.81.1), P is an associated prime of $\operatorname{Ext}^g_R(R/I, R)$, hence also an associated prime of R/I by Corollary 6.2.79. Therefore, $a \notin P$, hence $a/1 \in R_P$ is a unit. By localizing (6.2.81.1) at P, the right-most map is an isomorphism, thus implying that $\operatorname{Ext}^g_R(R/(I, a), R)_P = 0$, which is absurd.

Thus, one must have $\operatorname{Ext}^g_R(R/(I, a), R) = 0$, hence $\operatorname{grade}(I, a) \geq g + 1$, as needed.

One now proves (i). With same notation as in the first argument above, suppose that $\operatorname{Ext}_R^g(R/(I,a),R) \neq 0$ and let P be an associated prime thereof.

Claim. I_P is perfect.

To see this, if $\operatorname{grade}(I,a) = g$ then $\operatorname{Ext}_R^g(R/(I,a),R) \simeq \operatorname{Hom}(R/(I,a),R/(\mathbf{a}))$, where $\mathbf{a} \subset (I,a)$ is a maximal R-sequence. But

$$\operatorname{Ass}\big(\operatorname{Hom}(R/(I,a),R/(\mathbf{a}))\big) = \operatorname{Spec} R/(I,a) \cap \operatorname{Ass}\big(R/(\mathbf{a})\big)$$

by Proposition 5.2.6(vii). This implies that $(I,a) \subset P$ and $P \in \operatorname{Ass}(R/(\mathbf{a}))$. Necessarily then $\operatorname{grade} P_P = \operatorname{grade} P = g$, hence also $\operatorname{grade}(I,a)_P = \operatorname{grade}(I,a) = g$. By the Auslander–Buchsbaum formula, one has $\operatorname{hd}_{R_P}(R_P/I_P) \leq \operatorname{grade} P_P = g \leq \operatorname{grade} I_P$. It follows that I_P is perfect, as stated.

By part (ii), one has $\operatorname{grade}(I,a) = \operatorname{grade}(I,a)_P \geq \operatorname{grade} I_P \geq \operatorname{grade} I_P + 1 \geq \operatorname{grade} I + 1 = g + 1$; this is a contradiction. □

6.3 The method of the Koszul complex

The Koszul complex is a basic construct in algebraic topology, first devised by the French mathematician Jean-Louis Koszul. Its importance in commutative algebra originally came from having some sort of universal complex of free modules whose homology would measure how far off is a sequence of elements in a ring from being a regular sequence. In fact, the Koszul complex in its basic form gives a free resolution of the ideal generated by a regular sequence regardless of the nature of the ambient ring.

Definitions

The construction is based on taking the exterior algebra of a module, of which one will use but its basic properties. Since this is a book about commutative rings, there is no room to develop to some extent a theory of skew-commutative algebras. Some basic ideas about exterior powers have been mentioned in Section 3.2. The reader interested in going ab initio is referred to, *e. g.*, [25, Section 1.6].

In this book, one emphasizes the various ways of constructing the complex, all useful in commutative algebra; these are:

(I) As a chain complex whose terms are the exterior powers of a free module of finite rank;
(II) As an alternating associative algebra;
(III) As an iterated tensor product of "small" chain complexes.

Let R stand for a commutative ring. For any of the three approaches, one is preliminarily given a sequence of elements $a_1, \dots, a_n$ in R. Let further F denote a free R-module of rank n and let $\{e_1, \dots, e_n\}$ be a free basis of F. Then, for every integer $r \geq 0$, the rth exterior power $\bigwedge^r F$ is free with basis $\{e_{i_1} \wedge \cdots \wedge e_{i_r} \mid 1 \leq i_1 < \cdots < i_r \leq n\}$.

(I) For a given integer $r \geq 0$, the following assignment

$$e_{i_1} \wedge \cdots \wedge e_{i_r} \mapsto \sum_{t=1}^{r} (-1)^{t+1} a_{i_t} e_{i_1} \wedge \cdots \wedge e_{i_{t-1}} \wedge e_{i_{t+1}} \wedge \cdots \wedge e_{i_r} \tag{6.3.0.1}$$

defines a homomorphism of R-modules $\bigwedge^r R^n \xrightarrow{d_r} \bigwedge^{r-1} R^n$. By identifying $\bigwedge^1 R^n = R^n$ and $\bigwedge^0 R^n = R$, one gets the R-linear map $d = d_1 : R^n \to R$ such that $d(e_i) = a_i$, for $1 \leq i \leq n$.

Proposition 6.3.1. *The sequence of free modules and R-maps*

$$0 \to \bigwedge^n R^n \xrightarrow{d_n} \bigwedge^{n-1} R^n \longrightarrow \cdots \longrightarrow \bigwedge^2 R^n \xrightarrow{d_2} R^n \xrightarrow{d} R \to 0 \tag{6.3.1.1}$$

is a chain complex.

Proof. The proof is a straightforward calculation. Without loss of generality, assume that $i_t = t$, for $t = 1, \ldots, r$. Then, using the notation $\hat{e}_j$ for deletion of e_j, one has

$$\begin{aligned} d_{r-1}(d_r(e_1 \wedge \cdots \wedge e_r)) &= d_{r-1}(a_1 \hat{e}_1 \wedge e_2 \wedge \cdots \wedge e_r - a_2 e_1 \wedge \hat{e}_2 \wedge \cdots \wedge e_r + \cdots) \\ &= a_1 d_{r-1}(\hat{e}_1 \wedge e_2 \wedge \cdots \wedge e_r) - a_2 d_{r-1}(e_1 \wedge \hat{e}_2 \wedge \cdots \wedge e_r) + \cdots \\ &= (a_1 a_2 e_3 \wedge \cdots \wedge e_r - \cdots) - (a_2 a_1 e_3 \wedge \cdots \wedge e_r - \cdots) + \cdots \end{aligned}$$

Thus, the two summands $a_1 a_2 e_3 \wedge \cdots \wedge e_r$ and $-a_2 a_1 e_3 \wedge \cdots \wedge e_r$ above cancel each other and easy inspection shows that there are no other summands with coefficient $\pm a_1 a_2$. By an obvious symmetry, for each pair $1 \leq i < j \leq r$, there are exactly two summands with coefficient $a_i a_j$ and opposite signs, affecting the same wedge product $e_1 \wedge \cdots \hat{e}_i \wedge \cdots \hat{e}_j \wedge \cdots \wedge e_r$. □

The complex (6.3.1.1) is called the *Koszul complex* associated to the sequence of elements $\{a_1, \ldots, a_n\}$; it will be denoted $K_\bullet(\mathbf{a})$ or $K_\bullet(\mathbf{a}, R)$ to emphasize the ambient ring, where $\mathbf{a} = \{a_.1, \ldots, a_n\}$. Note that it has as augmentation the residue ring $R/(a_1, \ldots, a_n)$.

A very notable property of $K_\bullet(\mathbf{a})$ is its self-duality, by which one means roughly that two maps equidistant from the two extremes of the complex are transposed of each other. To make this precise, one has to use R-duals and dual bases, hereon indicated by a $*$ pegged to the upper right side of the object. For this, one introduces the following notation: given a subset $\mathfrak{I} \subset \mathfrak{N} := \{1, \ldots, n\}$, let $e_{\mathfrak{I}}$ denote the exterior product of the elements of $\{e_1, \ldots, e_n\}$ indexed by the elements of $\mathfrak{I}$.

For a given $0 \leq r \leq n$, consider the R-linear map $\mathfrak{D} : \bigwedge^r R^n \longrightarrow (\bigwedge^{n-r} R^n)^*$ defined by the assignment

$$\mathfrak{D}(e_{\mathfrak{I}}) = \sigma(\mathfrak{I}) e^*_{\mathfrak{N} \setminus \mathfrak{I}},$$

where $\mathfrak{I} \subset \mathfrak{N}$ has r elements, $e^*_{\mathfrak{N} \setminus \mathfrak{I}}$ denotes an element of the dual basis of $\bigwedge^{n-r} R^n$ and $\sigma(\mathfrak{I})$ is the number of pairs (i, j) with $i \in \mathfrak{I}$, $j \in \mathfrak{N} \setminus \mathfrak{I}$ such that $i > j$.

Although slightly cumbersome, $\sigma(\mathfrak{I})$ is just a way to "correct signs" typical in these matters. Its main purpose is to guarantee that $\mathfrak{D}$ be an isomorphism of chain complexes $K_\bullet(\mathbf{a}) \simeq K_\bullet(\mathbf{a})^*$, where the second complex is obtained from the first by dualizing all maps. The details are left to the interested reader.

(II) Set $\bigwedge R^n := \bigoplus_{r=0}^n \bigwedge^r R^n$. Then $\bigwedge R^n$ has a structure of a graded associative alternating R-algebra, with multiplication rules

$$(e_{i_1} \wedge \cdots \wedge e_{i_r}) \cdot (e_{j_1} \wedge \cdots \wedge e_{j_s}) = e_{i_1} \wedge \cdots \wedge e_{i_r} \wedge e_{j_1} \wedge \cdots \wedge e_{j_s}$$

$$v \wedge w = (-1)^{rs} w \wedge v, \quad \text{for } v \in \bigwedge^r R^n, w \in \bigwedge^s R^n$$

$$v \wedge v = 0, \quad \text{for } v \in \bigwedge R^r, r \text{ odd}.$$

Likewise, the differentials d_r of $K_\bullet(\mathbf{a}, R)$ are the graded parts of a graded R-linear homomorphism d of $\bigwedge R^n$ of degree -1 satisfying the following rules:

$$d^2 = 0$$

$$d(v \wedge w) = d(v) \wedge w + (-1)^r v \wedge d(w), \quad v \in \bigwedge^r R^n,$$

where the second of these rules is that of a so-called *antiderivation*.

Next is an example of the usefulness of this approach, where the notation is that of (6.2.37.1).

Proposition 6.3.2. *Set*

$$Z(K_\bullet(\mathbf{a}, R)) := \bigoplus_{i \geq 0} Z_i(K_\bullet(\mathbf{a}, R))$$

$$B(K_\bullet(\mathbf{a}, R)) := \bigoplus_{i \geq 0} B_i(K_\bullet(\mathbf{a}, R))$$

$$H(K_\bullet(\mathbf{a}, R)) := \bigoplus_{i \geq 0} H_i(K_\bullet(\mathbf{a}, R))$$

Then:
(i) $Z(K_\bullet(\mathbf{a}, R))$ *is an* R*-subalgebra of* $K_\bullet(\mathbf{a}, R)$.
(ii) $B(K_\bullet(\mathbf{a}, R))$ *is a two-sided ideal of* $Z(K_\bullet(\mathbf{a}, R))$.
(iii) *The ideal* $(\mathbf{a}) \subset R$ *annihilates* $H(K_\bullet(\mathbf{a}, R))$.

Proof. (i) From the above antiderivation rule and the rule of multiplication follows immediately that $Z(K_\bullet(\mathbf{a}, R))$ is closed under multiplication. The remaining axioms are easily verified.

(ii) Let $v \in Z_i(K_\bullet(\mathbf{a}, R))$ and $w = d(w') \in B_j(K_\bullet(\mathbf{a}, R))$. Then

$$d(v \wedge w') = 0 \wedge w' + (-1)^i v \wedge d(w') = (-1)^i v \wedge w,$$

thus showing that $v \wedge w \in B_{i+j}(K_\bullet(\mathbf{a}, R))$. Multiplying on the left is similar.

(iii) Noting that $(\mathbf{a}) = B_0(K_\bullet(\mathbf{a}, R))$, this follows immediately from (ii). □

(III) Recall the tensor product of chain complexes as defined in Subsection 6.2.3.2. As a mnemonic, one can write the differential of a tensor product in a way resembling the property of an antiderivation:

$$\partial_{C\otimes C'}(c\otimes c') = d(c)\otimes c' + (-1)^r c\otimes d'(c'), \tag{6.3.2.1}$$

where r is the degree of c in the complex C.

Lemma 6.3.3. *Let* $\mathbf{b} = \{b_1,\dots,b_r\} \subset R$ *and* $\mathbf{c} = \{c_1,\dots,c_s\} \subset R$. *Then there is a natural isomorphism of chain complexes:*

$$K_\bullet(\{\mathbf{b},\mathbf{c}\},R) \simeq K_\bullet(\mathbf{b},R)\otimes K_\bullet(\mathbf{c},R).$$

Proof. Let $L_{\mathbf{b}} : R^r \to R$ (resp., $L_{\mathbf{c}} : R^s \to R$) denote the R-linear map sending an element of the canonical basis of R^r (resp., R^s) to some b_i (resp., c_j). Then, up to a harmless identification, the sum map $L_{\mathbf{b}} + L_{\mathbf{c}} : R^r \oplus R^s \to R$ is defined by mapping the induced basis to $\{\mathbf{b},\mathbf{c}\}$. Since $\bigwedge(R^r\oplus R^s) \simeq \bigwedge(R^r)\otimes\bigwedge(R^s)$ as graded R-algebras, the underlying exterior algebras of the Koszul complexes $K_\bullet(\{\mathbf{b},\mathbf{c}\},R)$ and $K_\bullet(\mathbf{b},R)\otimes K_\bullet(\mathbf{c},R)$ are thus isomorphic.

Therefore, it suffices to compare the respective differentials. The differential $d_{\mathbf{b},\mathbf{c}}$ of $K_\bullet(\{\mathbf{b},\mathbf{c}\},R)$ is an antiderivation whose values are determined by its values in degree 1, *i. e.*, on $R^r\oplus R^s$. Since the differential $\partial_{\mathbf{b},\mathbf{c}}$ of the tensor product $K_\bullet(\mathbf{b},R)\otimes K_\bullet(\mathbf{c},R)$ is also defined by the characteristic property of an antiderivation as in (6.3.2.1), then its values too are determined by the values in degree 1. Thus, typically,

$$d_{\mathbf{b},\mathbf{c}}((x,0)) = L_{\mathbf{b}}(x) = d_{\mathbf{b}}(x)\otimes 1 = \partial_{\mathbf{b},\mathbf{c}}(x\otimes 1),$$

and, similarly, for an element $(0,y) \in R^r\oplus R^s$. □

Proposition 6.3.4. *Let* $\mathbf{a} = \{a_1,\dots,a_n\} \subset R$ *as before. Then there is a natural isomorphism of chain complexes*

$$K_\bullet(\mathbf{a},R) \simeq K_\bullet(a_1,R)\otimes\cdots\otimes K_\bullet(a_n,R).$$

Proof. Induct on n. For $n = 1$, there is nothing to prove, so let $n \geq 2$. By the inductive hypothesis,

$$K_\bullet(a_1,\dots,a_{n-1},R) \simeq K_\bullet(a_1,R)\otimes\cdots\otimes K_\bullet(a_{n-1},R),$$

hence it suffices to show that $K_\bullet(\mathbf{a},R) \simeq K_\bullet(a_1,\dots,a_{n-1},R)\otimes K_\bullet(a_n,R)$. This follows from Lemma 6.3.3 by taking $\mathbf{b} = \{a_1,\dots,a_{n-1}\}$ and $\mathbf{c} = \{a_n\}$. □

6.3.1 Long exact sequences of Koszul homology

A special case of tensor product deserves a particular notation. Namely, let $\mathbf{a} \subset R$ and let M denote an R-module. One sets $K_\bullet(\mathbf{a},M) := K_\bullet(\mathbf{a},R)\otimes M$, where M is thought of as a chain complex concentrated in degree zero.

A basic property of the Koszul complex is its functoriality in the following sense.

Proposition 6.3.5. *Given elements* $\mathbf{a} \subset R$ *and an exact sequence of* R*-modules* $0 \to M' \to M \to M'' \to 0$*, there exists a long exact sequence in homology*

$$\cdots \to H_i(K_\bullet(\mathbf{a}, M')) \longrightarrow H_i(K_\bullet(\mathbf{a}, M)) \longrightarrow H_i(K_\bullet(\mathbf{a}, M'')) \to \cdots.$$

Proof. Tensoring the given exact sequence on the left with $K_\bullet(\mathbf{a}, R)$ yields an exact sequence of chain complexes

$$0 \to K_\bullet(\mathbf{a}, M') \longrightarrow K_\bullet(\mathbf{a}, M) \longrightarrow K_\bullet(\mathbf{a}, M'') \to 0.$$

Now apply to this sequence the long exact sequence in homology as given in Proposition 6.2.38. □

Some fundamental properties of the Koszul complex are an offspring of the following commutative diagram of maps of (horizontal) chain complexes for a given element $a \in R$:

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & & & 0 & \to & R = R_0 & \to & 0 \\
 & & & & \downarrow & & \downarrow & & \\
0 & \to & K_1(a,R) & \xrightarrow{\cdot a} & K_0(a,R) & \to & 0 & & \\
 & & \| & & \| & & & & \\
 & & R & & R & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \to & R = R(-1)_1 & \to & 0 & & & & \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array} \tag{6.3.5.1}$$

where the nontrivial vertical maps are the identity.

Expressing in the usual form of a horizontal exact sequence, one gets the following split exact sequence of chain complexes:

$$0 \to R \longrightarrow K_\bullet(a, R) \longrightarrow R(-1) \to 0. \tag{6.3.5.2}$$

Since this sequence splits, for any given chain complex $C_\bullet$ one still has a split exact sequence

$$0 \to C_\bullet \xrightarrow{\iota} K_\bullet(a, R) \otimes C_\bullet \xrightarrow{\pi} C_\bullet(-1) \to 0. \tag{6.3.5.3}$$

Proposition 6.3.6. *Consider the long exact sequence in homology associated to the short exact sequence* (6.3.5.3)*:*

$$\begin{aligned}
\cdots \to\ & H_i(C_\bullet) \xrightarrow{H_i(\iota)} H_i(K_\bullet(a,R) \otimes C_\bullet) \xrightarrow{H_i(\pi)} H_i(C_\bullet(-1)) = H_{i-1}(C_\bullet) \\
& \xrightarrow{\delta_i} H_{i-1}(C_\bullet) \xrightarrow{H_{i-1}(\iota)} H_{i-1}(K_\bullet(a,R) \otimes C_\bullet) \xrightarrow{H_{i-1}(\pi)} H_{i-1}(C_\bullet(-1)) = H_{i-2}(C_\bullet) \\
& \xrightarrow{\delta_{i-1}} \cdots
\end{aligned}$$

Then: (a) $H_i(\iota)$ *is injective for every* i*.*

(b) $\delta_i = (-1)^i a$ *for every* i.

Proof. (a) This assertion follows from the fact that ι is split-injective.

(b) Since the connecting homomorphism is given by the snake lemma, one just have to perform the usual diagram chasing in a typical slice of (6.3.5.3) to see how a representative of an element in $H_i(C_\bullet(-1)) = H_{i-1}(C_\bullet)$ maps by δ_i:

$$\begin{array}{ccccccccc}
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & C_i & \xrightarrow{\iota} & C_i \oplus D_{i-1} & \xrightarrow{\pi} & C(-1)_i = C_{i-1} & \to & 0 \\
 & & \downarrow d_i & & \downarrow \partial_i & & \downarrow d_{i-1} & & \\
0 & \to & C_{i-1} & \xrightarrow{\iota} & C_{i-1} \oplus D_{i-2} & \xrightarrow{\pi} & C(-1)_{i-1} = C_{i-2} & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & &
\end{array}$$

where

$$\partial_i = \begin{pmatrix} d_i & (-1)^{i-1} \\ 0 & d_{i-1} \end{pmatrix}$$

is written in matrix form for convenience.

Start with an arbitrary $z_{i-1} \in Z_{i-1}(C_\bullet(-1))$ on the right most vertical complex. Then $\pi((0, z_{i-1})) = z_{i-1}$. On the other hand,

$$\partial_i((0, z_{i-1})) = ((-1)^{i-1} a z_{i-1}, d_{i-1}(z_{i-1})) = ((-1)^{i-1} a z_{i-1}, 0) = \iota((-1)^{i-1} a z_{i-1}).$$

By the obvious identification, it has been shown that δ_i is induced by multiplication by (signed) a. □

Corollary 6.3.7. *The ideal* $(\mathbf{a}) \subset R$ *annihilates the homology of the complex* $K_\bullet(\mathbf{a}, M)$.

Proof. Say, $\mathbf{a} = \{a_1, \ldots, a_n\}$. Fix an $i \in \{1, \ldots, n\}$ and consider the split exact sequence (6.3.5.3) with $a = a_i$ and $C_\bullet = K_\bullet(\mathbf{a}, M)$. Taking the associated long exact sequence in homology and using items (a) and (b) of Proposition 6.3.6 yield that a_i annihilates the homology $H(K_\bullet(\mathbf{a}, M))$. □

Corollary 6.3.8. *Given elements* $\{a_1, \ldots, a_n\} \subset R$ *and an* R*-module* M*, there is a long exact sequence in homology*

$$\cdots \to H_{i+1}(K_\bullet(a_1, \ldots, a_n)) \to H_i(K_\bullet(a_1, \ldots, a_{n-1})) \xrightarrow{(-1)^i a_n} H_i(K_\bullet(a_1, \ldots, a_{n-1}))$$
$$\cdots \to H_i(K_\bullet(a_1, \ldots, a_n)) \to H_{i-1}(K_\bullet(a_1, \ldots, a_{n-1})) \xrightarrow{(-1)^{i-1} a_n} H_{i-1}(K_\bullet(a_1, \ldots, a_{n-1}))$$
$$\cdots \to H_1(K_\bullet(a_1, \ldots, a_n)) \to H_0(K_\bullet(a_1, \ldots, a_{n-1})) \xrightarrow{a_n} H_0(K_\bullet(a_1, \ldots, a_{n-1}))$$

with augmentation $H_0(K_\bullet(a_1, \ldots, a_n)) \simeq M/(a_1, \ldots, a_n)M$.

Proof. Apply Proposition 6.3.6 to the exact sequence Proposition 6.3.6 with $C_\bullet = K_\bullet(a_1, \ldots, a_{n-1})$. □

Corollary 6.3.9. *If M is an R-module and $\mathbf{a} := \{a_1, \dots, a_n\} \subset R$ is an M-sequence, then $H_i(K_\bullet(\mathbf{a}, M)) = 0$ for $i \geq 1$. Therefore, in this case, $K_\bullet(\mathbf{a}, M)$ is a free R-resolution of the R-module $M/(\mathbf{a})M$.*

Proof. Induct on n. For $n = 1$, with $a = a_1$, one has $H_1(K_\bullet(a, M)) = 0$ since the latter is the kernel of multiplication by a on M according to the previous corollary.

Assuming $n \geq 2$, by the inductive hypothesis $H_i(K_\bullet(\mathbf{a} \setminus \{a_n\}, M)) = 0$ for $i \geq 1$. Therefore, by the previous corollary, $H_i(K_\bullet(\mathbf{a}, M)) = 0$ for $i \geq 2$ and $H_1(K_\bullet(\mathbf{a}, M)) = 0$ since the latter is the kernel of multiplication by a_n on $M/(a_1, \dots, a_{n-1})M$. □

Remark 6.3.10. Note that if one changes the order of the elements in the given sequence the resulting annihilation still holds, the reason being that the Koszul complex is independent of the order of the elements. This also says that a full converse does not hold in general, since the notion of M-sequence may depend on the order of the elements. However, see Proposition 6.3.12(ii) below.

Corollary 6.3.9 admits an important extension. Since it involves the notion of depth, the usual finiteness conditions will be assumed.

Proposition 6.3.11 (Sensitivity to depth). *Let R be Noetherian, let M be a finitely generated R-module and let $\mathbf{a} \subset R$ be a set of n elements such that $M/\mathbf{a}M \neq 0$. Then $n - \operatorname{depth}_{(\mathbf{a})}(M)$ is the largest nonnegative integer i such that $H_i(K_\bullet(\mathbf{a}, M)) \neq 0$.*

Proof. Let $q := \max\{i \geq 0 \mid H_i(K_\bullet(\mathbf{a}, M)) \neq 0\}$. Note that such an integer exists and is bounded by n since $H_0(K_\bullet(\mathbf{a}, M)) = M/\mathbf{a}M \neq 0$ by assumption and $H_i(K_\bullet(\mathbf{a}, M)) = 0$, for every $i \geq n + 1$.

Proceed by descending induction on q, starting with $q = n$. Now, $H_n(K_\bullet(\mathbf{a}, M)) = Z_n(K_\bullet(\mathbf{a}, M)) = 0 :_M (\mathbf{a})$ since the differential d_n acts by

$$e_1 \wedge \cdots \wedge e_n \otimes x \mapsto \left(\sum_i (-1)^{i+1} a_1 \wedge \cdots \wedge \widehat{e_i} \wedge \cdots \wedge a_n \right) \otimes x,$$

for any given $x \in M$. By hypothesis, $0 :_M (\mathbf{a}) \neq 0$ which means that $\mathbf{a}$ is knocked out by a nonzero element of M. This implies that $\operatorname{depth}_{(\mathbf{a})}(M) = 0$.

Now, assume that $q < n$. Then $0 :_M (\mathbf{a}) = H_n(K_\bullet(\mathbf{a}, M)) = 0$, hence there exists an element $a \in (\mathbf{a})$ which is a nonzero divisor on M. Consider the short exact sequence of R-modules

$$0 \to M \xrightarrow{\cdot a} M \longrightarrow M/aM \to 0,$$

and the following slice of the associated long exact sequence in homology as in Proposition 6.3.5

$$H_{q+1}(K_\bullet(\mathbf{a}, M)) \to H_{q+1}(K_\bullet(\mathbf{a}, M/aM)) \to H_q(K_\bullet(\mathbf{a}, M)) \xrightarrow{\cdot a} H_q(K_\bullet(\mathbf{a}, M)).$$

Since, by hypothesis, $H_i(K_\bullet(\mathbf{a}, M)) = 0$ for every $i \geq q + 1$, the above long sequence implies that $H_i(K_\bullet(\mathbf{a}, M/aM)) = 0$ for every $i \geq q + 2$. On the other hand, by Corollary 6.3.7

a annihilates $H_q(K_\bullet(\mathbf{a}, M))$. Therefore, still from the above long exact sequence, one has

$$H_{q+1}(K_\bullet(\mathbf{a}, M/aM)) \simeq H_q(K_\bullet(\mathbf{a}, M)) \neq 0.$$

Then, by the inductive hypothesis, $\operatorname{depth}_{(\mathbf{a})}(M/aM) = n - (q+1)$. But since a is regular on M, one has $\operatorname{depth}_{(\mathbf{a})}(M/aM) = \operatorname{depth}_{(\mathbf{a})}(M) - 1$. Thus, one is done. □

As a complement to Corollary 6.3.9, one can file the following result.

Proposition 6.3.12. *Let R be Noetherian, let $\mathbf{a} = \{a_1, \dots, a_n\} \subset R$ denote elements contained in the Jacobson radical of R and let M denote a finitely generated R-module.*
(i) (Rigidity) *Let $i \geq 1$ be an integer such that $H_i(K_\bullet(\mathbf{a}, M)) = 0$. Then*

$$H_j(K_\bullet(a_1, \dots, a_m, M)) = 0$$

for every $j \geq i$ and every $1 \leq m \leq n$.
(ii) (Converse to Corollary 6.3.9) *If $H_1(K_\bullet(\mathbf{a}, M)) = 0$, then $\{a_1, \dots, a_n\}$ is an M-sequence.*

Proof. (i) Induct on n. For $n = 1$, the statement is vacuous.

Suppose that $n \geq 2$. By Proposition 6.3.8, one has an injection

$$0 \to H_i(K_\bullet(a_1, \dots, a_{n-1}, M))/a_n H_i(K_\bullet(a_1, \dots, a_{n-1}, M)) \to H_i(K_\bullet(\mathbf{a}, M)),$$

hence by the lemma of Nakayama, one has $H_i(K_\bullet(a_1, \dots, a_{n-1}, M)) = 0$. By the inductive hypothesis, $H_j(K_\bullet(a_1, \dots, a_m, M)) = 0$ for every $j \geq i$ and every $1 \leq m \leq n-1$. Using Proposition 6.3.8 once more, one finds an exact slice

$$H_{i+1}(K_\bullet(a_1, \dots, a_{n-1}, M)) \to H_{i+1}(K_\bullet(\mathbf{a}, M)) \to H_i(K_\bullet(a_1, \dots, a_{n-1}, M)).$$

Since the two extremes are null, so is $H_{i+1}(K_\bullet(\mathbf{a}, M))$. Then iterate the procedure.

(ii) Again induct on n, the statement being easily verified for $n = 1$.

Assume $n \geq 2$. By part (i), one has $H_1(K_\bullet(a_1, \dots, a_{n-1}, M)) = 0$. By the inductive hypothesis, $\{a_1, \dots, a_{n-1}\}$ is an M-sequence. But $H_1(K_\bullet(\mathbf{a}, M)) = 0$ implies that the map

$$\begin{array}{ccc} H_0(K_\bullet(a_1, \dots, a_{n-1}, M)) & \xrightarrow{\cdot a_n} & H_0(K_\bullet(a_1, \dots, a_{n-1}, M)) \\ \| & & \| \\ M/(a_1, \dots, a_{n-1})M & & M/(a_1, \dots, a_{n-1})M \end{array}$$

is injective. Consequently, a_n is regular on $M/(a_1, \dots, a_{n-1})M$. □

The next two results have been proved before by different methods (Proposition 5.3.14 and Proposition 5.3.17, respectively).

Corollary 6.3.13. *Let R be a Noetherian ring and let M stand for a finitely generated R-module. If $a_1, \dots, a_n$ is an M-sequence contained in the Jacobson radical of R, then any permutation of its elements still gives an M-sequence.*

Proposition 6.3.14. *Let R be a Noetherian ring and let M stand for a finitely generated R-module. If $I \subset R$ is an ideal such that $IM \neq M$, then for every element a belonging to the Jacobson radical of R, one has*

$$\operatorname{depth}_{(I,a)}(M) \leq \operatorname{depth}_I(M) + 1$$

Proof. Say, $I = (a_1, \ldots, a_n)$. By Proposition 6.3.8, one has an injective map

$$0 \to H_i(K_\bullet(a_1, \ldots, a_n, M))/aH_i(K_\bullet(a_1, \ldots, a_n, M)) \to H_i(K_\bullet(a_1, \ldots, a_n, a, M)),$$

for any i. Therefore, by Nakayama, the vanishing of $H_i(K_\bullet(a_1, \ldots, a_n, a, M))$ implies that of $H_i(K_\bullet(a_1, \ldots, a_n, M))$.

Note that $(I, a)M \neq M$ since by assumption $IM \neq M$ and a belongs to the Jacobson radical of R. Therefore, by Proposition 6.3.11, one has

$$n - \operatorname{depth}_{(I,a)}(M) \geq n - 1 - \operatorname{depth}_I(M),$$

from which the statement follows immediately. □

6.3.2 The theorem of Serre

In this part, one proves a slight generalization of Serre's fundamental result on regular local rings, with essentially the same line of proofs. It ought to be noted that Serre's theorem and generalizations thereof have been proved by other methods in the later years ([112, Theorem 28.2] and Theorem 6.2.33).

Theorem 6.3.15 (Serre homological dimension theorem). *Let $(R, \mathfrak{m})$ be a Noetherian local ring and let $I \subset R$ be an ideal of finite homological dimension over R. If I contains elements $a_1, \ldots, a_n$ constituting a subset of minimal generators of $\mathfrak{m}$, then $n \leq \mathrm{h.d}_R(R/I)$.*

Proof. Note that the hypothesis implies that $\{a_1, \ldots, a_n\}$ is also a subset of minimal generators of I since $\mathfrak{m}I \subset \mathfrak{m}^2$. Thus, a minimal free resolution of R/I starts as

$$F_1 = K_1 \oplus G_1 \to F_0 = R \to R/I \to 0, \tag{6.3.15.1}$$

where K_1 is free and surjects onto $(a_1, \ldots, a_n)$. One now claims that one can choose minimal generators of $Z_1 = \ker(F_1 \to F_0 = R)$ in such a way that the corresponding free presentation $F_2 \twoheadrightarrow Z_1$ has $F_2 = K_2 \oplus G_2$, where $K_2 = \bigwedge^2 K_1$ and the restriction to this submodule is the differential $\bigwedge^2 K_1 \to K_1$ of the Koszul complex map associated to the sequence $\{a_1, \ldots, a_n\}$. (*N. B.* One is however not claiming that this restriction maps onto $\ker(K_1 \to K_0 = R)$.) From (6.3.15.1), there is anyway an induced map $K_2 \to F_2$. Since F_2 is free, in order to show that this map is split injective it suffices to argue that the map of k-vector spaces $K_2/\mathfrak{m}K_2 \to F_2/\mathfrak{m}F_2$ is injective (hence, split). So suppose $\alpha \in K_2$ maps down to $\mathfrak{m}F_2$. By construction, there is a commutative diagram

$$\begin{array}{ccc} F_2 & \to & F_1 \\ \uparrow & & \uparrow \\ K_2 & \to & K_1 \end{array}$$

By step one, the rightmost vertical arrow is split injective. Then it follows that the lower map takes α into $\mathfrak{m}^2 K_1$. Since this map is the Koszul differential $\bigwedge^2 K_1 \to K_1$ and $\{a_1, \dots, a_n\}$ is linearly independent modulo $\mathfrak{m}^2$ by assumption, it is immediate to see that $\alpha \in \mathfrak{m}K_2$. This shows the contention.

The rest of the proof iterates this step *ipsis literis* all the way through the last free module in a suitably constructed minimal free resolution of R/I, thus yielding a split injective map of complexes

$$\begin{array}{ccccccccccc} 0 & \to & F_h & \to & F_{h-1} & \to & \cdots & \to & F_1 & \to & F_0 = R \\ & & \uparrow & & \uparrow & & & & & & \| \\ & & K_h & \to & K_{h-1} & \to & \cdots & \to & K_1 & \to & K_0 = R \end{array}$$

where $h = \mathrm{h.d}_R(R/I)$ and the lower complex is the Kozsul complex on $\{a_1, \dots, a_n\}$. Now, if $h < n$ then one could do one more step so as to get an injective map $K_{h+1} \longrightarrow 0$, an absurd.

This proves our statement. □

Remark 6.3.16. It is important to note that the theorem does not claim that the minimal number of generators of I is bounded above by the homological dimension of R/I, which would be nonsense.

Corollary 6.3.17 (Serre). *Let $(R, \mathfrak{m})$ be a Noetherian local ring. If $\mathrm{hd}_R(R/\mathfrak{m}) < \infty$ then R is regular.*

Proof. Apply the preceding with $I = \mathfrak{m}$ and $n = \mu(\mathfrak{m})$. Then $\mu(\mathfrak{m}) \leq \mathrm{hd}_R(R/\mathfrak{m})$. By the Auslander–Buchsbaum equality (Theorem 6.2.19), one has

$$\mathrm{hd}_R(R/\mathfrak{m}) = \mathrm{depth}_{\mathfrak{m}}(R) - \mathrm{depth}_{\mathfrak{m}}(R/\mathfrak{m}) = \mathrm{depth}_{\mathfrak{m}}(R) \leq \dim R = \mathrm{ht}\,\mathfrak{m} \leq \mu(\mathfrak{m}).$$

Therefore, $\dim R = \mu(\mathfrak{m})$ and one concludes from Definition 6.1.3 (1). □

Remark 6.3.18. Serre's theorem also follows from the proof of Theorem 6.3.15 rather than its content, since it shows in this special case that the Koszul complex on the set of minimal generators of $\mathfrak{m}$ is acyclic. Then, by Proposition 6.3.12(ii), $\mathfrak{m}$ is generated by an R-sequence and one concludes from Definition 6.1.3(3).

Corollary 6.3.19. *Let $R, \mathfrak{m}$ be a Noetherian local ring of dimension d. If R has an ideal $I \subset R$ of finite homological dimension over R containing d elements $a_1, \dots, a_d$ forming a subset of minimal generators of $\mathfrak{m}$, then:*

(a) *$\mathfrak{m}$ is an associated prime of R/I.*

(b) *R is Cohen–Macaulay.*

(c) *The minimal free R-resolution of R/I has the expected bounds for its Betti numbers.*

Proof. By Theorem 6.3.15 and the Auslander–Buchsbaum formula, one has

$$\dim R \leq \mathrm{hd}_R(R/I) = \mathrm{depth}_{\mathfrak{m}}(R) - \mathrm{depth}_{\mathfrak{m}}(R/I) \leq \dim R - \mathrm{depth}_{\mathfrak{m}}(R/I).$$

Necessarily, $\mathrm{depth}_{\mathfrak{m}}(R/I) = 0$ and $\dim R = \mathrm{depth}_{\mathfrak{m}}(R)$, proving (a) and (b), respectively.

Item (c) follows from the proof of Theorem 6.3.15 because as was established the Koszul complex split-injects into a minimal free R-resolution of R/I. □

Note that Theorem 6.3.15 actually shows, under the conditions there, that R has a finitely generated perfect module of finite length. It is conceivable that the expected bounds for the Betti numbers are always satisfied in such a case even though R might not be regular. In case R is regular, this is known as the Buchsbaum–Eisenbud, Horrocks conjecture. Even the following relaxed form of this conjecture is open in general.

Conjecture 6.3.20 (Buchsbaum–Eisenbud, Horrocks extended conjecture). *Let $(R, \mathfrak{m})$ be a Noetherian local ring and let M be a finitely generated R-module of grade g having finite free resolution. Then the Betti numbers satisfy*

$$\beta_j(M) \geq \binom{g}{j}, \quad \forall j$$

6.4 Variations on the Koszul complex: determinantal ideals

In this section, one applies the method of the Koszul complex to study the free resolutions of certain determinantal ideals.

6.4.1 The Eagon–Northcott complex

The main result is due to Eagon and Northcott, but has been recovered by various mathematicians in different forms.

Let R denote an arbitrary commutative ring and let $\mathcal{A} = (a_{i,j})$ stand for an $r \times s$ ($r \leq s$) matrix with entries in R. One considers the following stray of the *symmetrization* of the Koszul complex $(K_\bullet(a_{t,1}, \ldots, a_{t,s}, R), \partial)$ based on the entries of the row of order t:

$$\mathrm{EN}_0 = R, \quad \mathrm{EN}_{q+1} := \bigwedge^{r+q}(R^s) \otimes_R \mathcal{S}_q(R^r), \quad 1 \leq q \leq s - r.$$

Thus, one has a complex

$$0 \to \mathrm{EN}_{s-r+1} \to \mathrm{EN}_{s-r} \to \cdots \to \mathrm{EN}_1 \to \mathrm{EN}_0 \to 0, \tag{6.4.0.1}$$

where the differential is given by

$$e_{i_1} \wedge \cdots \wedge e_{i_{q+r}} \otimes X_1^{j_1} \cdots X_r^{j_r} \mapsto \sum_{t=1, j_t \geq 1}^{r} \partial_t(e_{i_1} \wedge \cdots \wedge e_{i_{q+r}}) \otimes X_1^{j_1} \cdots X_t^{j_t - 1} \cdots X_r^{j_r}$$

for $q \geq 1$, while for $q = 0$ one sets

$$e_{i_1} \wedge \cdots \wedge e_{i_r} \otimes 1 \mapsto \det(a_{i,j})_{i_1 \leq j \leq i_r}.$$

Here, one has of course identified $\mathcal{S}(R^r)$ with the polynomial ring $R[X_1, \ldots, X_r]$. Note that the right most differential $\mathrm{EN}_1 \to \mathrm{EN}_0$ maps onto the ideal of r-minors of $\mathcal{A}$.

The complex (6.4.0.1) is called the *Eagon–Northcott* complex associated to the matrix $\mathcal{A}$. It will be denoted by $\mathrm{EN}(\mathcal{A}, R)$. Given an R-module, one can also consider the complex $\mathrm{EN}(\mathcal{A}, M) := \mathrm{EN}(\mathcal{A}, R) \otimes M$. The following result is an analogue of Proposition 6.3.11.

Theorem 6.4.1 (Eagon–Northcott theorem [46]). *Let $\mathcal{A}$ denote an $r \times s$ ($r \leq s$) matrix over a Noetherian ring R and let $I := I_r(\mathcal{A})$ denote its ideal of r-minors. Let M denote a finitely generated R-module such that $M/IM \neq 0$. Then the difference $s - r + 1 - \mathrm{depth}_I(M)$ equals the largest nonzero integer i such that $H_i(\mathrm{EN}(\mathcal{A}, M)) \neq 0$. In particular, $\mathrm{depth}_I(M) \leq s - r + 1$ and equality takes place if and only if $\mathrm{EN}(\mathcal{A}, M)$ is acyclic.*

The proof would be similar to that of Proposition 6.3.11 if one could easily see the homology at the tail. This is however quite more serious presently. And, in fact, the original argument of [46] depends on two basic preliminaries which are themselves analogues of the behavior of the Koszul complex.

Proposition 6.4.2. *Notation as in* Theorem 6.4.1. *If $\mathrm{depth}_I(M) = 0$, then the tail homology $H_{s-r+1}(\mathrm{EN}(\mathcal{A}, M))$ does not vanish.*

Proof. This step is the analogue of the first step in the inductive proof of Proposition 6.3.11, but the argument is more involved. It will consist in reducing to the case where an r-minor is invertible and then by means of elementary transformations to the case where the matrix has a very simple shape.

Namely, the hypotheses imply that I annihilates a nonzero element of M. Since one is at the tail of the complex then the claim is that the differential maps some nonzero element of EN_{s-r+1} to zero in EN_{s-r}. If $r = s$, the complex degenerates into the trivial complex $0 \to M \to M \to 0$ whose differential is multiplication by $D := \det \mathcal{A}$. Then D kills a nonzero element of M by assumption.

Suppose that $r < s$. If the ideal generated by the first row of $\mathcal{M}$ annihilates a nonzero element $y \in M$, then the element $(e_1 \wedge \cdots \wedge e_s \otimes X_1^{s-r}) \otimes y \in \mathrm{EN}_{s-r+1}$ is mapped to zero by the differential.

Therefore, one may assume that the set $\{1 \leq t \leq r \mid 0 :_M I_t(\mathcal{A}(t)) = 0\}$ is nonempty, where $\mathcal{A}(t)$ denotes the submatrix of $\mathcal{A}$ consisting of the first t rows. Let t_0 be the largest element of this set. Then there exists $0 \neq x \in M$ annihilating $I_{t_0+1}(\mathcal{A}(t_0+1))$.

Clearly, then, say, the t_0-minor D of the upper-right corner of $\mathcal{A}$ is such that none of its powers annihilates $0 :_R Rx \subset R$. Therefore, one can choose a prime ideal $P \in \mathrm{Spec}\, R$ such that P contains $0 :_R Rx$ but not D. Since all data at sight commute with fractions, one may trade R_P for R while keeping the assumptions, *i. e.*, there is still a nonzero

$x \in M$ annihilated by $I_{t_0+1}(\mathcal{A}(t_0+1))$. Only now the image of D is a unit, hence up to elementary row/column operations—which, once more, preserve all visible data—one can bring up the matrix to have the following shape over the local ring R:

$$\left(\begin{array}{ccccc|ccc} 1 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 & \dots & 0 \\ \hline b_{t_0+1,1} & b_{t_0+1,2} & b_{t_0+1,2} & \dots & b_{t_0+1,t_0} & b_{t_0+1,t_0+1} & b_{t_0+1,t_0+2} & \dots b_{t_0+1,s} \\ \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots \end{array}\right)$$

Set

$$\zeta := \sum_{j_1+\dots+j_{t_0+1}=s-r} (-1)^{j_1+\dots+j_{t_0}} b_{t_0+1,1}^{j_1} \cdots b_{t_0+1,t_0}^{j_{t_0}} e_1 \wedge \cdots \wedge e_s \otimes X_1^{j_1} \cdots X_{t_0}^{j_{t_0}} X_{t_0+1}^{j_{t_0+1}}.$$

Claim. $\zeta \otimes x \neq 0$ and is mapped to 0 by the differential.

For the first assertion, note that taking $j_1 = \cdots = j_{t_0} = 0$ and $j_{t_0+1} = s - r$, the basis element $e_1 \wedge \cdots \wedge e_s \otimes X_{t_0+1}^{s-r}$ is a term of ζ, hence $\zeta \otimes x \neq 0$. As for the second assertion, it suffices to recall that $I_{t_0+1}(\mathcal{A}(t_0+1))$ kills x, hence $b_{t_0+1,j}x = 0$ for all $j \geq t_0 + 1$. This shows that the differential maps ζ to 0. □

Proposition 6.4.3. *Notation as in* Theorem 6.4.1. *The homology* $H_\bullet(\mathrm{EN}(\mathcal{A}, M))$ *is annihilated by a power of* I *which depends only on the size of the matrix.*

No proof will be given here, instead some appropriate comments on the driving arguments are as follows. First, this is the analogue of Corollary 6.3.7, except that the ideal I itself may not annihilate the homology as in the Koszul case.

The proof takes the following steps:

- Let $\mathcal{B}$ (respectively, $\mathcal{C}$) denote the $r \times (s-1)$ submatrix of $\mathcal{A}$ omitting the last column (respectively, the $(r-1) \times (s-1)$ submatrix of $\mathcal{A}$ omitting the last column and the first row).
- Consider the respective Eagon–Northcott complexes $\mathrm{EN}(\mathcal{B}, R)$ and $\mathrm{EN}(\mathcal{C}, R)$ (eventually by taking coefficients in a given R-module); introduce a chain map $\alpha : \mathrm{EN}(\mathcal{B}, R) \to \mathrm{EN}(\mathcal{C}, R)$ and take the resulting mapping cone $(\mathbb{M}(\alpha), \delta)$.
- Define a chain map $\mathrm{EN}(\mathcal{A}, R) \to \mathbb{M}(\alpha)$ that fits in an exact sequence

$$0 \to \mathrm{EN}(\mathcal{B}, R) \to \mathrm{EN}(\mathcal{A}, R) \to \mathbb{M}(\alpha) \to 0$$

  (where the left most chain map is natural), which is term-wise split.
- Let D denote the r-minor as in the proof of Proposition 6.4.2. Then D^r kills the quotient $\mathbb{M}(\alpha)_1/\delta_2(\mathbb{M}(\alpha)_2)$ (this piece requires an involved argument using cofactors).

– The final blow consists in an inductive procedure on either r or s, assuming therefore that both $\mathrm{EN}(\mathcal{B}, R)$ and $\mathrm{EN}(\mathcal{C}, R)$ have homologies annihilated by a sufficient power of D; as a result, using this and the previous homology annihilation for the mapping cone in degree 1, one gets full annihilation of the mapping cone homology. Finally, this is taken into the above exact sequence to get the same result for the homology of $\mathrm{EN}(\mathcal{A}, R)$.

One now turns to the following.

Proof of Theorem 6.4.1. The proof follows the same steps as the proof of Proposition 6.3.11, but this time around one inducts on $d := \mathrm{depth}_I M$.

For $d = 0$, it follows from Proposition 6.4.2.

Suppose that $d > 0$. Let $\{a_1, \ldots, a_d\} \subset I$ denote a maximal M-sequence and let q denote the largest among the integers $i \neq 0$ such that $H_i(\mathrm{EN}(\mathcal{A}, M)) \neq 0$. The exact sequence $0 \to M \xrightarrow{\cdot a_1} M \to M/a_1M \to 0$ induces an exact sequence of chain maps $0 \to \mathrm{EN}(\mathcal{A}, M) \xrightarrow{\cdot a_1} \mathrm{EN}(\mathcal{A}, M) \to \mathrm{EN}(\mathcal{A}, M/a_1M) \to 0$ and the induced long exact sequence in homology

$$\begin{aligned} \ldots \to H_n(\mathrm{EN}(\mathcal{A}, M)) &\xrightarrow{\cdot a_1} H_n(\mathrm{EN}(\mathcal{A}, M)) \to H_n(\mathrm{EN}(\mathcal{A}, M/a_1M)) \\ &\longrightarrow H_{n-1}(\mathrm{EN}(\mathcal{A}, M)) \xrightarrow{\cdot a_1} H_{n-1}(\mathrm{EN}(\mathcal{A}, M)) \to \ldots \end{aligned}$$

Since $\mathrm{depth}_I(M/a_1M) = d - 1$, if p denotes the largest among the integers $i \neq 0$ such that $H_i(\mathrm{EN}(\mathcal{A}, M/a_1M)) \neq 0$, one has by the inductive hypothesis the equality $d-1+p = s - r + 1$.

Now, for $n \geq p + 1$ one has $H_n(\mathrm{EN}(\mathcal{A}, M/a_1M)) = 0$, hence a_1 is regular on $H_{n-1}(\mathrm{EN}(\mathcal{A}, M))$. On the other hand, by Proposition 6.4.3, some power of $a_1 \in I$ kills $H_{n-1}(\mathrm{EN}(\mathcal{A}, M))$, hence $H_{n-1}(\mathrm{EN}(\mathcal{A}, M)) = 0$ for $n \geq p + 1$.

It follows that the map $0 \to H_p(\mathrm{EN}(\mathcal{A}, M/a_1M)) \to H_{p-1}(\mathrm{EN}(\mathcal{A}, M))$ is injective, and hence $H_{p-1}(\mathrm{EN}(\mathcal{A}, M)) \neq 0$ because $H_p(\mathrm{EN}(\mathcal{A}, M/a_1M)) \neq 0$. This means that $q = p - 1$, *i. e.*, $q + d = s - r + 1$, as wished. □

Corollary 6.4.4. *Let $\mathcal{A}$ denote an $r \times s$ ($r \leq s$) matrix over a Noetherian ring R and let $I := I_r(\mathcal{A})$ denote its ideal of r-minors. If* $\mathrm{grade}\, I = s - r + 1$, *then R/I is perfect* (*hence, Cohen–Macaulay*).

It is natural to ask about the ideals of lower order minors. The first general result in this regard was given by J. Eagon in his Chicago PhD thesis and the method of the proof has been dubbed the "Eagon–Northcott indeterminate trick."

Theorem 6.4.5 (Eagon codimension theorem [45], [46]). *Let $\mathcal{A} = (a_{i,j})$ denote an $r \times s$ ($r \leq s$) matrix with entries in a Noetherian ring R and let $1 \leq t \leq \min\{r, s\}$. If $I_t(\mathcal{A}) \neq R$, then it has codimension at most $(r - t + 1)(s - t + 1)$.*

Proof. Set $I := I_t(\mathcal{A})$. It suffices to show that every minimal prime ideal of R/I has codimension at most $(r-t+1)(s-t+1)$. Let $P \supset I$ be such a prime ideal. One inducts on r. For $r = 1$, then necessarily $t = 1$ and I is generated by n elements, hence the result follows from Krull's principal ideal theorem.

Assuming $r > 1$ and localizing at P it is easy to see that one may suppose that R is a Noetherian local ring with maximal ideal P and that I is a P-primary ideal. One may further assume that $I_1(\mathcal{A}) \subset P$ otherwise some entry is a unit, and hence I will be generated by the minors of order $t-1$ of an obvious $(r-1)\times(s-1)$ matrix. In this case, the result follows from the inductive hypothesis on r. One may in addition suppose that $t > 1$ as the height of a minimal prime of R/I is at most the number of a set of generators (again by Krull's principal ideal theorem).

Now one is ready for the main step (trick). Let x denote an indeterminate over R and consider the "deformed" matrix

$$\mathcal{A}(x) := \begin{pmatrix} a_{1,1}+x & a_{1,2} & \dots & a_{1,s} \\ a_{2,1} & a_{2,2} & \dots & a_{2,s} \\ \vdots & \vdots & \dots & \vdots \\ a_{r,1} & a_{r,2} & \dots & a_{r,s} \end{pmatrix}$$

Consider the free extension $R \subset R[x]$. Set $\widetilde{I} := I_t(\mathcal{A}(x)) \subset R[x]$. Since $t > 1$ and $a_{i,j} \in P$ for all i, j, it follows that $\widetilde{I}$ is contained in the extended ideal $PR[x]$, which is prime in $R[x]$ of the same height as P. It is clear by direct inspection that $(\widetilde{I}, x) = (IR[x], x)$ and it is known that $PR[x]$ is a minimal prime of R[x]/IR[x]. We have the following.

Claim: $PR[x]$ is a minimal prime of $R[x]/\widetilde{I}$.

To see this, let $Q \subset R[x]$ be a prime ideal such that $\widetilde{I} \subset Q \subset PR[x]$. Introducing x one sees that $(PR[x], x)$ is a prime ideal containing the ideal (Q, x), hence there exists a minimal prime Q' of (Q, x) contained in $(PR[x], x)$. One has

$$IR[x] \subset \big(IR[x], x\big) = (\widetilde{I}, x) \subset (Q, x) \subset Q' \subset \big(PR[x], x\big).$$

By contraction back to R, one gets $I \subset Q' \cap R$ and since P is the only prime containing I (because I is P-primary) one must have $Q' \cap R = P$. It follows that $PR[x] \subset Q'$ and since $x \in Q'$ one gets an equality $Q' = (PR[x], x)$, *i. e.*, $(PR[x], x)$ is a minimal prime of (Q, x).

To conclude, one passes to the residue class ring $R[x]/Q$ and observes that its ideal $(Q, x)/Q$ is principal with minimal prime $(PR[x], x)/Q$. By Krull's principal ideal theorem, the latter has codimension at most 1. Therefore, the chain

$$\{0\} = Q/Q \subset PR[x]/Q \subset \big(PR[x], x\big)/Q$$

must collapse somewhere and it can only happens in the leftmost inclusion since $x \notin PR[x]$ as $1 \notin P$. This shows that $PR[x] = Q$ is a minimal prime of $R[x]/\widetilde{I}$ as was to be shown.

Now localize $R[x]$ at $P' := PR[x]$. Since $a_{1,1} + x \notin P'$ (again because $1 \notin P$), it becomes invertible in this localization, hence by the same argument as in the beginning of the proof, the prime ideal $P'_{P'}$ has by the inductive hypothesis codimension at most $(r - t + 1)(s - t + 1)$. But since P' is prime, P' and $P'_{P'}$ have the same codimension, and so do $P' = PR[x]$ and P. Thus, one is through. □

The bounds in the previous theorem are attained in the generic case. Precisely, we have the following.

Theorem 6.4.6 (Eagon ([45])). *Let* $(\mathbf{X})$ *denote an* $m \times n$ *matrix of indeterminate entries over a Noetherian ring* R *and let* $1 \le t \le \min\{m, n\}$. *Then the grade of the ideal* $I_t(\mathbf{X})$ *is* $(m - t + 1)(n - t + 1)$.

Proof. By Theorem 6.4.5 and by the preceding observation, it suffices to show that the grade of $I_t(\mathbf{X})$ is at least $(m - t + 1)(n - t + 1)$.

Proceed by induction on t. For $t = 1$, the result is trivial since the generators themselves form an R-sequence. Thus, assume that $t > 1$ and let $\{u_1, \dots, u_g\} \subset I$ denote an R-sequence of maximal length in I. Set $J := (u_1, \dots, u_g)$. The elements of I are zero-divisors on R/J, hence $I \subset P$ for certain associated prime ideal of R/J. Clearly, all three ideals $J \subset I \subset P$ have the same grade g. Since $t > 1$ and $g \le (m - t + 1)(n - t + 1)$, then $g < mn$. This means that some entry of $(\mathbf{X})$ does not belong to P; one may assume $x_{1,1} \notin P$.

Next, pass to the ring of fractions $\widetilde{R} := R[\mathbf{X}][x_{1,1}^{-1}]$ and let $\widetilde{J} \subset \widetilde{I} \subset \widetilde{P}$ denote the corresponding extended ideals. Note that the image of the regular R-sequence is a regular $\widetilde{R}$-sequence and $\widetilde{P}$ is an associated prime of $\widetilde{R}/\widetilde{J}$, hence all three extended ideals still have grade g.

But now, one performs elementary row and column operations so as to make vanish all entries along the first row and column of the corresponding matrix $\widetilde{(\mathbf{X})}$ over $\widetilde{R}$, except $x_{1,1}$. It follows that $\widetilde{I}$ is generated by the $(t-1) \times (t-1)$ minors of the submatrix of $\widetilde{(\mathbf{X})}$ obtained by omitting its first row and column. It remains to show that one is in a position as to apply the inductive hypothesis, in which case one has

$$\operatorname{grade}(I) = \operatorname{grade}(\widetilde{I}) = \big(m - 1 - (t-1) + 1\big)\big(n - 1 - (t-1) + 1\big) = (m - t + 1)(n - t + 1),$$

as required.

Note that one is in a more delicate situation than the localization at the end of the proof of Proposition 6.4.5, as one has to make sure that the localization is still a polynomial ring over a Noetherian ring, that is to say, that $\widetilde{R}$ be a ring of polynomials over a Noetherian subring. For this, one observes that $\widetilde{R} = \overline{R}[\mathbf{Y}]$, where

$$\overline{R} := R[x_{1,1}, \dots, x_{1,n}; x_{2,1}, \dots, x_{m,1}, x_{1,1}^{-1}] \quad \text{and} \quad \mathbf{Y} = \{x_{i,j} - x_{i,1}x_{1,j}x_{1,1}^{-1}\}_{\substack{2 \le i \le m \\ 2 \le j \le n}}.$$

Now, since $\{x_{i,j}, 2 \le i \le m, 2 \le j \le n\}$ is an algebraically independent set over $\overline{R}$ and $x_{i,1}x_{1,i}x_{1,1}^{-1} \in \overline{R}$, then so is the set $\mathbf{Y}$. Therefore, up to a trivial isomorphism, $\widetilde{R}$ is of the desired form. □

Theorem 6.4.5 admits a version for symmetric matrices.

Theorem 6.4.7 (Kutz codimension theorem [100], [88]). *Let $\mathcal{S} = (a_{i,j})$ denote an $r \times r$ symmetric matrix with entries in a Noetherian ring R and let $1 \leq t \leq r$. If $I_t(\mathcal{S}) \neq R$, then it has codimension at most $\binom{r-t+2}{2}$.*

The proof is pretty much the same as above and is left to the reader.

Note that, in particular, the grade of an ideal I_t of t-minors in both cases is bounded likewise. To go over to the question of the perfection of I_t, as was done in the case of maximal minors, one would in principle need a candidate for a free complex of length equal the bound for the grade. In the case where $t = r-1$ (submaximal minors) and the matrix is square, there exist such explicit complexes, as one next describes.

6.4.2 The Scandinavian complex

Let $\mathcal{A}$ denote an $r \times r$ matrix over a Noetherian ring R and let $I := I_{r-1}(\mathcal{A})$ denote its ideal of $(r-1)$-minors. A first step would be to try to figure out the module of syzygies of I. A straightforward candidate comes from the relations reading off the cofactor equation

$$\mathcal{A}\mathcal{A}^c = \mathcal{A}^c\mathcal{A} = (\det \mathcal{A})\mathcal{I}_r,$$

where $\mathcal{A}^c$ denotes the matrix of the (signed) cofactors of $\mathcal{A}$. Namely, set to zero all entries off the diagonal in both products and in addition equate any two diagonal entries in those products. This gives a total of $2r(r-1) + \binom{r}{2} = 3r(r-1)$ syzygies, certainly much larger than the required rank $\mu(I) - 1 = r^2 - 1$. However, these are not all independent, which is a drawback in wishing for a minimal complex.

To correct this discrepancy, Gulliksen and Négard ([66]) devised a more conceptual way to figure out the "expected" number of syzygies.

Namely, let $\mathcal{R}$ denote the R-module of $r \times r$ matrices over R. Clearly, this is a free R-module of rank r^2. Consider the submodule of $\mathcal{R} \oplus \mathcal{R}$ generated by the pairs of matrices having the same rank. Let $\mathcal{G}$ denote the quotient of this module by the submodule generated by the image of the map $R \to \mathcal{R} \oplus \mathcal{R}$ given by $1 \mapsto (\mathcal{I}_r, \mathcal{I}_r)$. As it is easy to see, $\mathcal{G}$ is again a free R-module, this time of rank $2(r^2 - 1)$.

Lemma 6.4.8. *There is a complex of free R-modules*

$$\mathrm{GN}(\mathcal{A}) : 0 \to R \xrightarrow{\partial_4} \mathcal{R} \xrightarrow{\partial_3} \mathcal{G} \xrightarrow{\partial_2} \mathcal{R} \xrightarrow{\partial_1} R \to 0 \tag{6.4.8.1}$$

such that

(1) $\partial_1(\mathcal{R}) = I$

(2) $\mathrm{GN}(\mathcal{A})$ *is self-dual*

(3) I^2 *annihilates the homology* $H(\mathrm{GN}(\mathcal{A}))$.

Proof. One has to define the differentials ∂_i so that the resulting sequence of maps and free R-modules is indeed a complex. Having the assertion of items (1) and (2) in mind, one can see the differentials of $i = 1, 4$. The problem is of course, to define conveniently the differentials for $i = 2, 3$ so that they are given on certain bases by a matrix and its transpose.

For this, it is easier to define the differential in a basis-free manner, as follows:

$\partial_4(1) = \mathcal{A}^c$.

$\partial_3(\mathcal{B}) = \overline{(\mathcal{A}\mathcal{B}, \mathcal{B}\mathcal{A})}$, where the bar tells to take the residue modulo the cyclic R-submodule $R(\mathcal{I}_r, \mathcal{I}_r)$ (note that $\mathcal{A}\mathcal{B}$ and $\mathcal{B}\mathcal{A}$ have the same trace).

$\partial_2(\overline{(\mathcal{B}, \mathcal{C})}) = \mathcal{B}\mathcal{A} - \mathcal{A}\mathcal{C}$, which is well-defined since $R(\mathcal{I}_r, \mathcal{I}_r)$ maps to zero.

$\partial_1(\mathcal{B}) = \operatorname{trace}(\mathcal{A}^c\mathcal{B})$.

A direct calculation show that $\partial_3 \circ \partial_4 = 0$ and $\partial_2 \circ \partial_3 = 0$. To see that $\partial_1 \circ \partial_2 = 0$, use the cofactor equation and that $\mathcal{B}$ and $\mathcal{C}$ have the same trace by hypothesis.

Now one argues for the three additional assertions.

(1) Let $\{e_{i,j}\}$ denote the canonical basis of $\mathcal{R}$, with 1 sitting on slot (i, j) and zeros elsewhere. Then $\partial(e_{i,j})$ is the (i, j) cofactor of $\mathcal{A}$, a generator of I and, clearly, this exhausts all of its generators.

(2) The claim is that upon identifying R and $\operatorname{Hom}_R(R, R)$, one has an isomorphism of complexes $\operatorname{GN}(\mathcal{A}) \simeq \operatorname{Hom}_R(\operatorname{GN}(\mathcal{A}), R)$ inducing termwise R-module isomorphisms

$$\operatorname{GN}(\mathcal{A})_i \simeq \operatorname{Hom}_R(\operatorname{GN}(\mathcal{A}), R)_{4-i}$$

for $0 \leq i \leq 4$. To see this, one uses the isomorphism $\delta : \mathcal{R} \to \operatorname{Hom}_R(\mathcal{R}, R)$ mapping an element of the canonical basis to its symmetric in the dual basis. Then $(\delta, -\delta)$ induces an isomorphism $\mathcal{G} \simeq \operatorname{Hom}_R(\mathcal{G}, R)$.

(3) One compares with the Koszul complex $(K_\bullet(I, R), d)$, by using its head and tail. Coming from the head, one can lift to a map $f : \bigwedge^2 \mathcal{R} \to \mathcal{G}$ such that $f \circ d_2 = \partial_2$. Next, now using the tails of the two complexes, which coincide up to duality, and the dual of f, one arrives at the following commutative diagram:

$$\begin{array}{ccccccccccc}
0 & \to & \bigwedge^{r^2}\mathcal{R} & \to & \bigwedge^{r^2-1}\mathcal{R} & \to & \bigwedge^{r^2-2}\mathcal{R} & & & & \\
 & & \| & & \| & & \uparrow f^* & & & & \\
0 & \to & \operatorname{GN}(\mathcal{A})_4 & \to & \operatorname{GN}(\mathcal{A})_3 & \to & \operatorname{GN}(\mathcal{A})_2 & \to & \operatorname{GN}(\mathcal{A})_1 & \to & \operatorname{GN}(\mathcal{A})_0 \\
 & & & & & & \uparrow f & & \| & & \| \\
 & & & & & & \bigwedge^2\mathcal{R} & \to & \bigwedge^1\mathcal{R} & \to & \bigwedge^0\mathcal{R}
\end{array}$$

Comparing homologies throughout and using that I annihilates the Koszul homology, one sees that I annihilates as well the homology of $\operatorname{GN}(\mathcal{A})$ except possibly in degree 2.

For this degree, one needs a special argument. Having now seen quite a bit of the argument of the lemma, the reader is referred to [66] for this part of the proof. □

Theorem 6.4.9 (Scandinavian theorem [66]). *Let $\mathcal{A}$ denote an $r \times r$ matrix over a Noetherian ring R and let $I := I_{r-1}(\mathcal{A})$ denote its ideal of $(r-1)$-minors, where it is*

assumed that $I \neq R$. *Let* q *denote the largest among the integers* $i \geq 0$ *such that* $H_i(\mathrm{GN}(\mathcal{A})) \neq 0$. *Then* $\operatorname{grade} I + q = 4$.

Proof. One inducts on $\operatorname{grade} I$. The argument is similar to the one in the proof of Theorem 6.4.1 or even to that in the case of the ordinary Koszul complex because at the tail both complexes coincide. The rest of the details is left to the reader. □

Corollary 6.4.10. *Notation as in Theorem* 6.4.9. *One has* $\operatorname{grade} I \leq 4$ *and if equality holds and R is a Gorenstein ring then I is a perfect Gorenstein ideal.*

Remark 6.4.11. The result of the theorem extends to coefficients on a finitely generated R-module without any essential effort.

6.4.3 The Japanese–Polish complex

The next complex was established, independently, in [60] and [88]. It has strong similarities with the previous one, in that it takes care of the general collapsing when moving from arbitrary square matrices to symmetric ones. Thus, *e. g.*, the expected grade of the ideal of submaximal minors is now $\binom{r-(r-1)+2}{2} = 3$, hence a potential complex ought to have length 3.

Both constructions are inspired on the Eagon–Northcott methods. The version presented here is closer to [60] because it clarifies the strong relationship to the Scandinavian complex. Alas, it assumes that 2 is invertible in the ground ring—whereas [60] does not. This is however a typical assumption because the complex involves alternating matrices.

Lemma 6.4.12. *Let* $\mathcal{S}$ *denote an* $r \times r$ *symmetric matrix over a Noetherian ring R such that the image of* 2 *by the canonical map* $\mathbb{Z} \to R$ *is a unit. Let* $I \subset R$ *denote the ideal of submaximal minors of* $\mathcal{S}$. *Then there is a complex of free R-modules*

$$\mathrm{J}(\mathcal{S}) : 0 \to \mathrm{J}(\mathcal{S})_3 \xrightarrow{\partial_3} \mathrm{J}(\mathcal{S})_2 \xrightarrow{\partial_2} \mathrm{J}(\mathcal{S})_1 \xrightarrow{\partial_1} R \to 0 \tag{6.4.12.1}$$

such that:
(1) $\partial_1(\mathrm{J}(\mathcal{S})_1) = I$
(2) $\mathrm{J}(\mathcal{S})$ *is a direct summand of the complex* $\mathrm{GN}(\mathcal{S})$
(3) I^2 *annihilates the homology* $H(\mathrm{J}(\mathcal{S}))$.

Proof. With the same notation as in Lemma 6.4.8, let $\mathrm{J}(\mathcal{S})_1$ (resp., $\mathrm{J}(\mathcal{S})_3$) stand for the R-submodule of $\mathcal{R}$ of symmetric (resp., alternating) matrices and let $\mathrm{J}(\mathcal{S})_2$ denote the R-submodule of the matrices with zero trace.

Then define:
– $\partial_1(\mathcal{B}) = \operatorname{trace} \mathcal{S}^c\mathcal{B}$, where as before the upper subscript c refers to the corresponding matrix of cofactors.

- $\partial_2(\mathcal{B}) = \mathcal{B}\mathcal{S} + \mathcal{S}^t\mathcal{B}^t$, where the upper subscript t denotes the transpose.
- $\partial_3(\mathcal{B}) = \mathcal{S}\mathcal{B}$.

The reader can easily verify that these definitions make the above a complex.

Item (1) is again as in Lemma 6.4.8, while (3) follows from (2) and item (3) of Lemma 6.4.8.

To prove (2), one considers the following commutative diagram of chain complexes

$$\begin{array}{ccccccccccccc}
 & & 0 & \to & \mathrm{J}(\mathcal{S})_3 & \to & \mathrm{J}(\mathcal{S})_2 & \to & \mathrm{J}(\mathcal{S})_1 & \to & R & \to & 0 \\
 & & & & \downarrow \iota & & \downarrow \eta & & \downarrow \iota & & \| & & \\
0 & \to & R & \to & \mathcal{R} & \to & \mathcal{G} & \to & \mathcal{R} & \to & R & \to & 0 \\
 & & & & \downarrow \alpha & & \downarrow \zeta & & \downarrow \beta & & \| & & \\
 & & 0 & \to & \mathrm{J}(\mathcal{S})_3 & \to & \mathrm{J}(\mathcal{S})_2 & \to & \mathrm{J}(\mathcal{S})_1 & \to & R & \to & 0
\end{array}$$

where ι denotes inclusion, while the other maps are defined as follows:

- $\eta(\mathcal{B}) = \overline{(\mathcal{B}, -\mathcal{B}^t)}$
- $\zeta\overline{(\mathcal{B}, \mathcal{C})} = (\mathcal{B} - \mathcal{C}^t)/2$
- $\alpha(\mathcal{B}) = (\mathcal{B} - \mathcal{B}^t)/2$
- $\beta(\mathcal{B}) = (\mathcal{B} + \mathcal{B}^t)/2$.

It is now left to the reader to check that the three composite maps are the identity maps. □

And the main result is the following.

Theorem 6.4.13 (Japanese–Polish theorem). *Let $\mathcal{S}$ denote an $r \times r$ symmetric matrix over a Noetherian ring R such that the image of 2 by the canonical map $\mathbb{Z} \to R$ is a unit. Let $I \subsetneq R$ denote the ideal of submaximal minors of $\mathcal{S}$. If q denote the largest of the integers $i \geq 0$ such that $H_i(\mathrm{J}(\mathcal{S})) \neq 0$, then* grade $I + q = 3$.

Proof. One inducts on grade I. As before, the main step is grade $I = 0$, whereby one wishes to show that the homology at the tail of the complex does not vanish—the rest of the proof when grade $I > 0$ is pretty much the same argument as in the case of the Eagon–Northcott and the Scandinavian complexes.

Thus, let $I \subset 0 : a$, for some $0 \neq a \in R$. Setting $\overline{R} := R/0 : a$ and $\overline{\mathcal{S}}$ for the symmetric matrix obtained by replacing the entries by their residues, it is easy to see the change of base property $\mathrm{J}(\overline{\mathcal{S}}) \simeq \mathrm{J}(\mathcal{S}) \otimes_R \overline{R}$. Therefore, one may assume that $I = \{0\}$, hence the updated matrix has rank $\leq r - 2$. On the other hand, one can assume, by localizing at an associated prime of R, that $(R, \mathfrak{m})$ is local and grade $\mathfrak{m} = 0$. Since coker ∂_3 has homological dimension ≤ 1 then in this scenario it must be free. It follows that ∂_3 is split injective, and hence one can move over to the residue field and assume that R is a field of characteristic $\neq 2$. In this setup, $\mathcal{S}$ is diagonalizable and since its rank is $\leq r-2$,

there is an invertible matrix $\mathcal{P}$ such that $(\mathcal{P}^t\mathcal{S}\mathcal{P})\mathcal{A} = 0$, where

$$\mathcal{A} = \left(\begin{array}{c|cc} \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & 0 & 1 \\ \mathbf{0} & -1 & 0 \end{array}\right)$$

But then one has $\mathcal{S}(\mathcal{P}^t\mathcal{A}\mathcal{P}^t) = 0$, with $\mathcal{P}^t\mathcal{A}\mathcal{P}^t \neq 0$, which gives a nonvanishing cycle in degree 3—a contradiction. □

Remark 6.4.14.

(1) Note that the path of the proof in the last theorem is similar to the one in the case of the Eagon–Northcott complex, by reducing the matrix to a simplest shape where one can easily devise a nonvanishing cycle at the tail of the complex.

(2) All complexes thus far are *generically perfect*; in particular, they are acyclic when the entries of the matrix form a regular sequence. Unfortunately, for lower size of minors such complexes would much harder to write down even in the case of indeterminate entries over a field, where it might depend on the characteristic of the latter.

Fortunately, the theory of generic perfection ([47], [76]) came to the rescue. This is a grand piece of hard algebra which, regrettably, will have to be told somewhere else. The reader is also referred to [27] for a more recent review of the theory.

6.4.4 The Osnabrück–Recife complex

The next complex is inspired by the study of the complexes resolving ideals of minors fixing a subset of columns. These ideals have been introduced as early as [76] and have been thoroughly reexamined in [27]. A generalization of such ideals have been recently considered in [115] particularly in regard to their primary decomposition—the methods are those of poset theory and of algebras with straightening law.

A more precise explanation is as follows. One considers an $n \times m$ ($n \leq m$) matrix $\mathcal{A}$ with entries in a ring R and an $n \times r$ submatrix $\mathcal{A}_r$, with $1 \leq r \leq n-1$. The main character is the subideal $J_r \subset I_n(\mathcal{A})$ generated by the n-minors fixing $\mathcal{A}_r$. Under the correct hypotheses on the grade of the various ideals of minors involved (which are automatically satisfied in the case where the entries of $\mathcal{A}$ are indeterminates over a field), the free resolution of J_r has been written down in the following cases ([2], [3], [4]):

- $r = n-1$ and $n \leq m$ arbitrary.
- $m = n+1$ and r arbitrary.
- $m = n+2$ and $r = n-2$.

The resolutions are obtained as suitable modification of the Buchsbaum–Rim complexes ([29])—in the third case, one introduces additionally a certain Cramer map and the trace map. Ideal theoretically, a difference among the above cases is that in the first two cases the ideal is non-unmixed, but of linear type, while in the third case the ideal is unmixed, but not of linear type.

In general, one has the following.

Conjecture 6.4.15. *Let R be a Noetherian ring. Suppose that* $\operatorname{grade} I_n(\mathcal{A}) \geq m - n + 1$, $\operatorname{grade} I_r(\mathcal{A}_r) \geq n - r + 1$ *and that* $(I_n(\mathcal{A}), I_r(\mathcal{A}_r))$ *is a proper ideal of grade* $\geq m - r + 1$. *Then* $\operatorname{hd}_R(R/J_r) = m - r$.

Some of the above discussion can be converted to modules, as follows from the work of W. Bruns and this author ([26]). Namely, let R be a Noetherian ring and let $\mathcal{A} = (x_{i,j})$ denote an $m \times n$ generic matrix over R, with $m \geq n$. Let M be the cokernel of the map defined by this matrix. Therefore, M is a finitely generated R-module such that $\operatorname{hd}_R(M) = 1$, with free resolution

$$0 \to R^n \xrightarrow{\mathcal{A}} R^m \longrightarrow M \to 0.$$

Fix an integer $1 \leq r \leq n$ and a decomposition $R^m = F \oplus G$. Pick a free basis $\{e_1, \ldots, e_m\}$ of R^m such that $F = \sum_{k=1}^{r} e_k$ and $G = \sum_{k=r+1}^{m} e_k$.

Thinking about $\mathcal{A}$ as an R-map, define $M_r := \mathcal{A}(G) \subset M$, the image of G under the restriction of $\mathcal{A}$. Let $\mathcal{A}_r : R^n \to F$ denote the composite of $\mathcal{A}$ and the projection $R^m \twoheadrightarrow F$ induced by the chosen basis.

Introduce a new R-map $\zeta : \bigwedge^{r+1} R^n \to G$ as the composite of the natural map $\bigwedge^{r+1} R^n \to \bigwedge^{r+1} R^m$ and the map $\xi : \bigwedge^{r+1} R^m \to G$ defined in the following way:

$$\xi(e_{i_1} \wedge \cdots \wedge e_{i_r}, \mathrm{e}_k) = \begin{cases} e_k, & \text{if } i_l = l, \text{ for } 1 \leq l \leq r, \text{ and } r+1 \leq k \leq m \\ 0, & \text{otherwise} \end{cases}$$

Consider the Buchsbaum–Rim complex ([29]) resolving $\mathcal{A}_r$:

$$\begin{aligned} 0 \to S_{n-r-1}(F^*) \otimes \bigwedge^{n} R^n \to S_{n-r-2}(F^*) \otimes \bigwedge^{n-1} R^n \to \cdots \to S_1(F^*) \otimes \bigwedge^{r+2} R^n \\ \xrightarrow{\eta} \bigwedge^{r+1} R^n \xrightarrow{\epsilon} R^n \xrightarrow{\mathcal{A}_r} F^*, \end{aligned}$$

where $*$ denotes R-dual. Let $\mathcal{C}_r$ denote the chain of maps obtained from the above by trading the two right most differentials by the map ζ.

Theorem 6.4.16 (Osnabrück–Recife theorem). *$\mathcal{C}_r$ is a free resolution of M_r over R.*

Proof. One first has to argue that $\mathcal{C}_r$ is indeed a complex, *i. e.*, that $\zeta \circ \eta = 0$. By the definition of η in [29], letting e_i^* denote the dual basis element corresponding to e_i, and letting $\{f_1, \ldots, f_n\}$ stand for a basis of R^n, one has

$$\eta(e_i^* \otimes f_{j_1} \wedge \cdots \wedge f_{j_{r+2}}) = \sum_k \pm \mathcal{A}_r(f_{j_k})(e_i) f_{j_1} \wedge \cdots \wedge \widehat{f_{j_k}} \wedge \cdots f_{j_{r+2}}$$
$$= \sum_k \pm x_{i,j_k} f_{j_1} \wedge \cdots \wedge \widehat{f_{j_k}} \wedge \cdots f_{j_{r+2}}$$

Applying ζ yields the element

$$\sum_{k=r+1}^{m} \left(\sum_j \pm x_{i,j} \Delta^{j_1,\ldots,\hat{j},\ldots,j_{r+2}}_{1,\ldots,r,k} \right) e_k \in G.$$

But, for fixed k, the summation inside the parentheses is the Laplace relations of the maximal minors of the $(r+2) \times (r+1)$ submatrix of $\mathcal{A}$ with columns $1, \ldots, r, k$ and rows $j_1, \ldots, j_{r+2}$, hence they vanish.

Therefore, one has a complex indeed.

Claim 1. $\mathcal{C}_r$ is exact at G.

By looking at the definition of ζ, it suffices to show that the kernel of the augmentation $G \twoheadrightarrow M_r$ is generated by the elements of the form $\sum_{k=r+1}^{m} \Delta^{j_1,\ldots,j_{r+1}}_{1,\ldots,r,k} e_k$, for all choices of $\{j_1, \ldots, j_{r+1}\} \subset \{1, \ldots, n\}$. This is a more or less standard calculation using Cramer rule—one refers to [26] or leaves it to the reader.

Claim 2. $\mathcal{C}_r$ is exact at $\bigwedge^{r+1} R^n$.

Since $\operatorname{coker} \eta \simeq \operatorname{im}(\epsilon)$ (in the Buchsbaum–Rim complex) is torsion-free and mapped onto $\operatorname{im}(\zeta)$, it suffices to show that $\operatorname{coker} \eta$ and $\operatorname{im}(\zeta)$ have the same rank. But this is clear as one has: $\operatorname{rank} \operatorname{im}(\zeta) = \operatorname{rank} G - \operatorname{rank} M_r = n - r = \operatorname{rank} R^n - \operatorname{rank} F = \operatorname{rank} \operatorname{coker} \eta$. □

Corollary 6.4.17. $\operatorname{hd}_R(M_r) = n - r$.

Proof. By the theorem, $\operatorname{hd}_R(M_r) \leq n - r$. Since $\operatorname{coker}(\mathcal{A}_r)$ has homological dimension $n - r + 1$ by the Buchsbaum–Rim result, one must have equality. □

This is as much as will be covered about determinantal ideals in this book. For further results and the state-of-the-art of the subject the reader is referred to [75], [76], [74] and [27] (the last of these references contains pretty much most of the material previously known).

6.5 Historic note

6.5.1 Projective modules

The terminology was inaugurated in the book of Cartan–Eilenberg ([32]) and was possibly inspired from the idea of a projection. The natural question arises at this point as to why one would care to introduce an almost obvious generalization of the notion of a free module instead of just working with the latter. In order to understand the choice

of projective modules in homology theory, the reader will have to await a few steps in the theory. At the other end, the notion came very handy for geometric purposes as it can be confronted with the notion of a vector bundle over an algebraic variety (see [136], also [139] for an elementary exposé). This facet of a projective module aroused an intense literature in past years on rings for which every finitely generated projective module is free, in the footsteps of what became known as "Serre's conjecture" for projective modules over a polynomial ring. Graded projective modules are in turn a lot easier to deal with, as are their generalization over noncommutative rings. This was originally tackled in [32], later reworked in [50] and [51]. A simple case is that of finitely generated graded modules over a standard graded polynomial ring over a field, which can be carried out like in Proposition 6.2.3.

6.5.2 Homology

The history of homological algebra since its dawn goes back to the second half of the nineteenth century with the work of B. Riemann and E. Betti. An excellent source on the matter, containing a detailed mathematical discussion, is the survey by C. Weibel ([163]). Homology has become an essential tool for commutative algebra in the footsteps of the book of H. Cartan and S. Eilenberg ([32]), with the deep work of M. Auslander and D. Buchsbaum ([7, 8, 9, 10]), J.-P. Serre ([135, 138]), and D. Rees ([128, 129]).

6.5.3 Injective modules

(More a justification than a historic piece.) The whole body comes from the functor $\mathrm{Hom}(M, \_)$, where M is a fixed R-module. Thus, this is a functor of the "second variable" and, as such it is a covariant functor. Moreover, it is also left-exact. If one tries to define a derived functor ${}^i\mathrm{Ext}_R(M, \_)$ by means of taking a projective resolution of a given module N in order to grab the definition of ${}^i\mathrm{Ext}_R(M, N) := {}^i\mathrm{Ext}_R(M, \_)(N)$ one is quickly lead to a bizarre behavior. Since one is aiming at a definition that hopefully implies a natural isomorphism ${}^i\mathrm{Ext}_R(M, N) \simeq \mathrm{Ext}^i_R(M, N)$ for all $i \geq 0$, this hope will be dashed.

For a simple example, let $a \in R$ denote a regular element and $M = N = R/(a)$. Applying $\mathrm{Hom}(R/(a), \_)$ to the free resolution $0 \to R \xrightarrow{\cdot a} R \longrightarrow R/(a) \to 0$ of the second variable $R/(a)$ and truncating as usual in the rightmost term, one gets a complex whose terms are either $\mathrm{Hom}(R/(a), R)$ or zero; but $\mathrm{Hom}(R/(a), R) = 0$ as well as a is regular. Therefore, ${}^i\mathrm{Ext}_R(R/(a), R/(a)) = 0$ for every $i \geq 0$. However, on the other hand, $\mathrm{Ext}^i_R(R/(a), R/(a)) \simeq R/(a)$, for $i = 0, 1$ as one readily verifies by the definition.

This tells that projective resolutions are no longer applicable for $\mathrm{Hom}(R/(a), \_)$ if one wishes to recover the previous definition. The salvation comes through the notion of injective resolutions (of the second variable for the case on the agenda). Naturally,

this presupposes the notion of an injective module. The theory has a high degree of sophistication and requires a long exposition, so it would have been required to dedicate a substantial part of the chapter to fill in all details that are expected in a textbook. In addition, given the overall style of the book, doing this at this point would have been a slight anticlimax at the point.

Alas, as it often happens, the inception of this concept had very little to do with the present need to devise an injective resolution, having first being studied by R. Baer ([12]) in connection with a problem related to split inclusions $G \subset G'$ of Abelian groups, for a fixed G and arbitrary G'. According to C. Weibel ([163]), the terminology is apparently due to S. Eilenberg.

6.5.4 Determinantal ideals

The history of matrices and determinants goes back as far as a few centuries before our era. An interesting account can be found in *MacTutor History of Mathematics* and, most certainly, in many other appropriate sources. From the viewpoint of commutative algebra, a few discoveries along the way proved to be more critical than others. Thus, for example, a spectacular consequence of Sylvester's work on submatrices and ranks—although not foreseen by him—is the consideration of the ideal generated by the t-minors of a matrix A, here denoted $I_t(A)$. Clearly, the full nature of this ideal would not come up when taking the ground ring to be a field (except to declare whether it vanishes or not). Yet, regardless of the nature of the ground ring, one of the beautiful properties of the ideal of minors is its invariance under conjugation, to wit, $I_t(A) = I_t(VAW)$, where U, W are invertible matrices of order $m \times m$ and $n \times n$, respectively. In other words, the ideal is invariant under the action of the product group $\mathrm{GL}(m, R) \times \mathrm{GL}(n, R)$ on the set of $m \times n$ matrices with entries in the ring R. After such a realization, these ideals ought to have a special designation. For this, one would have to wait about half a century after Sylvester, with the work of the German mathematician Hans Fitting, and then only after the notion of a module was well known. Fitting proved the spectacular result about these ideals that is given in the book, namely, that for a finitely generated module M the ideals of minors of a matrix presentation of M are invariant of M. However, as has been seen earlier in the book, to make it work one has the to reverse the size t of the minor to $e - t$, whenever the matrix comes up by choosing a set of e generators of M. As a due recognition of this surprisingly strong invariance of the ideals of minors, they are often called *Fitting ideals*. Perhaps the most remarkable use of the Fitting ideals was the parallel study taken up by Kähler of the so-called *Kähler differents*, which had a strong impact in the theory of differentials. There were many kinds of differents (Dedekind, Noether), some of which give a hard time to compute, so it is nice to know that one of these has a determinantal character (*cf.* Section 4.4).

Two important subsequent developments took place: the systematic use of determinantal ideals in classical invariant theory and the advent of part of combinatorics, as related to poset theory and straightening law, giving a tremendous recharge to the classical knowledge. Regrettably, neither account could be included in the book, both for reason of space and for its uselessness due to the existence of existing appropriate accounts.

6.6 Exercises

Exercise 6.6.1. Let $R = k[x_1, \dots, x_n]$ be a polynomial ring over a field k and let $P \subset R$ be a prime ideal.

(i) Show, without using the Serre–Vasconcelos theorems, that R_P is regular.
(Hint: establish the existence of a *primbasis* as follows: if $d = \operatorname{trdeg}_k(R/P)$, assume that $x_1, \dots, x_d$ are k-algebraically independent modulo P; localize at the multiplicatively closed subset $\mathfrak{S} := k[x_1, \dots, x_d] \setminus \{0\}$ and show that $\mathfrak{S}^{-1}P$ is a maximal ideal of $\mathfrak{S}^{-1}R$.)

(ii) Write an explicit primbasis for the following prime ideals: (1) $P = (x^2 - yz, y^2 - xz, z^2 - xy)$; (2) $P = (x^2 - yz, y^2 - xz, z^2 + xy)$; (3) $P =$ the homogeneous defining ideal of the rational normal cubic in $\mathbb{P}^3_k$; (4) $P =$ the homogeneous defining ideal of the rational nonnormal quartic in $\mathbb{P}^3_k$.

Exercise 6.6.2. Write explicit free resolutions for each of the prime ideals P in item (ii) of the previous exercise. What happens to the shape of these resolutions by localizing at P?

Exercise 6.6.3. Write the shape of the (nonfinite) free resolutions of the following ideals:

(1) The maximal ideal of $k[x, y]_{(x,y)}/(y^2 - x^3)_{(x,y)}$.
(2) The ideal generated by the residues of x, z in $k[x, y, z]_{(x,y,z)}/(z^2 - xy)_{(x,y,z)}$.
(3) The maximal ideal of $k[x, y, z]_{(x,y,z)}/(xy, xz, yz)_{(x,y,z)}$.

Exercise 6.6.4. Consider the 2×4 generic matrix over a field

$$(\mathbf{x}) = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_5 & x_6 & x_7 & x_8 \end{pmatrix}.$$

Let $I \subset R = k[\mathbf{x}]$ denote the ideal generated by the 2-minors fixing the first column.

(i) Prove that I is a radical, non-unmixed, generically complete intersection ideal of height 2, finding its associated primes.

(ii) Give the explicit free resolution of I.
(Hint: besides the 3 trivial (Koszul) syzygies, an additional syzygy comes from the Plücker equation of the 2-minors. For a full generalization of this result, see [2].)

(iii) Prove that I is of linear type.
(iv) Prove that the Rees algebra of I is Cohen–Macaulay.
(Hint: show that the symmetric algebra of I is Cohen–Macaulay, a property that follows from since I is an almost complete intersection, provided the bound $\operatorname{depth} R/I \geq \dim R/I - 1$ takes place.)
(v) Deduce that $\operatorname{gr}_I(R)$ is Cohen–Macaulay and prove that $\operatorname{gr}_I(R)$ is not Gorenstein.

Exercise 6.6.5. Let $R = k[x_1, \ldots, x_6, y]$ be a polynomial ring in 7 variables and let $I = (x_1x_2, x_2x_3, x_3x_4, x_4x_5, x_5x_6, x_1x_6, x_1y, x_3y, x_5y)$.
(i) Find generators for the defining ideal of the fiber cone $\mathcal{F}(I)$ (Section 7.3.3).
(Hint: if it becomes easier, think about the generators of I as coming from the edge ideals of a simple graph on 7 vertices.)
(ii) Deduce the value $\ell(I)$ of the analytic spread of I.
(iii) Show that the defining ideal of $\mathcal{F}(I)$ is Cohen–Macaulay of linear type.

Exercise 6.6.6. Consider the ideal $I \subset k[x_1, \ldots, x_6]$ generated by the following polynomials:

$$f_1 = x_2x_4 + x_3x_6, \quad f_2 = x_3x_5 + x_1x_6, \quad f_3 = x_1x_2 - x_2x_5 + x_3x_5 - x_5x_6,$$
$$f_4 = x_2x_3 + x_2x_4 + x_2x_6 + x_6^2 \quad f_5 = x_3^2 + x_3x_4 + x_3x_6 - x_4x_6,$$
$$f_6 = x_1x_3 + x_1x_4 + x_4x_5 + x_1x_6,$$

discussed in Exercise 5.6.12. Discuss as much as possible the following assertions, before moving on to computer algebra program:
(i) I has a linear resolution of the shape

$$0 \to R(-4)^3 \to R(-3)^8 \to R(2)^6 \to I \to 0.$$

(ii) The Jacobian matrix of the generators of I has rank 5; hence $\ell(I) = 5$.
(iii) The generator of the ideal of the fiber cone $\mathcal{F}(I)$ is a quadric.
(iv) Let Φ (resp., $\tilde{\Phi}$) the one-column syzygy of the Jacobian (resp., transposed Jacobian) matrix of I.
- Show that $I_1(\tilde{\Phi}) = I$.
- The ideal $I_1(\Phi)$ has height 2 and homological dimension 2.
- The minimal free resolution of $I_1(\Phi)$ has the form

$$0 \to R \xrightarrow{\Psi} R^6 \to R^6 \to I_1(\Phi) \to 0$$

and $I_1(\Psi) = I$.

Exercise 6.6.7. Let $R = k[x, y, t, u]$ be a polynomial ring over a field k and let $m \geq 1$ be an integer. Set $I = (xt - yu, (t, u)^m)$ (called an *m-multiplicity structure* on the line $t = u = 0$).

(i) Show that I is a (t,u)-primary ideal and has a free resolution of the following shape:

$$0 \to R(-(m+2)^{m-1} \to R(-(m+1))^{2m} \to R(-m)^{m+1} \oplus R(-2) \to I \to 0.$$

(ii) (Geramita–Maroscia–Vogel) Prove that I is not self–linked, *i.e.*, for any R-sequence of forms f,g in I, one has $I \neq (f,g) : I$.
(Hint: if $I = (f,g) : I$ then $I/(f,g) \simeq \operatorname{Ext}^2_R(R/I,R)$; then dualize the free resolution into R and make all complex maps explicit to deduce that $\{f,g\}$ would have to be part of a minimal set of generators of I^2; a calculation will show this is impossible.)

Exercise 6.6.8. Let $(R,\mathfrak{m})$ be a Noetherian local ring and let M be a finitely generated R-module of homological dimension ≤ 1. Prove the zero-divisor theorem in this case: if $a \in \mathfrak{m}$ is M-regular then it is regular.

Exercise 6.6.9. Let $(R,\mathfrak{m})$ be a Noetherian local ring and $I = (\mathbf{a}) = (a_1,\dots,a_n) \subset \mathfrak{m}$ an ideal.

(1) Show that $\sqrt{0 : H_i(\mathbf{a};R)} \subset \sqrt{0 : H_{i+1}(\mathbf{a};R)}$.

(2) Let $\mathbf{b} \subset I$ denote a maximal R-sequence. Show that

$$\dim R/I \geq \dim H_i(\mathbf{a};R) \geq \dim R/(\mathbf{b} : (\mathbf{b} : I)),$$

for $0 \leq i \leq n$.

(3) Suppose that R is Cohen–Macaulay. Prove that $\dim \dim H_i(\mathbf{a};R) = \dim R/I$, for $0 \leq i \leq n$.
(Hint: if R is Cohen–Macaulay and I has grade zero then $\dim R/I = \dim R/(0 : (0 : I))$-for this, argue that for a prime ideal $P \subset R$ such that $\dim R/I = \dim R/P$ one has $0 : (0 : I) \subset P$.)

Exercise 6.6.10. Let R be a Noetherian ring and $I = (\mathbf{a}) = (a_1,\dots,a_m) \subset R$ an ideal. Consider a free presentation $R^n \xrightarrow{\varphi} R^m \to I \to 0$.

(i) Show that there is an exact sequence of R-modules

$$0 \to \delta(I) \to H_1(\mathbf{a};R) \to (R/I)^m \to I/I^2 \to 0,$$

where $\delta(I) = Z \cap IR^m/B(\mathbf{a};R)$, where $Z = \ker(\varphi)$ and $B(\mathbf{a};R)$ denotes the first boundary module of $K(\mathbf{a};R)$.

(ii) Give an argument showing that $\delta(I)$ does not depend on the chosen set of generators of I.

(iii) If R is local, show that if $H_1(\mathbf{a};R)$ is a torsion-free R/I-module then $\delta(I) = \{0\}$.

(iv) If R is local, show that if $\delta(I) = \{0\}$ and I/I^2 is (R/I)-free then I is generated by an R-sequence.

(v) (Gulliksen–Levin) If $H_1(\mathbf{a};R)$ is (R/I)-free then I is generated by an R-sequence.
(Hint: this is quite more difficult; see [65].)

Exercise 6.6.11 (Complements to the previous exercise ([140])). Let R be a Noetherian ring and let $I \subset R$ be an ideal.

(i) Prove that $\delta(I) \simeq \operatorname{Tor}_1^R(I, R/I)/\mathcal{A}(\bigwedge^2 I)$, where $\mathcal{A} : \bigwedge^2 I \to \operatorname{Tor}_1^R(I, R/I)$ is the anti-symmetrization map $u \wedge v \mapsto u \otimes v - v \otimes u$.

(ii) Deduce that $\delta(I) \simeq \mathcal{S}_2(I) \to \mathcal{R}_2(I)$.

(iii) Compute $\delta(P)$, where P is the defining ideal of the fiber cone in Exercise 6.6.5.

Exercise 6.6.12. Write the Eagon–Northcott resolution of the ideal $I = I_2(\mathcal{A})$, where $\mathcal{A} = (x_{i,j})$ is the generic 2×4 matrix over a field.

(i) Justify that the syzygies of I are the usual Laplace–Cramer relations of a 2×3 submatrix.

(ii) Let ψ denote the left most map in the complex. Argue that the unmixed part of the ideal $I_3(\psi)$ is I and $(x_{i,j})$ is an embedded prime.

Exercise 6.6.13. Write the Scandinavian resolution of the ideal $I = I_2(\mathcal{A})$, where $\mathcal{A}$ is the generic 3×3 matrix over a field.

(i) Explain the syzygies with only 3 nonzero coordinates in the same light as (i) of the previous exercise. What about the other syzygies requiring at least 4 nonzero coordinates?

(ii) Give a maximal regular sequence of I in degree 2.

Exercise 6.6.14. Pursue the case of the resolution of $I = I_2(\mathcal{S})$ (where $\mathcal{S}$ is 3×3 symmetric) along the same line of inquiry as in the two previous exercises.

7 Graded structures

In this book, one focuses exclusively the case of "singly" graded structures, as opposite to the more comprehensive "multigraded" structures. Though the latter is a well established piece of modern mathematics, and in fact there is a reasonable notion of Hilbert function in this context—starting with the pioneering work by van der Waerden in [154]—it seems to this author that a full theory with marked differences is not sufficiently stable as to appear in a textbook of general scope such as this.

Of course, the curious reader will have no difficulty in fetching more advanced texts and papers where the multigraded setup is dealt with.

7.1 Graded preliminaries

One has already met special cases of graded structures as related to the definition of the Hilbert function of a homogeneous polynomial ideal (Section 2.7). Here, one gives a more encompassing treatment of these notions.

Definition 7.1.1. Let A be a commutative ring and let $\mathbb{G}$ be a commutative monoid (additive notation). A $\mathbb{G}$-*graded algebra* is a commutative A-algebra with a decomposition into a direct sum of additive subgroups

$$R = \bigoplus_{u\in\mathbb{G}} R_u,$$

such that $R_0 = A$ and $R_u R_v \subset R_{u+v}$ for all $u, v \in \mathbb{G}$. In particular, each R_u is an A-module and called the *component* or the *homogeneous part of degree* u of R. The algebra R is said to be endowed with a $\mathbb{G}$-*grading*.

A $\mathbb{G}$-*graded* R-*module* M is defined similarly as an R-module possessing a decomposition into a direct sum of subgroups

$$M = \bigoplus_{u\in\mathbb{G}} M_u,$$

such that $R_u M_v \subset M_{u+v}$ for all $u, v \in \mathbb{G}$. It follows, in particular, that each M_u is an A-module.

Typically, in the book all graded modules are finitely generated.

This definition is general enough to encompass the multigraded case as well as sufficiently prone to be transported to the so-called super algebras. However, as said above, one will be particularly focused, by assuming throughout that $\mathbb{G}$ is either $\mathbb{N}$ or $\mathbb{Z}$—while in the multigraded setup, one would typically use $\mathbb{N}\times\cdots\times\mathbb{N}$ or $\mathbb{Z}\times\cdots\times\mathbb{Z}$, respectively. In this case, one will be talking about $\mathbb{N}$-grading or $\mathbb{Z}$-grading.

Example 7.1.2. The foremost and simpler example is that of a polynomial ring A over a field $A = k$, endowed with an $\mathbb{N}$-grading as introduced in Section 2.7. This grading is so

https://doi.org/10.1515/9783110616989-007

natural that it has been awarded the name *standard grading*. Note that, as a k-algebra, it is generated by the homogeneous part of degree $1 \in \mathbb{N}$.

More generally, for any commutative ring A, an A-algebra R is said to be a *standard graded* A-algebra if it is $\mathbb{N}$-graded and finitely generated by elements of degree one. Any such algebra is exactly the residue algebra of some standard polynomial ring $R = A[x_1, \dots, x_n]$ by a certain *homogeneous* (*i. e.*, $\mathbb{N}$-graded) subideal of R. Important examples of this generality are the symmetric algebras, Rees algebras and form rings, all studied in the upcoming sections.

Graded structures have a strategic mobility through a so-called *degree shifting* or *degree translation*. Namely, if M is a $\mathbb{G}$-graded module over a $\mathbb{G}$-graded ring R, given any $v \in \mathbb{G}$, one defines $M(v)$ by means of setting $M(v)_u := M_{u+v}$. One then speaks informally of this procedure as being the v-shifted module of M.

A useful application is to transform any graded homomorphism of graded modules into one mapping elements of a given degree in the source to elements of the same degree in the target—such shifted homomorphisms being often called *homogeneous*, if no confusion arises. Thus, for example, let M be a $\mathbb{G}$-graded module finitely generated by elements of degrees $u_1, \dots, u_m$. Then the usual free presentation map $R^m \longrightarrow M$ induced by this set of generators becomes a surjective homogeneous homomorphism $R(-u_1) \oplus \cdots \oplus R(-u_m) \longrightarrow M$, where the source module is still the same free module R^m, that was generated in degree 0 by the natural basis, only now with shifted degrees for the elements of this basis, so that the map becomes homogeneous (of degree 0). This map is mostly interesting when it is extended by its kernel, which is a graded submodule, then repeating the procedure. Namely, one gets a *graded free presentation*

$$\bigoplus_j R(-v_j) \longrightarrow \bigoplus_i R(-u_i) \longrightarrow M \to 0$$

The presentation is said to be *linear*—or that M has linear syzygies—if $u_i = u$ for every i and $v_j = u + 1$ for every j. Linear presentation has a pervasive role throughout the theory.

This procedure is of course pretty general, so by iteration one can talk about graded homogeneous free complexes of graded modules and, in particular, about free graded homogeneous resolutions. For word saving, one normally omits the term "homogeneous" in the hope that saying "graded" complies with the full meaning intended.

Thus, a typical *finite free graded resolution* may be written as

$$0 \to \bigoplus_j R(-v_{d,j})^{\beta_{d,j}} \to \bigoplus_j R(-v_{d-1,j})^{\beta_{0,j}} \to \cdots \to \bigoplus_j R(-v_{0,j})^{\beta_{d-1,j}} \to M \to 0, \quad (7.1.2.1)$$

where one has used the same symbol for the current index in each graded term of the complex. The exponents $\beta_{i,j}$ are called the *graded Betti numbers* of M (see Definition 6.2.60). The resolution is said to be *pure* if $v_{i,j} = v_i$ for all i, j, and *linear* if it is pure and, moreover, $v_i = v_{i-1} + 1$, for all i.

7.2 The symmetric algebra

Departing from the previous notation R for a ring, let A denote a commutative ring and let M denote an A-module. The symmetric algebra $\mathcal{S}(M) = \mathcal{S}_A(M)$ of M is the most basic commutative algebra associated to M. The basic definition, already given in Section 3.2, is recorded anew for the reader convenience.

Definition 7.2.1. Let $T_A(M) = \bigoplus M^{\otimes t}$ denote the graded tensor algebra of M—also known as the free algebra generated by M. Then $\mathcal{S}_A(M) := T_A(M)/\mathfrak{C}$, where $\mathfrak{C}$ is the two-sided ideal generated by the elements of the form $e \otimes e' - e' \otimes e$, for all $e, e' \in M$.

One can check that any iterated "symmetrization"

$$\cdots \otimes e \otimes \cdots \otimes e' \otimes \cdots - \cdots \otimes e' \otimes \cdots \otimes e \otimes \cdots$$

lies in $\mathfrak{C}$, and hence the latter can be given as the two-sided ideal generated by all such iterations.

Note that $\mathcal{S}_A(M)$ acquires a grading from the tensor algebra. Let $\mathcal{S}^t(M) \subset \mathcal{S}(M)$ denote its tth graded piece, called the tth *symmetric power* of M. In particular, $\mathcal{S}^0(M) = A$, $\mathcal{S}^1(M) = M$. As such, $\mathcal{S}_A(M)$ is a standard graded A-algebra since it is generated in degree 1 over A.

Lemma 7.2.2 (Universal property). *Let A and M be as above. Given an A-module map $\varphi : M \longrightarrow B$, where B is a commutative R-algebra, then there is a unique A-algebra homomorphism $\mathcal{S}_A(M) \longrightarrow B$ whose restriction to the first symmetric power $\mathcal{S}^1(M) = M$ is φ.*

Proof. Left to the reader. □

As an easy application, one can see that if F is a free A-module with basis $\mathfrak{B}$ then $\mathcal{S}_A(F)$ is isomorphic as graded A-algebra to the polynomial ring $A[\mathbf{X}_{\mathfrak{B}}]$, where $\mathbf{X}_{\mathfrak{B}}$ denotes a set of indeterminates over A in bijection with $\mathfrak{B}$.

In general, one is interested in getting a hold of the defining equations of $\mathcal{S}_A(M)$, *i. e.*, of the nature of the ideal $\ker(A[\mathbf{X}_\alpha] \twoheadrightarrow \mathcal{S}_A(M) = \mathcal{S}_A(\sum A\mathfrak{g}_\alpha))$, $\mathbf{X}_\alpha \mapsto \mathfrak{g}_\alpha$, where $\{\mathfrak{g}_\alpha\}$ is a set of generators of M. This ideal can be understood theoretically in the following way.

Lemma 7.2.3. *Let $F_1 \xrightarrow{\Phi} F_0 \longrightarrow M \to 0$ stand for a free presentation of M as an A-module, associated to a given set $\{\mathfrak{g}_\alpha\}$ of generators of M. Then*

$$\mathcal{S}_A(M) \simeq A[\mathbf{X}_\alpha]/\mathfrak{I},$$

with $\mathfrak{I}$ the ideal generated by the image of the A-algebra map $\mathcal{S}(\Phi) : \mathcal{S}_A(F_1) \longrightarrow A[\mathbf{X}_\alpha]$ in degree 1.

Proof. The proof is obtained by applying the universal property along the given presentation, thus getting a polynomial presentation of $\mathcal{S}_A(M)$

$$\mathcal{S}_A(F_1) \xrightarrow{\mathcal{S}(\Phi)} A[\mathbf{X}_\alpha] \longrightarrow \mathcal{S}_A(M) \to 0. \qquad \square$$

7.2.1 Torsion-freeness

The question as to when the symmetric algebra of a module is torsion-free is central and has been frequently considered in the literature (see, *e. g.*, [159] and the references thereof).

Let A denote a Noetherian ring and let B denote an A-algebra of finite type. Recall that the *A-torsion submodule* $\tau_A(M)$ of an A-module M is the kernel of the natural module homomorphism $M \to \mathfrak{S}_A^{-1}M$, where $\mathfrak{S}_A$ is the multiplicative set of the nonzero divisors of A. As usual, one says that M is torsion-free if $\tau_A(M) = \{0\}$.

By definition, the A-torsion of the A-algebra B is its the A-torsion submodule of its underlying A-module structure. But since the map $B \to \mathfrak{S}^{-1}B$ is now a ring homomorphism as well, the torsion in this case is actually an ideal of B. If, moreover, as is assumed, A is Noetherian ring and B is of finite type over A then $\tau_A(B)$ is annihilated by a single nonzero element, hence is contained in some associated prime of B. In general, it may or may not coincide with such an associated prime.

In any case, saying that $\tau_A(B) = \{0\}$ is tantamount to having any associated prime of B contract to a prime contained in (not necessarily equal to, in general) some associated prime of A. Of course, the contraction will be in fact a minimal prime of A if A has no embedded primes.

There is a general elementary principle to go from torsion-freeness to reducedness. Since one has proved even easier things, this one will be dealt with afresh.

Lemma 7.2.4. *If B_p is reduced for every $p \in \operatorname{Ass} A$, then $B/\tau_A(B)$ is reduced; in particular, in this case there is a natural surjection $B_{\mathrm{red}} \twoheadrightarrow B/\tau_A(B)$ factoring the canonical surjection $B \twoheadrightarrow B/\tau_A(B)$.*

Proof. Since $\tau_A(B) = \{0\}$, it suffices to see that $\mathfrak{S}_A^{-1}B$ is reduced. Clearly, one has $B_p = (A \setminus p)^{-1}B = (\mathfrak{S}_A^{-1}B)_{\mathfrak{S}_A^{-1}p}$ by well-known properties. If $b/1 \in \mathfrak{S}_A^{-1}B$ is nilpotent then, by hypothesis, for each $p \in \operatorname{Ass} A$ there is some $s_p \in A \setminus p$ annihilating b. Consider the annihilator $0 :_A b$ of b in A. Then one has shown that $0 :_A b \not\subset \bigcup_{p \in \operatorname{Ass} A} p$. As is well known, there is then an element $s \in 0 :_A b$ not belonging to any of these primes, *i. e.*, $s \in \mathfrak{S}_A$. Therefore, $b/1 = 0$ in $\mathfrak{S}_A^{-1}B$, as required. $\square$

Corollary 7.2.5. *If B is torsion-free over A, and if B_p is reduced for every $p \in \operatorname{Ass} A$, then B is reduced.*

For the sake of the next corollary, will say that $\operatorname{Spec} C$ of a Noetherian ring C is *irreducible* if C has a unique minimal prime.

Corollary 7.2.6. *If B_p is reduced for every $p \in \operatorname{Ass} A$ and $\operatorname{Spec} B$ is irreducible, then $B_{\mathrm{red}} \simeq B/\tau_A(B)$.*

Proof. This is clear by Lemma 7.2.4 and by the hypothesis as then $\tau_A(B)$ and the nilradical of B must coincide with the unique minimal prime of B. □

Lemma 7.2.7. *Suppose that B is reduced. If B is not torsion-free over A then there is a prime $p \in \operatorname{Spec} A$ such that, setting $A' = A_p$, $\mathfrak{m} = pA_p$, $K = A'/\mathfrak{m}$, $B' = B_p = B \otimes_A A'$, one has:*

(i) $\tau_{A'}(B') \cap \mathfrak{m}B' = \{0\}$

(ii) *If, moreover, B' is standard graded over A' and $B' \otimes_{A'} K$ is a polynomial ring over K then*

$$\dim_K(\tau_{A'}(B')_t) \geq \binom{t-r+n-1}{n-1}$$

for every $t \geq r$, where r is the initial degree of $\tau_{A'}(B')$ and $n = \mu(B'_+)$.

Proof. By Lemma 7.2.4, $B/\tau_A(B)$ is reduced. On the other hand, as has been seen quite generally, $\tau_A(B)$ is contained in some associated, hence minimal, prime of B. Therefore, $\tau_A(B)$ is a finite intersection of primes one of which is a minimal prime of B.

Now, suppose that $\tau_A(B) \neq 0$. Then there exists an associated (hence, minimal) prime of B contracting to a nonminimal prime of A. One may further take such a nonminimal prime—call it p—to be minimal possible among all nonminimal primes of A that are contracted from some minimal prime of B. By localizing at p, does not change either the hypotheses or the conclusion of the statement, so renaming $A_p, pA_p, A_p/pA_p, B_p$ to $A, \mathfrak{m}, K, B$, respectively, one now has that $\mathfrak{m}$ is the contraction of minimal prime of B. Moreover, no nonminimal prime of A properly contained in $\mathfrak{m}$ is contracted from a minimal prime of B. Therefore, every minimal prime of B not containing $\mathfrak{m}$ must contract to a minimal prime of A, hence contains the torsion $\tau_A(B)$. Since one is assuming that B is reduced, it follows that

$$\tau_A(B) \cap \mathfrak{m}B = \{0\}. \tag{7.2.7.1}$$

This proves (i).

To prove (ii), note that the (7.2.7.1) means that $\tau_A(B)$ is mapped isomorphically onto its natural image in $B/\mathfrak{m}B$. Since the latter is assumed to be a polynomial ring over K in $n = \mu(B_+)$ variables and $\tau_A(B)$ is up to this identification a homogeneous ideal, picking a form in $\tau_A(B)$ of degree equal to the initial degree r of $\tau_A(B)$ clearly implies that

$$\dim_K(\tau_A(B)_t) \geq \binom{t-r+n-1}{n-1}$$

for every $t \geq r$, as required. □

Next, a nontrivial converse to Corollary 7.2.5 in the realm of symmetric algebras. Curiously, it will say that if a module, whose symmetric algebra is reduced, has "few" linear syzygies then its symmetric algebra is torsion-free. Thus, morally, it seems to go in the wrong direction of the usual expectation about "enough" linear syzygies implying good properties.

Theorem 7.2.8. *Let A be a reduced Noetherian ring and let M be a finitely generated A-module such that:*
(i) *M is generically free*
(ii) *For every nonminimal prime $\wp \in \operatorname{Spec} A$,*

$$\mu(Z_\wp/Z_\wp \cap \wp_\wp^2 A_\wp^{\mu(M_\wp)}) \leq \operatorname{edim} A_\wp - 1, \tag{7.2.8.1}$$

where $0 \to Z_\wp \to A_\wp^{\mu(M_\wp)} \to M_\wp \to 0$ is a minimal presentation of M at $\wp$.

Then $\mathcal{S}_A(M)$ is reduced (if and) only if it is A-torsion-free.

Proof. The "if" statement follows from Corollary 7.2.5, using assumption (i).

Conversely, suppose that $\tau_A(\mathcal{S}_A(M)) \neq \{0\}$. Localization at a nonminimal prime of A does not affect either the assumptions or the conclusion of the theorem. Thus, by Lemma 7.2.7, one can assume that $(A, \mathfrak{m}, K)$ is local, $\mathfrak{m}$ is the contraction of minimal prime of $\mathcal{S}_A(M)$ and the following hold:

$$\tau_A(\mathcal{S}_A(M)) \cap \mathfrak{m}\mathcal{S}_A(M) = \{0\}, \quad \dim_K(\tau_A(\mathcal{S}_A(M))_t) \geq \binom{t-r+n-1}{n-1},$$

where $n = \mu(M)$ and r is the initial degree of $\tau_A(\mathcal{S}_A(M))$.

So far for generalities. One now digs further into assumption (ii). Consider a minimal presentation of M:

$$0 \to Z \to A^n \to M \to 0.$$

Setting $\ell := \mu(Z/Z \cap \mathfrak{m}^2 A^n)$ and $\overline{A} := A/\mathfrak{m}^2$, $\overline{\mathfrak{m}} := \mathfrak{m}/\mathfrak{m}^2$, one obtains a minimal free presentation over $\overline{A}$:

$$\overline{A}^\ell \to \overline{A}^n \to M \otimes_A \overline{A} \to 0.$$

Applying the symmetric tth functor yields an exact sequence for every $t \geq 1$,

$$\overline{A}^\ell \otimes_{\overline{A}} S_{t-1}(\overline{A}^n) \longrightarrow S_t(\overline{A}^n) \longrightarrow (\mathcal{S}_A(M))_t \otimes_A \overline{A} \longrightarrow 0.$$

Now, a second look at the equality (7.2.7.1) tells us that, for every $t \geq 0$, the graded piece $\tau_A(\mathcal{S}_A(M))_t$ of $\tau_A(\mathcal{S}_A(M))$ is a K-vector space direct summand of $(\mathcal{S}_A(M))_t$. Set $h(t) := \dim_K(\tau_A(\mathcal{S}_A(M))_t)$. Then $(\mathcal{S}_A(M))_t \otimes_A \overline{A}$ too admits $K^{\oplus h(t)}$ as a direct summand.

Therefore, $\overline{\mathfrak{m}}^{\oplus h(t)}$ is a direct summand of the image of $\overline{A}^{\ell} \otimes_{\overline{A}} S_{t-1}(\overline{A}^n)$ in $S_t(\overline{A}^n)$, which implies that

$$\ell \cdot \begin{pmatrix} t-1+n-1 \\ n-1 \end{pmatrix} \geq \mu(\overline{\mathfrak{m}})h(t) \geq \mu(\overline{\mathfrak{m}}) \cdot \begin{pmatrix} t-r+n-1 \\ n-1 \end{pmatrix},$$

for every $t \geq r$, hence $\ell \geq \mu(\overline{\mathfrak{m}})$. But, since $\operatorname{edim} A = \mu(\mathfrak{m}) = \mu(\overline{\mathfrak{m}})$, this inequality contradicts the assumption $\ell \leq \operatorname{edim} A - 1$. □

Corollary 7.2.9. *Let $A = k[X_1, \ldots, X_d]$ be a standard graded polynomial ring over a field k and let M be a graded A-module with free graded minimal presentation*

$$A(-(\delta+1))^{\ell} \oplus \sum_{s \geq 2} A(-(\delta+s)) \to A(-\delta)^n \to M \to 0.$$

If $\ell \leq d-1$ and M is locally free on the punctured homogeneous spectrum of A, then $\mathcal{S}_A(M)$ is reduced (if and) only if it is A-torsion-free.

Example 7.2.10. The following example shows that the estimate $\ell \leq d-1$ is best possible in general in Corollary 7.2.9. Let $d = 4$ above and consider the tail of the Koszul complex on X_1, X_2, X_3, X_4:

$$0 \to A \to A^4 = \bigwedge^3 A^4 \xrightarrow{\kappa_3} A^6 = \bigwedge^2 A^4.$$

Let φ denote a 5×4 matrix obtained by omitting a row of κ_3 after sufficiently many general elementary row transformations. Then $M := \operatorname{coker}(\varphi)$ has rank 2 and locally free on the punctured homogeneous spectrum of A, such that $\ell = 4 = \dim A$. A calculation with the help of a computer program shows that $\tau_A(\mathcal{S}_A(M)) \cap (\mathbf{X})\mathcal{S}_A(M) = \{0\}$, hence $\mathcal{S}_A(M)$ is reduced but not a domain. Actually, another calculation shows that the Rees algebra $\mathcal{R}_A(M) = \mathcal{S}_A(M)/\tau_A(\mathcal{S}_A(M))$ is a Gorenstein ring (Pfaffians) while $\mathcal{S}_A(M)$ is not even Cohen–Macaulay.

7.2.2 Ideals of linear type, I

Let R denote a ring and let $I \subset R$ be an ideal.

A remarkable algebra on these data is the R-subalgebra of the polynomial algebra $R[t]$ (t an indeterminate) generated by the elements ft, for all $f \in I$. It is denoted by $R[It]$ and called the *Rees algebra* of I in R. It can be expressed as an internal direct summand of R-submodules or an external direct summand of ideals,

$$R[It] = \bigoplus_{i \geq 0} I^i t \simeq \bigoplus_{i \geq 0} I^i,$$

whichever is more convenient on a situation.

This algebra will be studied in more detail in later sections. For the moment, one is interested in the canonical surjective R-algebra homomorphism

$$S_R(I) \overset{\alpha}{\twoheadrightarrow} R[It] \tag{7.2.10.1}$$

that maps a symmetric power product to the corresponding ordinary power product.

This R-homomorphism induces a surjective homomorphism of R/I-algebras

$$S_{R/I}(I/I^2) \simeq S_R(I)/IS_R(I) \overset{\alpha}{\twoheadrightarrow} R[It]/IR[It] = \mathrm{gr}_I(R). \tag{7.2.10.2}$$

Definition 7.2.11. An ideal I of a ring R is said to be of *linear type* if the map (7.2.10.1) is injective.

This terminology was suggested by R. Robbiano and G. Valla. The basic model of an ideal of linear type is given by an ideal generated by a regular sequence.

Proposition 7.2.12. *Let I be generated by an R-sequence $\{a_1, \ldots, a_n\}$. Then the map* (7.2.10.1) *is an isomorphism.*

Proof. Perhaps the easiest proof is by using the fact that both algebras are $\mathbb{N}$-graded with R sitting in degree zero and I in degree one. For any such graded R-algebra A, one denotes by A_+ its R-submodule generated in positive degree. Also note that α above preserves degrees.

One inducts on n.

For $n = 1$, both algebras are isomorphic to a polynomial ring in one variable over R. Assuming $n \geq 2$, set $a := a_1$ and consider the ideal $\bar{I} := I/(a) \subset \overline{R} := R/(a)$ generated by the images of $a_2, \ldots, a_n$, which are a regular sequence in $\overline{R}$. By the inductive hypothesis, the residual map $\overline{\alpha} : S_{\overline{R}}(\bar{I}) \overset{\alpha}{\longrightarrow} \overline{R}[\bar{I}t]$ is injective. Now, by the universal property of the symmetric algebra, one has a natural isomorphism $S_{\overline{R}}(\bar{I})_d \simeq S_R(I)_d/aS_R(I)_{d-1}$, the subscripts denoting degrees, where $d \geq 1$. Therefore, $S_{\overline{R}}(\bar{I})_+ \simeq S_R(I)_+/aS_R(I)$.

On the other hand, the restriction of $\overline{\alpha}$ to $S_{\overline{R}}(\bar{I})_+$ is an isomorphism onto $\overline{R}[\bar{I}t]_+$. By the naturality of the maps, this forces a similar equality isomorphism $\overline{R}[\bar{I}t]_+ \simeq R[It]_+/aR[It]$.

Summing up, one can encapsulate the information so far in the following commutative diagram of R-algebra homomorphisms:

$$\begin{array}{ccccccccc} 0 & \to & aS_R(I) & \to & S_R(I)_+ & \overset{\pi_s}{\longrightarrow} & S_{\overline{R}}(\bar{I})_+ & \to & 0 \\ & & \downarrow & & \downarrow \alpha & & \| \overline{\alpha} & & \\ 0 & \to & aR[It] & \to & R[It]_+ & \overset{\pi_r}{\longrightarrow} & \overline{R}[\bar{I}t]_+ & \to & 0 \end{array} \tag{7.2.12.1}$$

Suppose $\alpha(w) = 0$, with $w \in S_R(I)_+$ of smallest possible degree d. Then $\pi_s(w) = 0$ because $\overline{\alpha}$ is injective. Therefore, $w = av$, for some homogeneous $v \in S_R(I)$ of degree $d - 1$. It follows that $a\alpha(v) = \alpha(w) = 0$. But, since a is regular in R it is also regular in $R[It] \subset R[t]$, and hence $\alpha(v) = 0$—a contradiction v since has smaller degree than w. □

Remark 7.2.13. Other sequences have been studied that have a recurrent definition similar to regular sequence (see [70] for a collection of some of these). However, for those one may need a more sophisticated tool, often of homological content. One important example is that of a d-sequence (see Section 7.3.4.2).

The following is a basic property of an ideal of linear type.

Proposition 7.2.14. *If I is an ideal of linear type, then $\mu(I_P) \leq \operatorname{ht} P$ for every prime ideal $P \subset R$ containing I.*

Proof. Since both algebras commute with localization one can assume that $R, \mathfrak{m}$ is local and that $I \subset \mathfrak{m}$. But then

$$\mu_R(I) = \mu_{R/\mathfrak{m}}(I/\mathfrak{m}I) = \dim\big(S_R(I)/\mathfrak{m}S_R(I)\big) \leq \dim\big(S_R(I)/IS_R(I)\big) = \dim \operatorname{gr}_I(R),$$

the latter equality since I is of linear type. But, in the local case $\dim \operatorname{gr}_I(R) = \dim R$ (Theorem 7.3.6, Section 7.3). □

Ideals satisfying the upshot of the proposition play quite some independent role in the theory. Recall from Section 3.3 that they are said to satisfy property (F_1). They will come up in the subsequent part.

7.2.3 Dimension

The following proposition is an easy consequence of the general dimension formula of Huneke–Rossi (see Theorem 7.2.20 below). Next is a different proof of this formula.

Proposition 7.2.15. *If* $\operatorname{grade} I \geq 1$, *then* $\dim S(I) = \max\{\dim R + 1, \dim S(I/I^2)\}$.

Proof. Consider the canonical map (7.2.10.1): for every $P \in \operatorname{Spec} R$ such that $I \not\subset P$, the induced localization $\alpha_P : S(I)_P \to R_P[I_P t]$ is clearly an isomorphism since $I_P = R_P$. This shows that $I^t \ker \alpha = (0)$ for $t \gg 0$, hence every prime ideal of the ring $S(I)$ contains either $IS(I)$ or $\ker \alpha$. Therefore,

$$\begin{aligned}\dim S(I) &= \max\{\dim R[It], \dim S_{R/I}(I/I^2)\}\\ &= \max\{\dim R + 1, \dim S_{R/I}(I/I^2)\},\end{aligned}$$

since $\dim R[It] = \dim R + 1$ for ideals containing regular elements. □

Corollary 7.2.16. *Let $R, \mathbf{m}$ be a local ring. If $I \subset R$ is an $\mathbf{m}$-primary ideal, then* $\dim S(I) = \max\{\dim R + 1, \mu(I)\}$.

Proof. Since $\operatorname{supp} S(I/I^2) = \operatorname{supp} S(I/\mathbf{m}I)$, the result follows from Proposition 7.2.15. □

Ideals satisfying the formula of Corollary 7.2.16 were originally considered by G. Valla. However, they cover but a certain number of situations.

Example 7.2.17. Let $R = k[X, Y, Z]_{(X,Y,Z)}$, $\mathbf{n} = (X, Y, Z)_{(X,Y,Z)}$ and let $J \subset R$ be $\mathbf{n}$-primary with 5 generators. Let t be an indeterminate over R, let $T = R[t]_{(\mathbf{n},t)}$, $\mathbf{m} = (\mathbf{n}, t)R$ and let $I = JR$. Then $\dim S_T(I) = \dim S_R(J) + 1$, thus showing that the ideal I does not satisfy Valla's formula.

Determinantal ideals also fail to comply with this formula, except for special row and column sizes [82]. For a family of ideals that do satisfy this value, see Exercise 7.6.3.

Ideals of linear type, or rather their residual property (F_1), are important also because of the next nearly obvious result.

Proposition 7.2.18. *Let A be a Noetherian ring and let $I \subset A$ be an ideal satisfying property (F_1). Then*

$$\dim A \geq \sup_{P \supseteq I}\{\dim A/P + \mu(I_P)\}.$$

Proof. Since $\dim A \geq \dim A/P + \mathrm{ht}(P)$ for any prime ideal, the assertion is an immediate consequence of property (F_1). □

One may ask what additional conditions are sufficient for having the equality above. It clearly suffices to find a prime ideal $P \supset I$ such that $\dim A \leq \dim A/P + \mu(I_P)$. Surprisingly, a sufficient condition is a rather typical requirement, namely, that I admits a minimal prime ideal P such that a maximal chain of primes contains P as an element of the chain. For in this case, $\dim A = \dim A/P + \mathrm{ht}\, P = \dim A/P + \mathrm{ht}(I_P) \leq \mu(I_P)$.

The condition $\dim A = \dim A/P + \mathrm{ht}\, P$ is satisfied for an arbitrary prime ideal P in the so-called catenary rings, examples of which are domains of finite type over fields and Cohen–Macaulay rings.

It turns out that a refined version makes the inequality of Proposition 7.2.18 an equality quite generally. Namely, we have the following.

Proposition 7.2.19 (Herrmann–Moonen–Villamayor). *Let A denote a Noetherian ring of finite dimension and let $I \subset A$ be an ideal contained in the Jacobson radical of A. Then*

$$\dim A = \sup_{P \supseteq I}\{\dim A/P + \ell(I_P)\},$$

where $\ell(I_P)$ denotes the local analytic spread of I at P.

Proof. By Proposition 7.3.16, $\ell(I_P) \leq \mathrm{ht}\, P_P = \mathrm{height}\, P$, hence the inequality

$$\dim A \geq \sup_{P \supseteq I}\{\dim A/P + \ell(I_P)\}$$

is trivial.

For the reverse inequality, let $Q \subset \mathrm{gr}_I(A)$ be a prime ideal such that $\dim \mathrm{gr}_I(A)/Q = \dim \mathrm{gr}_I(A)$ and set $P := Q \cap A$. Since I is contained in the Jacobson radical of A, then $\dim \mathrm{gr}_I(A) = \dim A$ (Theorem 7.3.6 and the Remark after it). Now apply Corollary 2.5.38:

$$\dim A = \dim \mathrm{gr}_I(A)/Q \leq \dim A/P + \mathrm{gr}_{I_P}(A_P)/P_P\mathrm{gr}_{I_P}(A_P) = \dim A/P + \ell(I_P),$$

since $\ell(I_P) = \dim A_P[I_P t]/P_P A_P[I_P t] \simeq \mathrm{gr}_{I_P}(A_P)/P_P \mathrm{gr}_{I_P}(A_P)$. □

The above makes up for another proof of the Huneke–Rossi formula. The latter is as follows.

Theorem 7.2.20 (Dimension of the symmetric algebra [82]). *Let R be a Noetherian ring and let M be a finitely generated R-module. Then*

$$\dim S_R(M) = \sup_{P \in \operatorname{Spec} R}\{\dim R/P + \mu(M_P)\}.$$

Proof. One will apply Proposition 7.2.19 with $A = S_R(M)$. Since $S_R(M)$ is graded with R as its zero part, its dimension will not change by passing to the ring of fractions $S(M)_{1+S(M)_+}$. The extended ideal $I := (S(M)_+)S(M)_{1+S(M)_+}$ is clearly contained in the (graded) Jacobson radical of $S(M)_{1+S(M)_+}$, any prime Q containing I being of the form (P, I), where $P \in \operatorname{Spec} R$.

Claim. $S(M)_+$ is an ideal of linear type.

This result is originally due to P. Salmon ([131]) but has been revisited a few times later ([153], [70, Example 2.3]). Perhaps the quickest proof is as follows: by definition of a symmetric power of M as a residue of the respective tensor power, the canonical R-module surjections

$$\begin{array}{ccc} M \otimes M^{\otimes t} = M^{\otimes(t+1)} & \longrightarrow & S^{t+1}(M) \\ \downarrow & & \\ M \otimes S^t(M) & & \end{array}$$

induce a surjection $M \otimes S^t(M) \twoheadrightarrow S^{t+1}(M)$, hence an R-module surjection $M \otimes S(M) \twoheadrightarrow S(M)_+$. Taking the tth symmetric power of this map and using the ring base change $R \longrightarrow S(M)$ gives a surjection

$$S^t(M) \otimes S(M) \simeq S^t\big(M \otimes S(M)\big) \twoheadrightarrow S^t\big(S(M)_+\big)$$

which composed with the natural surjection $(S(M)_+)^t \twoheadrightarrow S^t(M) \otimes S(M)$ gives a surjection $(S(M)_+)^t \twoheadrightarrow S^t(S(M)_+)$, which must be an inverse to the natural surjection $S^t(S(M)_+) \twoheadrightarrow (S(M)_+)^t$.

This proves the claim.

Clearly, then I is an ideal of linear type as well. Therefore, I satisfies the property (F_1) and I has maximal analytic spread locally everywhere. On the other hand, for any $P \in \operatorname{Spec} R$ and $Q := (P, I)$, one has

$$I_Q = \big(S_{R_P}(M_P)_+\big)_{(P_P, S_{R_P}(M_P)_+)},$$

since taking symmetric powers commutes with localization. It follows that $\mu(I_Q) = \mu(M_P)$ as $S_{R_P}(M_P)_+$ is generated by M_P and locally at $(P_P, S_{R_P}(M_P)_+)$ the local number of generators does not decrease. Therefore, $\mu(M_P) = \ell(I_Q)$. □

7.2.3.1 Further dimension obstructions

It has been seen that, quite generally, over a reasonable ring R, one has the following formula (Theorem 3.3.12):

$$\dim \mathcal{S}(M) = \dim R + \operatorname{rank} M + \operatorname{fd}(M),$$

for a finitely generated R-module having rank. Here, $\operatorname{fd}(M)$ is the dimension defect of the symmetric algebras. This is a rather difficult invariant to move around, so one bends over to the close condition (F_0). One recalls (see Section 3.3) that for a finitely generated R-module M having a rank, the condition means, equivalently:

- $\mu(M_P) \leq \dim R + \operatorname{rank} M$ for every prime ideal P;
- For some (any) free presentation $G \xrightarrow{\varphi} F \to M \to 0$, one has $\operatorname{ht} I_t(\varphi) \geq \operatorname{rank} \varphi - t + 1$, for $1 \leq t \leq \operatorname{rank} \varphi$.

For of an ideal $I \subset R$, even without rank, the first condition makes sense in the expected form $\mu(I_P) \leq \dim R + 1$. Thus, when one talks about the (F_0) condition for an ideal one always means this one.

For arbitrary Noetherian rings and ideals, one has the following consequence of the Huneke–Rossi dimension formula.

Corollary 7.2.21. *Let R be a Noetherian ring and $I \subset R$ an ideal not contained in at least one minimal prime of R of maximal dimension. Then:*

(a) $\dim S_R(I) \geq \dim R + 1$.

(b) *If R is moreover Cohen–Macaulay, then* $\dim S_R(I) = \dim R + 1$ *if and only if the condition (F_0) holds for I.*

Proof. (a) Let $P \in \operatorname{Spec} R$ denote a minimal prime of R of maximal dimension not containing I. Then $\dim R/P = \dim R$, while $I_P = R_P$, and hence $\mu(I_P) = 1$. Now use Huneke–Rossi dimension formula in Theorem 7.2.20.

(b) Suppose F_0 holds, *i. e.*, $\mu_P \leq \operatorname{ht} P + 1$ for any prime ideal $P \subset R$. Clearly, then $\dim R/P + \mu(I_P) \leq \dim R - \operatorname{ht} I + \operatorname{ht} I + 1 = \dim R + 1$ (no need for the Cohen–Macaulay hypothesis in this direction). Therefore, Theorem 7.2.20 takes over.

The converse is similar by noting that $\operatorname{ht} P = \dim R - \dim R/P$ for any prime ideal P because R is Cohen–Macaulay. □

Likewise, one has the following.

Corollary 7.2.22. *Let R be a Cohen–Macaulay Noetherian ring and let $I \subset R$ be an ideal of height ≥ 1. Let $R^m \xrightarrow{\varphi} R^n \to I \to 0$ be a free presentation of I and set $S_R(I) \simeq R[\mathbf{T}]/\mathcal{J}$, with $\mathbf{T} = \{T_1, \ldots, T_n\}$ and $\mathcal{J} = I_1(\mathbf{T} \cdot \varphi)$ the corresponding presentation of the symmetric algebra. Then*

(a) $\operatorname{ht} \mathcal{J} \leq \operatorname{rank} \varphi$.

(b) $\operatorname{ht} \mathcal{J} = \operatorname{rank} \varphi$ *if and only if* $\dim S_R(I) = \dim R + 1$.

Proof. Since R is Cohen–Macaulay, $\dim S_R(I) = \dim R + n - \operatorname{ht} \mathcal{J}$. On the other hand, I has a rank because $\operatorname{ht} I \geq 1$, hence so does the matrix φ, giving $\operatorname{rank} \varphi = n - 1$. Thus, the result follows from this and the dimension inequality of Corollary 7.2.21. □

Remark 7.2.23. (1) The dimension inequality in Corollary 7.2.21 also follows from Proposition 7.3.3 in the next section, by using (7.2.10.1). For the equality it suffices, as usual, to assume that R is catenary or alike.

(2) One notes that a similar result as in Corollary 7.2.22 holds true for a finitely generated R-module having a rank.

Proposition 7.2.24. *Notation as in* Corollary 7.2.22. *Suppose, moreover, that R is a domain. If $\mathcal{J}$ is height-unmixed then* $\dim S_R(I) = \dim R + 1$*; in particular, this is the case when $S_R(I)$ is Cohen–Macaulay.*

Proof. By Corollary 7.2.22, it suffices to prove that $\operatorname{ht} \mathcal{J} \geq \operatorname{rank} \varphi$, but actually the full equality will be argued. For this localize at the multiplicatively closed set $\mathfrak{S} := R \setminus \{0\}$ to reduce to the case where the ring of coefficients is the field $K = \mathfrak{S}^{-1}R$. In this scenery, the image of $\mathcal{J}$ is generated by linear forms in $K[\mathbf{T}]$, hence its height coincides with its K-vector dimension, which is the rank of the extended matrix $\mathfrak{S}^{-1}\varphi$ of φ over K. On the other hand, if $P \subset R[\mathbf{T}]$ is an associated prime of $\mathcal{J}$ then $\operatorname{ht} P = \operatorname{ht} \mathcal{J}$ by assumption. But $\mathfrak{S}^{-1}P$ is an associated prime of $\mathfrak{S}^{-1}\mathcal{J}$ (actually equals this ideal as the latter is prime) Therefore, one has

$$\operatorname{rank} \varphi = \operatorname{rank} \mathfrak{S}^{-1}\varphi = \operatorname{ht} \mathfrak{S}^{-1}\mathcal{J} = \operatorname{ht} \mathfrak{S}^{-1}P = \operatorname{ht} P = \operatorname{ht} \mathcal{J},$$

as was to be shown. □

Corollary 7.2.25 (Valla [152, Theorema 3.6]). *Let R be a Cohen–Macaulay ring and let $I \subset R$ be an ideal generated by an R-sequence of length $r \geq 2$. Then the symmetric algebra of a power I^n is Cohen–Macaulay if and only if either $n = 1$ or else $r = n = 2$.*

Proof. First, assume the numerical values as stated. For $n = 1$, the syzygies of ideal $I^1 = I$ are the Koszul relations of the given regular sequence $\{a_1, \ldots, a_r\}$, hence the defining ideal of $\mathcal{S}(I)$ is the 2×2 minors of the matrix

$$\begin{bmatrix} T_1 & T_2 & \ldots & T_r \\ a_1 & a_2 & \ldots & a_r \end{bmatrix},$$

where the T's are the presentation variables. By Proposition 7.2.12, the ideal I is of linear type, hence the height of the ideal of minors is $\dim R[\mathbf{T}] - (\dim R + 1) = r - 1$. By the Eagon–Northcott theorem (6.4.4), this ideal is Cohen–Macaulay.

Now, assume that $r = n = 2$. An immediate calculation tells that the syzygies of $I^2 = (a_1^2, a_1a_2, a_2^2)$ are generated by the two reduced Koszul syzygies $(a_2, -a_1, 0)^t$ and $(0, a_2, -a_1)^t$. Therefore, the defining ideal is itself generated by a regular sequence of two forms.

For the converse, by Proposition 7.2.24 the dimension of $\mathcal{S}(I^n)$ is $\dim R + 1$. Since $\mathcal{S}(I^n)$ is unmixed by assumption, Proposition 7.2.15 implies that $\dim \mathcal{S}_{R/I}(I^n/I^{n+1}) \leq \dim R + 1$. But since I is generated by an R-sequence the R/I-module I^n/I^{n+1} is free of rank $\mu(I^n) = \binom{n+r-1}{r-1}$. It follows that $\binom{n+r-1}{r-1} \leq r+1$. An easy verification leads to $n = 1$ or else $n = r = 2$. □

Another application where the dimension defect vanishes is the following.

Proposition 7.2.26. *Let R be a Cohen–Macaulay Noetherian ring and let $\mathcal{A}$ denote an $r \times r$ matrix with entries in R having a rank. Suppose that the height inequalities prescribed by the condition (F_0) are satisfied by the minors of $\mathcal{A}$. If $\mathbf{X} := \{X_1, \ldots, X_r\}$ is a set of indeterminates over R, then the elements of the product $\mathbf{X}\mathcal{A}$ form a regular sequence in $R[\mathbf{X}]$.*

Proof. Recall that (F_0) implies in particular that $\operatorname{rank} \mathcal{A} = r$. Let M denote the cokernel of the free map $R^r \to R^r$ given by $\mathcal{A}$. Then $\mathcal{S}_R(M) \simeq R[\mathbf{X}]/I_1(\mathbf{X}\mathcal{A})$. But (F_0) says that the dimension defect vanishes, which implies that $\dim \mathcal{S}_R(M) = \dim R + \operatorname{rank} M = \dim R$ (alternatively, one can use Remark 7.2.23, (2)). On the other hand, since R is Cohen–Macaulay, $\operatorname{ht} I_1(\mathbf{X}\mathcal{A}) = \dim R[\mathbf{X}] - \dim \mathcal{S}_R(M)$. Therefore, $\operatorname{ht} I_1(\mathbf{X}\mathcal{A}) = r$, hence the generators form a regular sequence (of length r). □

Remark 7.2.27. The last proposition greatly generalizes [100, Proposition 4.3], an important step in the configuration of the main results on ideals of minors of symmetric matrices (see Theorem 6.4.7). The reason it can be applied to *loc. cit.* is that the generic symmetric matrix satisfies (F_0). However, to avoid being trapped in circularity, an independent proof of this fact has to be given that does not follow from the bounds obtained by Kutz.

The following template gives a modicum to attack further this sort of problem.

Proposition 7.2.28. *Let R denote a Cohen–Macaulay Noetherian domain and let $I \subset R$ be a nonzero ideal. The following are equivalent conditions:*
(i) *I satisfies the condition (F_1) and $S_R(I)$ is height-unmixed.*
(ii) *I is of linear type.*

(ii) ⇒ (i) One piece has already been mentioned, while the second comes from the fact that R is a domain and $S_R(I) = R[It] \subset R[t]$.

(i) ⇒ (ii) The goal is to show that for any associated prime ideal $P \subset R[\mathbf{T}]$ of $S_R(I)$, one has $P \cap R = \{0\}$. This will be carried out by induction on $\dim R$.

Since $S_R(I)$ is height-unmixed, by Proposition 7.2.24 and the notation there, one has $\operatorname{rank} \varphi = \operatorname{ht} \mathcal{J} = \operatorname{ht} P$. At the other end, the (F_1) conditions tells, in particular, that $\operatorname{ht} I_1(\varphi) \geq \operatorname{rank} \varphi - 1 + 2 = \operatorname{rank} \varphi + 1$. It follows that $\operatorname{ht} P \cap R \leq \operatorname{ht} P < \operatorname{ht} I_1(\varphi)$. Set $\wp = P \cap R$ and localize at $\wp$. Then $\dim R_\wp < \dim R$ and the assumptions are preserved likewise and, moreover, $\operatorname{ht}(\wp_\wp) < \operatorname{ht} I_1(\varphi_\wp)$. By the inductive assumption, $(\wp_\wp) = 0$, hence $\wp = 0$ as $R_\wp$ is a domain.

It remains to establish the case where $\dim R = 1$. But this follows as well by the inequality $\operatorname{ht} P \cap R \leq \operatorname{ht} P < \operatorname{ht} I_1(\varphi) \leq 1$.

As a consequence, $S_R(I)$ is now torsion-free over R. But since R is a domain, the canonical map (7.2.10.1) is an isomorphism as its kernel is annihilated by a power of the nonzero ideal I. □

For any ring R, one denotes by R^{red} its *reduced ring*, *i. e.*, its residue ring modulo the nil-radical. Without assuming that R is a domain, one gets the following version.

Proposition 7.2.29. *Let R denote a Cohen–Macaulay Noetherian ring and let $I \subset R$ be an ideal. Suppose that I is generically a complete intersection of height ≥ 1. If I satisfies condition (F_1) and $S_R(I)$ is height-unmixed, then $S_R(I)^{\mathrm{red}} \simeq R[It]^{\mathrm{red}}$.*

Proof. Since the hypothesis on I says that it has a rank, a suitable adaptation of Proposition 7.2.24 for the nondomain case, one has $\dim S_R(I) = \dim R + 1$. Alternatively, note that (F_1) in this setup implies (F_0).

Claim. $\dim S_{R/I}(S(I/I^2)) = \dim R$.

To see this first note that, since I is generically a complete intersection of $\operatorname{ht} I$ then I/I^2 has rank $\operatorname{ht} I$. As already noted, condition (F_0) holds. Let $R^m \xrightarrow{\varphi} R^n \to I \to 0$ be a free presentation of I. Then the induced free presentation of the (R/I)-module I/I^2 has a matrix of rank $n - \operatorname{ht} I = \operatorname{rank} \varphi + 1 - \operatorname{ht} I$. Let an upper bar denotes modulo I. Since R is Cohen–Macaulay, $\operatorname{ht} \bar{I}_t = \operatorname{ht} I_t - \operatorname{ht} I$, for $1 \leq t \leq \operatorname{rank} \overline{\varphi}$. Therefore, $\operatorname{ht} \bar{I}_t \geq \operatorname{rank} \varphi - t + 2 - \operatorname{ht} I = \operatorname{rank} \overline{\varphi} - t + 1$, for every $1 \leq t \leq \operatorname{rank} \overline{\varphi}$. Thus, I/I^2 satisfies (F_0), hence $\dim S_{R/I}(S(I/I^2)) = \dim R + \operatorname{rank} I/I^2 = \dim R - \operatorname{ht} I + \operatorname{ht} I = \dim R$, as asserted.

By Proposition 7.2.15 and unmixedness again, one gets a contradiction unless the minimal primes of $S_R(I)$ are the same as those of $R[It]$. Thus, one is through. □

7.3 Rees algebras

The literature on Rees algebras is unthinkably large. The purpose of this section is to give the beginner a solid grip on the main foundational results, aiming at those that are fairly encompassing. Since this is book is supposed to be used as a textbook, there is hardly place to give an account of more sophisticated results out of a recent crop.

7.3.1 Geometric roots

From the geometric side, it all starts with the map $\mathbb{A}^2 \setminus \{(0,0)\} \to \mathbb{P}^1$ that takes a point $(x,y) \neq (0,0)$ to the direction $(x : y)$ of the line through $(0,0)$ and (x,y). Clearly, $(x : y) = (xt : yt)$ for every $t \in k \setminus \{0\}$. Now the graph of this map is the set

$$\begin{aligned}&\{((x,y),(xt : yt)) \mid (x,y) \in \mathbb{A}^2 \setminus (0,0), t \in k \setminus \{0\}\}\\ &\quad = \{((x,y),(z : w)) \in (\mathbb{A}^2 \setminus (0,0)) \times \mathbb{P}^1 \mid (z : w) = (x : y)\}\end{aligned}$$

In the simplicity of these expressions one finds two basic ideas in algebraic geometry. The first form gives the graph as a generic locus (*i. e.*, as the locus of a generic point in the sense of the early Weil school), while the second form yields the graph as a locus of points satisfying a property (namely, the vanishing of the pertinent determinant $XW - YZ$).

Taking the full algebraic side of this, one lands on the two k-algebras $k[X, Y, Xt, Yt] = k[X, Y][Xt, Yt] \subset k[X, Y][t]$ and $k[X, Y, Z, W]/(XW - YZ)$ which are isomorphic (even as $R = k[X, Y]$-algebras) and are both isomorphic to the abstract R-algebra $\oplus_s I^s$, with $I = (X, Y)$ (the ideal of the point $(0, 0)$).

Note that the above rational map is induced by a polynomial map $\mathbb{A}^2 \to \mathbb{A}^2$ given by (X, Y). Picking up from there, one could more generally consider any polynomial map $(f_1, \dots, f_m) : \mathbb{A}^n \to \mathbb{A}^m$. It induces a regular map

$$\mathbb{A}^n \setminus V(f_1, \dots, f_m) \to \mathbb{A}^m \setminus \{0\},$$

hence also a regular map $\mathbb{A}^n \setminus V(f_1, \dots, f_m) \to \mathbb{P}^{m-1}$. The graph of the latter is similarly defined. However, its closure in general will only be contained in (not equal to) the locus

$$\begin{aligned} \{(\mathbf{x}, \mathbf{z}) &= \big((x_1, \dots, x_n), (z_1, \dots, z_m)\big) \in \mathbb{A}^n \times \mathbb{P}^{m-1} \mid \mathbf{z} = \big(f_1(\mathbf{x}), \dots, f_m(\mathbf{x})\big)\} \\ &= \left\{(\mathbf{x}, \mathbf{z}) \in \mathbb{A}^n \times \mathbb{P}^{m-1} \mid \det_{2\times 2} \begin{pmatrix} z_1 & \dots & z_m \\ f_1(\mathbf{x}) & \dots & f_m(\mathbf{x}) \end{pmatrix} = 0\right\} \qquad (7.3.0.1) \\ &= V\left(I_2 \begin{pmatrix} Z_1 & \dots & Z_m \\ f_1 & \dots & f_m \end{pmatrix}\right), \end{aligned}$$

where $I_d(\mathcal{M})$ stands for the ideal generated by the $d \times d$ minors of the matrix $\mathcal{M}$. The true graph is of course the closure of the set

$$\{((x_1, \dots, x_n), (f_1(\mathbf{x})t, \dots, f_m(\mathbf{x})t)) \mid \mathbf{x} \notin V(f_1, \dots, f_m), t \neq 0\} \qquad (7.3.0.2)$$

Again, the algebraic version of (7.3.0.1) and (7.3.0.2) yields a homomorphism of $R = k[\mathbf{X}]$-algebras

$$R[\mathbf{Z}]/I_2 \begin{pmatrix} Z_1 & \dots & Z_m \\ f_1 & \dots & f_m \end{pmatrix} \twoheadrightarrow R[f_1 t, \dots, f_m t] = R[It] \subset R[t],$$

where $I = (f_1, \dots, f_m) \subset R$. Let us emphasize for the sake of the records that this homomorphism is an isomorphism if $f_1, \dots, f_m$ is a regular sequence. Also, the whole procedure is extendable to the case of an affine map restricted to a subvariety.

Thus, more generally, for any ring R and any ideal $I \subset R$, it would seem quite natural to define the *blowup* of Spec R along Spec R/I as Proj$(R[It])$, where $R[It] \simeq \oplus_s I^s$ is naturally R-graded by the powers of I. The residue class ring $R[It]/IR[It] \simeq \oplus_s I^s/I^{s+1}$ is again R-graded—it is most of the times denoted by $\mathrm{gr}_I(R)$ and called the *associated*

graded ring of I. The geometric version $\operatorname{Proj}(\operatorname{gr}_I(R))$ is called the *exceptional locus* of the blowup.

Note the fundamental diagram of R-maps (as a very rough parody to Euler's famous equation $e^{2\pi i} = 1$ involving the main parts of mathematics):

$$\begin{array}{lccc} \text{(algebra)} & R & \longrightarrow & R[It] \quad \text{(analysis)} \\ & \downarrow & & \downarrow \\ \text{(geometry)} & R/I & \longrightarrow & \operatorname{gr}_I(R) \quad \text{(hard analysis...)} \end{array}$$

Dragging information from $\operatorname{gr}_I(R)$ up to $R[It]$ is a tall order of blowup theory—this facet will be explored in the subsequent parts.

7.3.2 Dimensions

Not many properties of the Rees algebra $R[It]$ are available without further restrictions. Throughout, one assumes that (at least) R is a Noetherian ring. Recall that $R[It]$ is standard $\mathbb{N}$-graded over $R = R[It]_0$. As such, the ideal $R[It]_+ := (It)R[It]$ generated by the elements of positive degree is often called *irrelevant* as a slight association with a mesmerizing concept of algebraic geometry.

A first easy formula comes out immediately from Theorem 2.5.39.

Proposition 7.3.1. *Let R denote a Noetherian domain and $I \subset R$ a nonzero ideal. Then* $\dim R[It] = \dim R + 1$ *and* $\operatorname{ht} R[It]_+ = 1$.

Proof. Take $S = R[It]$ in Theorem 2.5.39 and $P = R[It]_+$, taking in account that $\operatorname{trdeg}_R(R[It]) = \operatorname{trdeg}_K(K(t)) = 1$, where K denotes the field of fractions of R. □

As usual, in formulas like the above, both sides can be infinite.

In the case where R is not a domain, the result has to be slightly modified. As a case "sans gloire," if I is a nilpotent ideal then $R[It]$ is a finitely generated R-module, hence $\dim R[It] = \dim R$.

One needs the following basic result.

Lemma 7.3.2. *Let R denote a Noetherian ring and let $I \subset R$ be a proper ideal. Then the association $p \mapsto pR[t] \cap R[It]$ establishes a bijection between the minimal primes of R and the minimal prime ideals of $R[It]$.*

Proof. Clearly, for any $p \in \operatorname{Spec} R$, the ideal $pR[t]$ is a homogeneous prime ideal of $R[t]$, hence its contraction $pR[t] \cap R[It]$ is a homogeneous prime ideal of $R[It]$. Note that $(pR[t] \cap R[It]) \cap R = p$, hence the association is one-to-one. From this follows immediately that if $p \in \operatorname{Spec} R$ is such that $pR[t] \cap R[It]$ is a minimal prime of $R[It]$ then p is a minimal prime of R.

Claim 1. Every $\wp \in \operatorname{Min}(R[It])$ is of the form $pR[t] \cap R[It]$, for some $p \in \operatorname{Spec} R$.

– One may assume that I is not nilpotent.
  Indeed, if I is nilpotent then $I \subset p$ for every minimal prime p of R. Let p be any one of these. Since $\wp$ is homogeneous, then $\wp = (p, \wp_+)$. Say, $(\wp_+) = (b_1 t, \ldots, b_r t)$. Then $\wp$ is the kernel of the natural surjection $R[It] \twoheadrightarrow R/p[((b_1, \ldots, b_r), p)/pt]$. On the other hand, (p, It) is the kernel of $R[It] \twoheadrightarrow R/p[(I,p)pt] = R/p \subset R/p[((b_1, \ldots, b_r), p)/pt]$, since $I \subset p$. Therefore, $(p, It) \subset \wp$. But $(p, It) = pR[t] \cap R[It]$, hence $\wp = pR[t] \cap R[It]$ by minimality of $\wp$.
– $It \subset \wp$.
  Then, letting $p := \wp \cap R$, one must have $\wp = (p, It)$ since the latter is a prime ideal contained in $\wp$. But $pR[t] \cap R[It] = (p, pR[t] \cap R[It]_+) \subset (p, It)$, hence $\wp = pR[t] \cap R[It]$ by minimality of $\wp$.
– $It \not\subset \wp$.
  Let $\{a_1, \ldots, a_m\}$ stand for a set of generators of I. Say, $at \notin \wp$, with $a = a_m$ nonnilpotent. Localizing at the powers of at gives $\wp = \iota^{-1}(\iota(\wp)R[It]_{at})$, where $\iota : R[It] \to R[It]_{at}$ is the structural map. On the other hand, $R[It]_{at} = S[at, (at)^{-1}]$, where $S = R[a_1/a, \ldots, a_{m-1}/a] \subset R_a$, where by abuse one writes R for its image $R/(0 :_R a^\infty)$ under the structural map $R \to R_a$. Note that $S[at, (at)^{-1}]$ is a graded algebra over its degree zero part S. Since $P := \iota(\wp)R[It]_{at}$ is a prime ideal, it follows that P is a homogeneous ideal of the form (q, P_+), where $q \in \operatorname{Spec} S$. Let $p := q \cap R$ under the map $R \to S$, restriction of the structural map $R \to R_a$.

If $a \notin p$, then pR_a is a prime ideal, $pR_p = (pR_a)_{pR_a} \subset R_p[t]$ and $q = pR_p \cap S = pR_p[t] \cap S$. Clearly, then $\iota(pR[t] \cap R[It]) \subset \iota(\wp)R[It]_{at} = P$, hence $pR[t] \cap R[It] \subset \wp$ and one must have equality by the minimality of $\wp$.

Suppose that $a \in p$. Since $IS \subset aS$ (actually, $IS = aS$), then $I \subset IS \cap R \subset aS \cap R \subset pS \cap R \subset q \cap R = p$. In this case, the argument is ipsis litteris the one in the first item above.

To complete the proof, it suffices to show the following.

Claim 2. If $p \in \operatorname{Min}(R)$ then $pR[t] \cap R[It] \in \operatorname{Min}(R[It])$.

Let $\wp \subset pR[t] \cap R[It]$ be a minimal prime of $R[It]$. By the first claim, $\wp = p'R[t] \cap R[It]$, for some prime $q \in \operatorname{Spec} R$. Clearly, then $p' \subset p$, hence $p' = p$ by assumption and one is through. □

Proposition 7.3.3. *Let R denote a Noetherian ring and let $I \subset R$ stand for an ideal. Then* $\dim R[It] = \dim R + 1$ *if and only if I is not contained in at least one minimal prime of R of maximal dimension.*

Proof. For any $p \in \operatorname{Spec} R$, it can be seen that the kernel of the natural surjective homomorphism of Rees algebras

$$R[It] \twoheadrightarrow \frac{R}{p}\left[\frac{(I,p)}{p}t\right] \subset \frac{R}{p}[t]$$

is $pR[t] \cap R[It]$. By Lemma 7.3.2, one has

$$\dim R[It] = \max_p\{\dim R[It]/pR[t] \cap R[It]\} = \max_p\left\{\dim \frac{R}{p}\left[\frac{(I,p)}{p}t\right]\right\}, \qquad (7.3.3.1)$$

where p runs through the set of minimal primes of R.

Now, since R/p is a domain, by Proposition 7.3.1 one has $\dim \frac{R}{p}[\frac{(I,p)}{p}t] = \dim R/p+1$ provided $I \not\subset p$. By assumption, $I \not\subset p$ for some p such that $\dim R = \dim R/p$. Therefore, for such a prime the right-hand side above attains the maximum, hence $\dim R[It] = \dim R + 1$, showing one direction.

The converse is also obvious by the same argument. □

Remark 7.3.4. The degree zero part $S = R[a_1/a, \ldots, a_{m-1}/a]$ of the ring of fractions $R[It]_{at}$ (a not nilpotent) is often called a *monoidal ring transform* of R because it is the coordinate ring of the geometric monoidal transform introduced by Zariski in his work on resolution of singularities. It has only been used above in its scraps. Its seeming elementary form hides deep information about the singularities, at least as much as the blowing-up does. In fact, the defining equations are, in analogy to those of the Rees algebra, obtained by the I-saturation of monoidal Koszul relations of the form $aX_i - a_i, 1 \le i \le m-1$ in the above notation.

7.3.2.1 The extended Rees algebra

Next, one deals with the dimension of the associated graded ring $\mathrm{gr}_I(R)$.

For this, it will be handier to work with the *extended Rees algebra* $R[It, t^{-1}] \subset R[t, t^{-1}]$ instead. It has at the outset (at least) two advantages over its subalgebra $R[It]$: first, it carries the regular element t^{-1}; second, one has $R[It, t^{-1}]/(t^{-1}) \simeq \mathrm{gr}_I(R)$. To see this isomorphism, note that multiplying by t^{-1} shifts the degrees by one, yielding $t^{-1}R[It, t^{-1}] = \cdots \oplus Rt^{-1} \oplus I \oplus I^2t \oplus \cdots = \cdots \oplus Rt^{-1} \oplus IR[It]$, hence

$$R[It, t^{-1}]/t^{-1}R[It, t^{-1}] \simeq R[It]/IR[It] = \mathrm{gr}_I R.$$

The analogue of Proposition 7.3.3 comes with no restrictions.

Proposition 7.3.5. *Let R denote a Noetherian ring and $I \subset R$ any ideal. Then* $\dim R[It, t^{-1}] = \dim R + 1$.

Proof. As in the proof of Lemma 7.3.2, the association $p \mapsto pR[t, t^{-1}] \cap R[It, t^{-1}]$ is one-to-one between the prime ideals of R and certain prime ideals of the extended Rees algebra. By the same token, if $pR[t, t^{-1}] \cap R[It, t^{-1}]$ is a minimal prime of $R[It, t^{-1}]$ then p is a minimal prime of R.

On the other hand, let $\wp$ denote a minimal prime of $R[It, t^{-1}]$. Since t^{-1} is a regular element then $\wp R[It, t^{-1}]_{t^{-1}}$ is a prime ideal of the Laurent polynomial ring, hence must be of the form $pR[t, t^{-1}]$, for some $p \in \mathrm{Spec}\, R$. It follows that $\wp = pR[t, t^{-1}] \cap R[It, t^{-1}]$.

Summing up, any minimal prime of $R[It, t^{-1}]$ is of the form $pR[t, t^{-1}] \cap R[It, t^{-1}]$, for some $p \in \operatorname{Min}(R)$. It also follows that if $p \in \operatorname{Min}(R)$ then $pR[t, t^{-1}] \cap R[It, t^{-1}]$ is a minimal prime of the extended Rees algebra.

Finally, $R[It, t^{-1}]/pR[t, t^{-1}] \cap R[It, t^{-1}] \simeq \frac{R}{p}[\frac{(I,p)}{p}t, t^{-1}]$. Therefore, as in (7.3.3.1) one has

$$\dim R[It, t^{-1}] = \max_p \left\{ \dim \frac{R}{p}\left[\frac{(I,p)}{p} t, t^{-1} \right] \right\},$$

where p runs through the set of minimal primes of R. Thus, one is reduced to the case where R is a domain and $I \subset R$ is any ideal (possibly the null ideal). In this case, let $P := (It, t^{-1})R[It, t^{-1}]$, a prime ideal contracting to zero in R. Applying Proposition 2.5.39 to the inclusion $R \subset R[It, t^{-1}]$ yields

$$\dim R[It, t^{-1}] = \dim R + \operatorname{ht} P = \dim R + \operatorname{trdeg}_K K(t),$$

where K is the field of fractions of R. This proves the stated result with the bonus of having $\operatorname{ht}(It, t^{-1})R[It, t^{-1}] = 1$ (plainly, ≥ 1 anyway as t^{-1} is regular). □

Theorem 7.3.6. *If $(R, \mathfrak{m})$ is a Noetherian local ring and $I \subset \mathfrak{m}$ an ideal, then* $\dim \operatorname{gr}_I R = \dim R$.

Proof. If R is not necessarily local, then $\dim \operatorname{gr}_I R \leq \dim R[It, t^{-1}] - \operatorname{ht}(t^{-1}) \leq \dim R + 1 - 1 = \dim R$ by Proposition 7.3.5.

On the other hand, when R is local, let $p_0 \subsetneq p_1 \subsetneq \cdots \subsetneq p_d = \mathfrak{m}$ denote a maximal chain of primes, *i. e.*, $\dim R = d$. Then

$$p_0 R[t, t^{-1}] \cap R[It, t^{-1}] \subset \cdots \subset p_d R[t, t^{-1}] \cap R[It, t^{-1}] = \mathfrak{m} R[t, t^{-1}] \cap R[It, t^{-1}]$$

is a proper chain of primes. Note that $\mathfrak{m}R[t, t^{-1}] \cap R[It, t^{-1}] = (\mathfrak{m}, It)$. Therefore, $\operatorname{ht}(\mathfrak{m}, It) = \dim R$. Since $I \subset (\mathfrak{m}, It)$, one has $\dim \operatorname{gr}_I R \geq \dim(\operatorname{gr}_I R)_{(\mathfrak{m},It)} = \operatorname{ht}(\mathfrak{m}, It) = \dim R$. □

Remark 7.3.7. Same argument as above works if I is assumed to lie in the Jacobson radical of a Noetherian ring of finite Krull dimension.

7.3.2.2 The Artin–Rees lemma

In the proof of Krull's intersection theorem (Theorem 5.2.18), a crucial inclusion of certain submodules played a main role. Here, one wishes to strip this inclusion of its particularities and set it up in a general framework. This was the work of E. Artin and D. Rees, acting independently of each other.

As will be seen, the result is a simple consequence of the finite generation of certain graded modules over the standard graded Rees algebra $R[It]$ over a Noetherian ring R.

First, as for the version for ideals, which was Rees' original purpose, we have the following.

Proposition 7.3.8 ([127]). *Let R denote a Noetherian ring and let $I, J \subset R$ be two ideals. Then there exists an integer $k \geq 0$ such that*

$$I^n \cap J = I^{n-k}(I^k \cap J),$$

for all $n \geq k$.

Proof. Consider the Rees algebra $R[It] \subset R[t]$. An element of the homogeneous ideal $JR[t] \cap R[It]$ has the form $\sum_{i\geq 0} b_i t^i$, with $b_i \in J \cap I^i$. Pick a finite set of homogeneous generators of this ideal and let k be the highest degree among them. Then $I^n \cap J \subset I^{n-k}(I^k \cap J)$ for $n > k$, the reverse inclusion being trivial. □

A generalization to modules goes as follows: one still keeps one of the ideals, say, I, replaces the other ideal by a module N and introduces an auxiliary finitely generated R-module containing N.

The argument relies on the following notion.

Definition 7.3.9. Given an ideal $I \subset R$ and an R-module M, a decreasing filtration $M := M_0 \supset M_1 \supset \cdots$ of submodules is an *I-filtration* if $IM_i \subset M_{i+1}$ for every $i \geq 0$. The I-filtration is *stable* if $IM_i = M_{i+1}$ for $i \gg 0$.

Given an I-filtration $M := M_0 \supset M_1 \supset \cdots$, one sets

$$R_M[It] := \bigoplus_{i\geq 0} M_i,$$

a naturally graded $R[It]$-module with an action induced by the R-module structure of M_i and the rule $It \cdot M_i = IM_i \subset M_{i+1}$.

Lemma 7.3.10. *$R_M[It]$ is a finitely generated $R[It]$-module if and only if the corresponding I-filtration is stable.*

Proposition 7.3.11 (Artin–Rees for modules). *Let R denote a Noetherian ring. Given an ideal $I \subset R$ and R-modules $N \subset M$, with M finitely generated, then there exists an integer $k \geq 0$ such that*

$$I^n M \cap N = I^{n-k}(I^k M \cap N),$$

$R[It]$ for all $n \geq k$.

Proof. Besides the Rees algebra $R[It]$, consider the graded $R[It]$-module

$$R_M[It] := \bigoplus_{i\geq 0} I^i M.$$

Note that the role of M is merely as modular coefficients for the graded parts of $R[It]$. Therefore, $R_M[It]$ is generated by the elements of IM. □

7.3.3 The fiber cone and the analytic spread

Let $(R, \mathfrak{m})$ denote a Noetherian local ring and its unique maximal ideal. Given an ideal $I \subset \mathfrak{m}$, one defines the *fiber cone algebra* (or *special fiber algebra*) of I to be the $R/\mathfrak{m}$-algebra $F(I) := R[It]/\mathfrak{m}R[It]$. As the material flows, one usually omits the word "algebra" in the terminology.

The dimension of this algebra is called the *analytic spread* of I, denoted $\ell(I)$. This terminology was introduced by D. Rees, as a reminder of the case where I is generated by analytically independent elements, in which case the fiber cone is a polynomial ring over $R/\mathfrak{m}$. However, in other special cases, $\ell(I)$ will give the dimension of a certain $R/\mathfrak{m}$-subalgebra of $R[It]$ and, geometrically, one plus the dimension of the image of a certain rational map.

One has both upper and lower bounds for $\ell(I)$; first, one has the upper bounds, which are far easier.

Proposition 7.3.12. *For any ideal $I \subset \mathfrak{m}$, one has $\ell(I) \leq \min\{\mu(I), \dim R\}$.*

Proof. Since

$$F(I) \simeq \big(R[It]/IR[It]\big)/\big(\mathfrak{m}R[It]/IR[It]\big) = \operatorname{gr}_I(R)/\mathfrak{m}\operatorname{gr}_I(R)$$

then $\dim F(I) \leq \dim \operatorname{gr}_I(R) = \dim R$ by Theorem 7.3.6.

At the other end, the surjective homomorphism of (7.2.10.1) below induces the surjection

$$S_{R/\mathfrak{m}}(I/\mathfrak{m}I) \twoheadrightarrow R[It]/\mathfrak{m}R[It] = F(I).$$

Since $R/\mathfrak{m}$ is a field, $S_{R/\mathfrak{m}}(I/\mathfrak{m}I)$ is a polynomial ring of dim $\mu(I/\mathfrak{m}I) = \mu(I)$ (Krull–Nakayama). □

If the minimum above is attained, one says that I has *maximal analytic spread*.

7.3.3.1 Reductions

The above upper bounds resulted from some external comparison. For the lower bound, one needs an "internal" comparison, namely via considering certain distinguished subideals of I. This is the theory of reductions introduced by Northcott and Rees ([121]). Some of its features have been considered in Section 2.2.3, but for the reader convenience one starts anew.

Let R denote a Noetherian local ring and $I \subset R$ a proper ideal.

Definition 7.3.13. A subideal $J \subset I$ is a *reduction* of I if, equivalently:

(i) For any $a \in I$, there exists $n \geq 1$ such that

$$a^n + b_1 a^{n-1} + \cdots + b_{n-1}a + b_n = 0, \tag{7.3.13.1}$$

for certain $b_i \in J^i$, $1 \leq i \leq n$.

(ii) The equality $I^n = JI^{n-1}$ holds for $n \gg 0$.
(iii) $R[It]$ is a finitely generated module over its subalgebra $R[Jt]$.

Proof (*That the three stated conditions are equivalent*). (i) $\Rightarrow$ (ii) Fixing $a \in I$, by assumption one has

$$a^n = -b_1 a^{n-1} - \cdots - b_{-1} a - b_n \in (JI^{n-1}, \ldots, J^{n-1}I, J^n) \subset JI^{n-1},$$

for some n (depending on a). Now pick a finite set of generators of I and take $n \gg 0$ so as to have $a^n \in JI^{n-1}$ for every $a \in I$.

(ii) $\Rightarrow$ (iii) By assumption, $R[It]$ is generated by the finite set $\{R, It, \ldots, I^{n-1}t^{n-1}\}$ as an $R[Jt]$-module. Since I is finitely generated, one is done.

(iii) $\Rightarrow$ (i) Say, $\{R, It, \ldots, I^{n-1}t^{n-1}\}$ generates $R[It]$ as an $R[Jt]$-module. Then, for every $a \in I$, by homogeneity one has a relation

$$a^n t^n = (b_1 t)(a^{n-1}t^{n-1}) + \cdots + (b_{n-1}t^{n-1})(at) + b_n t^n,$$

for certain $b_i \in J^i$, $1 \leq i \leq n$. The result follows by "canceling" t^n in both sides. □

Condition (i) above is the notion of the ideal I being *integral* over its subideal J, as discussed in Section 2.2.3. The condition immediately implies that J and I share the same radical. In particular, $\operatorname{ht} J = \operatorname{ht} I$. As to condition (ii), the following concept emerges.

Definition 7.3.14. Let $J \subset I$ be a reduction. The least integer $n - 1 \geq 0$ satisfying condition (ii) is called the *reduction number* of J.

Winning the game here is to find J as "small" as possible, say, with smallest possible number of generators.

As a starter, one takes a naive notion of minimality: one says that a reduction $J \subset I$ of an ideal I is *minimal* if it does not properly contain another reduction of I. This terminology was introduced by Northcott and Rees ([121]).

When J runs through the set of minimal reductions of I, the *absolute reduction number* of I is the minimum of the reduction numbers of these reductions. In general, for a particular minimal reduction, its reduction number may be larger than the absolute one.

Another important related notion was brought up by Chevalley ([34]). For this, recall that the fiber cone algebra $R[It]/\mathfrak{m}R[It]$ is a standard graded k-algebra, where $k = R/\mathfrak{m}$. As such it is generated over k by $I/\mathfrak{m}I$. Any set of elements $\{a_1, \ldots, a_r\} \subset I$ defines a homomorphism of k-graded algebras

$$\rho : k[X_1, \ldots, X_r] \to k[\overline{a}_1, \ldots, \overline{a}_r] \subset R[It]/\mathfrak{m}R[It], \quad X_i \mapsto \overline{a}_i, \tag{7.3.14.1}$$

where $\overline{a}_i$ denotes the image of a_i in $I/\mathfrak{m}I$.

Definition 7.3.15. A set of elements $\{a_1, \ldots, a_r\} \subset I$ is said to be *analytically independent* in I if ρ in (7.3.14.1) is injective.

It is clear that this notion is a natural analogue of algebraic independence in field theory. The sequel will also explain the choice of Northcott and Rees for the terminology analytic spread.

Proposition 7.3.16. *Let $(R, \mathfrak{m})$ denote a Noetherian local ring such that $R/\mathfrak{m}$ has infinitely many elements. Then, for any ideal $I \subset \mathfrak{m}$, one has:*

(i) *Any set of minimal generators of a minimal reduction J of I is analytically independent.*

(ii) $\operatorname{ht} I \leq \ell(I)$.

Proof. (i) (Northcott–Rees) The proof has some similarity with the proof of the Noether normalization lemma over an infinite field—and in fact, the content of this item is equivalent of having a Noether normalization (as in the conclusion below in item (ii)). Thus, let $\{a_1, \ldots, a_r\}$ be a minimal set of generators of J and assume that $\overline{F} = \overline{F}(X_1, \ldots, X_r) \in \ker \rho$ as in (7.3.14.1) stand for a form of degree d.

Claim 1. The coefficient of the term in X_1^d vanishes.

Lift $\overline{F}$ to a form F over R. If the coefficient does not vanish, one must have $a_1^d \in (a_2, \ldots, a_r)J^{d-1} \equiv 0 \bmod I^d\mathfrak{m}$. Then $J^d \subset (a_2, \ldots, a_r)J^{d-1} \equiv 0 \bmod I^d\mathfrak{m}$. Say, $JI^m = I^{m+1}$, for some $m \geq 0$. After sufficient manipulation, one gets rid of J, obtaining $I^{m+d} \subset (a_2, \ldots, a_r)I^{m+d-1} \equiv 0 \bmod I^{m+d}\mathfrak{m}$. By Krull–Nakayama, $I^{m+d} \subset (a_2, \ldots, a_r)I^{m+d-1}$. This says that $(a_2, \ldots, a_r)$ is a reduction of I, contradicting the minimality of J and the minimality of the set of generators of J.

Claim 2. Let $\{c_1, \ldots, c_r\} \subset R$ be an arbitrary set of elements such that some $c_i \not\equiv 0 \bmod \mathfrak{m}$. Then there exists an $r \times r$ matrix invertible over R such that $(c_1 \ldots c_r)$ is its first row.

This can be proved by induction on r and is left to the reader.

Applying to $\{a_1, \ldots, a_r\}$ the elementary transformation corresponding to such a matrix $(c_{i,j})$, with $c_{1,1} = c_1, \ldots, c_{1,r} = c_r$, yields another set of minimal generators of J such that the new form $G = F(\sum c_{1,j}X_j, \ldots, \sum c_{r,j}X_j) \in R[X_1, \ldots, X_n]$ vanish on it modulo $I^d\mathfrak{m}$. Applying the result of Claim 1 to this form, one obtains that the coefficient of its X_1^d term vanishes modulo $\mathfrak{m}$. But this coefficient is $F(c_1, \ldots, c_r)$. Since there are infinitely many such sets of elements, $k = R/\mathfrak{m}$ being infinite forces the vanishing of $\overline{F}$, as required.

(ii) Let $J \subset I$ be a minimal reduction. It suffices to show that a minimal set of generators of J has (at most) $\ell(I)$ elements. For this, item (iii) of Definition 7.3.13 implies that $R[It]/\mathfrak{m}R[It]$ is a finitely generated module over the subalgebra generated by a minimal set of generators of J. Therefore, the latter has dimension $\ell(I)$ and since by (i) it is a polynomial ring over k, it follows that a minimal set of generators of J has $\ell(I)$ elements. □

Proposition 7.3.17. *Let $(R, \mathfrak{m})$ denote a Noetherian local ring such that $R/\mathfrak{m}$ is infinite. Then the following assertions are equivalent:*

(i) *I has no proper reductions.*
(ii) *I is generated by an analytically independent set in I.*
(iii) $\ell(I) = \mu(I) = \dim_k(I/\mathfrak{m}I)$.

Proof. (i) $\Rightarrow$ (ii) Since I has no proper reductions, it is a minimal reduction o itself, hence this implication follows from item (i) of the previous proposition.

(ii) $\Rightarrow$ (iii) Let $\{a_1, \ldots, a_r\}$ denote an analytically independent set in I generating I. Then the fiber cone is a polynomial ring in r variables over k, hence has dimension r. Therefore, $\ell(I) = r$. To conclude that $\ell(I) = \mu(I)$, it suffices to argue that any analytically independent set in I is a minimal set of generators of the ideal they generate. But this is clear from the very definition.

(iii) $\Rightarrow$ (i) Let $J \subset I$ denote a minimal reduction of I and let $\{a_1, \ldots, a_r\}$ denote a set of minimal generators of J. By item (i) of the previous proposition, this set is analytically independent in I, hence the subalgebra their residues generate in the fiber cone $R[It]/\mathfrak{m}R[It]$ is isomorphic to $k[X_1, \ldots, X_r]$. Since J is a reduction of I this inclusion is a finite module, hence $\ell(I) = r$. By assumption, then $\mu(I) = r$. Therefore, the result is a consequence of the following.

Claim. $\{a_1, \ldots, a_r\}$ can be extended to a set of minimal generators of I.

First, quite generally, for any ideals $J \subset I \subset \mathfrak{m}$, any minimal set of generators of J can be extended to one of I if and only if $J \cap \mathfrak{m}I = \mathfrak{m}J$. Indeed, this follows from tensoring the inclusion $J \subset I$ with $R/\mathfrak{m}$ so as to get $J \cap \mathfrak{m}I/\mathfrak{m}J = \ker(J/\mathfrak{m}J \to I/\mathfrak{m}I)$. Then one argues with dimensions of k-vector spaces and the Krull–Nakayama lemma.

At the other end, $J \cap \mathfrak{m}I/\mathfrak{m}J = 0$ if and only if $\dim_k(J/\mathfrak{m}J) = \dim_k(J/J \cap \mathfrak{m}I)$, so one proceeds to show this dimension equality. Letting $\{a_1, \ldots, a_r\} \subset J$ be such that their residues modulo $J \cap \mathfrak{m}I$ form a k-basis of $J/J \cap \mathfrak{m}I$, one argues that the ideal $(a_1, \ldots, a_r) \subset J \subset I$ is also a reduction of I. More generally, if J', J'' are two ideals with $J'' \subset \mathfrak{m}I$, such that (J', J'') is a reduction of I, then J' is a reduction of I. This follows immediately from the Krull–Nakayama lemma.

Now, since J is a minimal reduction, $\{a_1, \ldots, a_r\}$ generates J and is necessarily a set of minimal generators of J. Then the residues of these generators give a k-basis of $J/\mathfrak{m}J$, thus showing the sought vector dimension equality. □

Remark 7.3.18. If any of the conditions in the above proposition holds for $I = \mathfrak{m}$, then $\mathfrak{m}$ is generated by a regular sequence, *i. e.*, R is a regular local ring. This has been generalized to prime ideals of the principal class, *i. e.*, generated by a set of generators of cardinality equal to its height ([41]). For nonprime ideals, the question seems more difficult.

7.3.4 Ideals of linear type, II

Proposition 7.2.28 yields a general template to decide whether an ideal is of linear type. Although the condition (F_1) is often verifiable in the context, not so much un-

mixedness, which may require a previous knowledge about the associated primes of the symmetric algebra.

The question is whether one can replace (F_1) by a "slightly" stronger hypothesis that takes over the role of unmixedness. The notion that comes naturally to mind is that of analytically independent elements, through the impact of Proposition 7.3.17. Note that if $(R, \mathfrak{m})$ is a Noetherian local ring and $I \subset \mathfrak{m}$ is an ideal generated by analytically independent elements then it satisfies (F_1). Indeed, one has $\ell(I) = \mu(I) = \dim \mathcal{F}(I) \leq \dim \operatorname{gr}_I(R) = \dim R$.

Taking this approach, the following "half-way" path to linear type has been devised by C. Huneke ([83]):

Proposition 7.3.19. *Let R be a Noetherian reduced ring and let $I \subset R$ be an ideal of grade ≥ 1. Then the following statements are equivalent:*

(i) $S_R(I)^{\mathrm{red}} \simeq R[It]$.

(ii) I_P *is generated by analytically independent elements for every prime ideal* $P \in \operatorname{Spec} R$ *containing* I.

Proof. (i) $\Rightarrow$ (ii). The question is evidently local, so by localizing one can assume that $(R, \mathfrak{m})$ is local. By assumption, $\mathcal{K} := \ker S_R(I) \to R[It]$ is nilpotent, hence $\mathcal{K} \subset \mathfrak{m}S_R(I)$ since the latter is a prime ideal because $S_R(I)/\mathfrak{m}S_R(I)$ is a polynomial ring over $R/\mathfrak{m}$. But then $\mathcal{F}(I) = R[It]/\mathfrak{m}R[It] \simeq S_R(I)/\mathfrak{m}S_R(I)$ is a polynomial ring over $R/\mathfrak{m}$, *i. e.*, I is generated by analytically independent elements.

(ii) $\Rightarrow$ (i). It suffices to show that $\ker S_R(I) \to R[It]$ is nilpotent locally everywhere on $\operatorname{Spec} S_R(I)$. Since R is reduced, then so is $R[It]$. Therefore, the canonical surjection $S_R(I) \to R[It]$ implies a surjection $S_R(I)^{\mathrm{red}} \to R[It]$.

But if $P \in \operatorname{Spec} S_R(I)$ then $S_R(I)_P = S_R(I)_{\wp}$, where $\wp = R \cap P$. Therefore, the problem is local on $\operatorname{Spec} R$ as well, so one can assume that $(R, \mathfrak{m})$ is local. By induction on $\dim R$, $S_R(I_{\wp})^{\mathrm{red}} \simeq R[I_{\wp}t]$ for $\wp \neq \mathfrak{m}$ and one wishes that $S_R(I)^{\mathrm{red}} \simeq R[It]$ as well. But locally on $\operatorname{Spec} R \setminus \{\mathfrak{m}\}$ the induced map $S_R(I)^{\mathrm{red}} \to R[It]$ is injective by the present assumption. Then, taking presentations,

$$S_R(I) \simeq R[\mathbf{T}]/\mathcal{J} \twoheadrightarrow R[It]/\mathcal{I},$$

induced by a set of analytically independent generators of I, one has $\mathfrak{m}^t\mathcal{I} \subset \sqrt{\mathcal{J}}$ for some $t \geq 0$. But $\mathcal{I} \subset \mathfrak{m}R[\mathbf{T}]$ by analytic independence. Thus, a power of $\mathcal{I}$ lies in $\mathcal{J}$, hence $\mathcal{I} = \sqrt{\mathcal{J}}$, thus proving the assertion. □

Remark 7.3.20. For a slightly different argument, see [159, Proposition 2.2.4].

7.3.4.1 Determinantal ideals

One focus on ideals of minors of notable matrices. Because ideals of linear type satisfy the property (F_1) there are just a few sizes of minors that stand a chance to be so. Thus, for an $r \times s$ matrix $\mathcal{A}$ and $t \leq \min\{r, s\}$, typically $I_t(\mathcal{A})$ will require anything near

$\binom{r}{t}\binom{s}{t}$ generators, while the ground ring of the entries may well have a much smaller dimension.

But there is another obstruction lying on a subtler level and that is the existence of the so-called Plücker relations. Those are quadratic polynomial relations of the t-minors that exist provided $2 \leq t \leq s-2$. Thus, *e.g.*, denoting the 2-minors of a 2×4 matrix by $\Delta_{i,j}$ $(1 \leq i < j \leq 4)$, there is a relation $\Delta_{1,2}\Delta_{3,4} - \Delta_{1,3}\Delta_{2,4} + \Delta_{1,4}\Delta_{2,3} = 0$. But, clearly an ideal of linear type cannot admit such polynomial relations because the corresponding fiber cone is a polynomial ring.

To bring up the discussion to the "generic" level, one considers initially the case where the entries are indeterminates over a ground ring. In this case, one has the following.

Theorem 7.3.21 (The ideal of submaximal minors is of linear type [83]). *Let R be a Noetherian domain and let $\mathcal{A} = (X_{i,j})$ denote an $r \times r$ matrix of indeterminates over R. Then the ideal of submaximal minors of $(X_{i,j})$ is of linear type.*

Proof. Set $\mathbf{X} = \{X_{i,j}\}$ and $I := I_{r-1}(\mathbf{X})$. One proceeds by steps, as follows.

Claim 1. I is locally everywhere on $\operatorname{Spec} R[\mathbf{X}]/I$ generated by analytically independent elements.

Induct on r. If $r = 1$, there is nothing to prove, so assume that $r \geq 2$.

Let $P \in \operatorname{Spec} R[\mathbf{X}]$ contain I and consider the localization $I_P \subset R[\mathbf{X}]_P$. If $I_1(\mathcal{A}) \subset P$, then $P = (\wp, (\mathbf{X}))$, where $\wp = P \cap R =$ so one can first take fractions relative to $R \setminus \{\wp\}$. Thus, one may assume that $(R, \mathfrak{m})$ is local and $P \cap R = \mathfrak{m}$. Let K denote the field of fractions of R. Then one has an inclusion

$$R[\mathbf{X}]_P[It] \subset K[\mathbf{X}]_{(\mathbf{X})}[I_K t] \subset K[\mathbf{X}]_{(\mathbf{X})}[t],$$

where $I_K = I \otimes_R K$. Since one can take the same set of generators of I throughout, one has an inclusion $\mathcal{I} \subset \mathcal{I}_K$ of the respective defining ideals of the two Rees algebras. Thus, it suffices to show the inclusion $\mathcal{I}_K \subset (\mathbf{X})_{(\mathbf{X})}[\mathbf{T}]$, where $\mathbf{T} = \{T_{i,j}\}$ with $T_{i,j}$ mapping to the cofactor $\Delta_{i,j}$ of $X_{i,j}$. But this follows from the fact that the cofactors are algebraically independent over K, *i.e.*, that the field extension $K(\Delta_{i,j}) \subset K(\mathbf{X})$ is algebraic—this fact is possibly long known as it depends essentially on the easy equality $\det(\mathcal{A})^{r-1} = \det \operatorname{Cof}(\mathcal{A})$, where $\operatorname{Cof}(\mathcal{A})$ is the matrix of the cofactors of $\mathcal{A}$ (see [27, Proposition 10.16 (b)], also [40]).

Thus, one now assumes that $I_1(\mathcal{A}) \subsetneq P$. Then locally at P some entry of $\mathcal{A}$ is invertible, say, $X_{1,1}$. Upon taking first fractions with respect to the powers of $X_{1,1}$, by the usual row/column elementary transformations, $\mathcal{A}$ is conjugate to a matrix with zeros throughout first row and first column, except $X_{1,1}$. It follows that the submaximal minors of this matrix is generated by the $(r-2)\times(r-2)$ minors of the submatrix obtained by omitting its first row and column. Since the ideal of minors is unchanged by elementary transformations, one has that $I_{X_{1,1}}$ it too is generated by these minors. It remains to show that one is in a position as to apply the inductive hypothesis. For this, as in

the proof of Theorem 6.4.6, one has to make sure that upon localization one still has a localization of a polynomial ring over a Noetherian ring, namely, that $R[\mathbf{X}][X_{1,1}^{-1}]$ be a ring of polynomials over a Noetherian subring. But indeed, $R[\mathbf{X}][X_{1,1}^{-1}] = \widetilde{R}[\widetilde{\mathbf{X}}]$, where

$$\widetilde{R} := R[X_{1,1}, \dots, X_{1,r}; X_{2,1}, \dots, X_{r,1}, X_{1,1}^{-1}] \quad \text{and} \quad \widetilde{\mathbf{X}} = \{X_{i,j} - X_{i,1}X_{1,j}X_{1,1}^{-1}\}_{\substack{2\le i\le r\\ 2\le j\le r}}.$$

Now, since $\{X_{i,j}, 2 \le i \le r, 2 \le j \le r\}$ is an algebraically independent set over $\widetilde{R}$ and $X_{i,1}X_{1,i}X_{1,1}^{-1} \in \widetilde{R}$, then so is the set $\widetilde{\mathbf{X}}$. Therefore, up to a trivial isomorphism, $R[\mathbf{X}][X_{1,1}^{-1}]$ is of the desired form and one can apply induction to conclude that $I_P = (I_{X_{1,1}})_P$ is generated by analytically independent elements.

So much for Claim 1. By Proposition 7.3.19, $S_{R[\mathbf{X}]}(I)^{\mathrm{red}} \simeq R[\mathbf{X}][It]$.

Claim 2. The image of $D := \det \mathcal{A} \in I$ as an element of degree 1 in $S_{R[\mathbf{X}]}(I)$ is not nilpotent.

From Claim 1 and Proposition 7.3.19, it would follow that the image Dt in $R[\mathbf{X}][It]$ is zero, which is absurd, since $D \neq 0$ in $R[\mathbf{X}]$.

Claim 3. The residue algebra $S_{R[\mathbf{X}]}(I)/DS_{R[\mathbf{X}]}(I)$ is reduced.

This is the hardest. Part of it is accomplished within the framework of the book by invoking the Scandinavian complex; actually, it suffices to use the obvious cofactor relations of the submaximal minors as pointed out there (6.4.2). Thus, by letting again $\mathbf{T}$ denote new variables to present $S_{R[\mathbf{X}]}(I)$ as an $R[\mathbf{X}, \mathbf{T}]$-algebra, one gets, perhaps not minimally:

$$S_{R[\mathbf{X}]}(I)/DS_{R[\mathbf{X}]}(I) \simeq R[\mathbf{X}, \mathbf{T}]/(I_1(\mathcal{A}\mathcal{B}), I_1(\mathcal{B}\mathcal{A})),$$

where $\mathcal{B}$ denotes the matrix of $\mathbf{T}$ entries.

Then one draws upon the results of [149], also [95], to the effect that if R is reduced then the above ideal is radical.

Summing up, we have the following.

Claim 4. $S_{R[\mathbf{X}]}(I)$ is reduced.

By Claim 3, the nilradical $\sqrt{0} \subset S := S_{R[\mathbf{X}]}(I)$ is contained in the principal ideal DS. Thus, any nilpotent $f \in S$ is of the form gD, for some $g \in S$. But since $D \notin \sqrt{0}$, it follows that $g \in \sqrt{0}$. This gives $\sqrt{0} \subset D\sqrt{0}$, hence $\sqrt{0} = 0$ by Krull–Nakayama. □

Remark 7.3.22. A similar result has been shown in the case of the generic symmetric matrix ([95]) and the Pfaffians of the generic skew–symmetric matrix ([14]). The methods are those of Young diagrams and tableaux and Hodge algebras, important facets of algebraic combinatorics, regrettably outside the scope of the book.

A much easier example of determinantal ideal of linear type consists of the maximal minors of a generic $(r+1) \times r$ matrix. More precisely, one has the following.

Proposition 7.3.23. *Let R denote a Cohen–Macaulay domain and let $\mathcal{A} = (X_{i,j})$ be a generic $(r+1) \times r$ matrix. Then the ideal $I_r(\mathcal{A})$ is of linear type.*

Proof. Set $I = (r+1) \times r$. One applies Proposition 7.2.28. By the theorem of Hilbert–Burch (Theorem 6.2.32), $\mathcal{A}$ is the syzygy matrix of I. Using this canonical presentation, one sees that the property (F_1) follows immediately from Theorem 6.4.6.

As for the unmixedness property, note that, since (F_1) obviously implies (F_0), then $\dim S_R(I) = \dim R+1$. Therefore, as R is Cohen–Macaulay, one has $\operatorname{ht} \mathcal{J} = \dim R+r+1-(\dim R+1) = r$, where $R[\mathbf{T}]/\mathcal{J} \simeq S_R(I)$. But $\mathcal{J}$ is generated by r forms and again, since R is Cohen–Macaulay, then $\mathcal{J}$ is generated by a regular sequence. Therefore, $S_R(I)$ is Cohen–Macaulay. □

Remark 7.3.24. Note that the above result may comfortably hold even for certain Cohen–Macaulay specializations of the polynomial ring $R[\mathbf{X}]$: all one needs is that (F_1) be satisfied.

7.3.4.2 Sequences

While in the preceding examples, the given ideal had a kind of "external" character, in the sense that it carried a canonically defined set of generators, the present one will have some "internal" character, namely, will depend on admitting a set of generators of a particular behavior.

The following notion has been introduced by C. Huneke ([79]). It had previously been defined by M. Fiorentini ([57]) in a slightly different form.

Definition 7.3.25. A set of elements $a_1, \dots, a_n$ in a ring R is called a *d-sequence* if it satisfies the following equalities:

$$(a_{i_1}, \dots, a_{i_l}) : a_t a_m = (a_{i_1}, \dots, a_{i_l}) : a_t,$$

for all $\{i_1, \dots, i_l\} \subset \{i_1, \dots, i_n\}$, $t, m \in \{i_1, \dots, i_n\} \setminus \{i_1, \dots, i_n\}$.

Often, a minimality condition is imposed on $a_1, \dots, a_n$ as a set of generators of the ideal it generates in R.

Clearly, any permutable regular sequence is a d-sequence, but the latter is a lot more flexible to move around as shown in [70, Section 6]. There is an interesting list of examples of ideals having a d-sequence as a set of generators ([79]). Here, the main focus is on the following result.

Proposition 7.3.26 ([79, Theorem 3.1]). *Let R be a Noetherian ring and $I \subset R$ an ideal generated by a d-sequence. Then I is of linear type.*

Proof. The original proof by Huneke is quite involved and long. The following shorter argument can be found in [70, Proposition 3.6], by usage of the following result of Valla ([153]; see also [70, Proposition 3.3]):

Claim 1. Let R be a Noetherian ring and $I \subset R$ be an ideal. Suppose there is an element $a \in I$ such that $(0 : a) \cap I^t \subset (0 : a)I^t$ for every $t \geq 0$. If $I/(a)$ is of linear type as an ideal of $R/(a)$ then I is of linear type.

The proof of these results is pretty much the same as the main step in the proof of Proposition 7.2.12, so much as one proves the following simple facts.

Claim 2. If $\{a_1, \dots, a_n\}$ is a d-sequence in R, then the residues of $\{a_2, \dots, a_n\}$ in $R/(a_1)$ form a d-sequence.

This follows immediately from the definition.

Claim 3. $(0 : a_1) \cap (a_1, \dots, a_n) = \{0\}$.

This is again quite clear by induction on n, so the details are left to the reader. □

Example 7.3.27 ([80]). The maximal minors of a generic $r \times (r+1)$ matrix over a field form a d-sequence.

The proof of this is not trivial, involving the fact that the ideal of the maximal minors in this case is prime (Eagon–Northcott) and some linear algebra of cofactor theory. It implies the result of Proposition 7.3.23 in a rather roundabout fashion. Another homological theoretic roundabout way is by use of the so-called $\mathcal{M}$-complex of [70]. The interested reader is urged to refer to these sources for further details.

7.3.5 Special properties (survey)

In this section, one surveys a few situations as regards notable properties, normality and Cohen–Macaulayness being foremost. The totality of such results in this respect is too vast and would easily itself fill up a book. Thus, it is to expect that many interesting pieces will not be found here.

Since this is but a survey, no proofs will be given, for which one counts on the reader's indulgence. Some of these could actually be reproduced here without much toil, but others are quite harder, involving additional technology not developed in the book.

7.3.5.1 Smoothness

Perhaps a natural reason for focusing on the Cohen–Macaulay and normality properties is the fact that very seldom a blowup algebra is smooth in its projective version, even though this sounds like a surprise as they are supposed to be the tool by excellence to resolve singularities. Of course, in resolution of singularities one usually blows along a regular center. For that, one has the following general result.

Proposition 7.3.28 ([69, 14.8], [123, Theorem 2.1]). *Let* $(R, \mathfrak{m})$ *denote a local ring and let* $I \subset \mathfrak{m}$ *be an ideal generated by a regular sequence of length* ≥ 2. *Then* $\operatorname{Proj}(\mathcal{R}(I))$ *is smooth if and only if* R/I *is regular.*

The proof is not difficult, but the result itself will not play a role in this book. However, it should be noted that it forces the ambient ring to be regular and the regular sequence to be a regular subsystem of parameters.

As a consequence, it would seem natural to seek for weaker properties that may actually throw additional light on the structure of the ideals in question.

7.3.5.2 Regular sequences

Perhaps among the earliest results is the case of a regular sequence.

Proposition 7.3.29 (Valla [152]). *Let R be a Noetherian Cohen–Macaulay ring and let $I \subset R$ be an ideal generated by a regular sequence. Then $\mathcal{R}_R(I^n)$ is Cohen–Macaulay for any $n \geq 1$.*

Valla actually showed that if $\{a_1, \ldots, a_r\}$ is a regular sequence in a Noetherian ring R then, for any $n \geq 1$, the sequence $\{a_1^n, a_1^n T + a_2^n, \ldots, a_{r-1}^n T + a_r^n, a_r^n T\}$ is regular in $R[I^n T] \subset R[T]$. Then one can show that this can be extended to a full maximal regular sequence in $R[I^n T]$ by elements of R.

Now, if R is moreover a domain, since $\dim R[I^n T] = \dim R + 1 = \dim R + \operatorname{ht}(I^n T)$ (the second equality by Proposition 2.5.39) then the grade of the positively graded ideal $(I^n T)$ is at most 1. Thus, a regular sequence in $R[I^n T]$ could use at most one homogeneous element. This throws some light on the format obtained by Valla.

On the other hand, the residue of Valla's regular sequence in $\operatorname{gr}_{I^n}(R)$ is the regular sequence of homogeneous elements $\{(a_1^n)^*, \ldots, (a_{r-1}^n)^*, (a_r^n)^*\}$ (note that $\operatorname{gr}_{I^n}(R)$ is also Cohen–Macaulay and this regular sequence can likewise be extended to a full regular sequence by elements of the base ring R/I^n).

7.3.5.3 Primary ideals in dimension 2

This is probably the best known of the topics concerning integrally closed and normal ideals. The early core was the work by Zariski on complete (*i. e.*, integrally closed in nowadays terminology) ideals in 2-dimensional local rings ([169, Appendix 5]). He proved, among other things, the following.

Proposition 7.3.30. *Let $(R, \mathfrak{m})$ be a 2-dimensional regular local ring. If $I \subset R$ is an integrally closed $\mathfrak{m}$-primary ideal, then the Rees algebra $\mathcal{R}_R(I)$ is normal.*

What was actually proved is that the product of two such integrally closed ideals is integrally closed, hence all powers of an integrally closed ideal are integrally closed, *i. e.*, such an ideal is normal.

One of the first results in the aftermath of Zariski's work was proved by J. Lipman and B. Teissier ([104]) and one version can be stated in the following way.

Proposition 7.3.31. *Let $(R, \mathfrak{m})$ be a Noetherian local 2-dimensional ring with infinite residue field and let $I \subset R$ be an integrally closed $\mathfrak{m}$-primary ideal. Then the reduction number of any minimal reduction of I is* 1.

Although the assertion looks quite simple, no elementary proof is apparently known. The original proof is complex analytically minded, by means of the Briançon–

Skoda theorem, while a second proof by C. Huneke and J. Sally ([84]) involves elements of monoidal transformations à la Zariski.

One basic ingredient of Zariski's theory is the notion of a contracted ideal (from a monoidal extension). The nowadays terminology for such ideals is $\mathfrak{m}$-*full*. The terminology is due to Rees, later investigated by J. Watanabe ([161]). A thorough review of these ideals can be found in the beautiful book by I. Swanson and C. Huneke ([150]). It can be shown, among other things, that an integrally closed ideal in a 2-dimensional regular local ring is $\mathfrak{m}$-full, but not vice versa. Drawing upon this idea, the following addendum to the theorem of Zariski was subsequently proved.

Proposition 7.3.32 ([150, Theorem 3.2]). *Let $(R, \mathfrak{m})$ be a 2-dimensional regular local ring. If $I \subset R$ is an integrally closed $\mathfrak{m}$-primary ideal then the Rees algebra $\mathcal{R}_R(I)$ is Cohen–Macaulay and has minimal multiplicity.*

The multiplicity above is the usual local multiplicity with respect to the maximal graded ideal $\mathcal{N} := (\mathfrak{m}, \mathcal{R}_R(I)_+)$. The proof is based on the above Proposition 7.3.31 and a careful choice of a system of parameters of $\mathcal{N}$ pretty much in the shape of the regular sequence established in the proof of Proposition 7.3.29. This is a very natural proof as compared to the technology employed in the previous results.

The condition for the Cohen–Macaulay property of the Rees algebra has previously been established in the following way.

Proposition 7.3.33 ([61]). *Let $(R, \mathfrak{m})$ be a 2-dimensional Cohen–Macaulay local ring with infinite residue field and let $I \subset R$ be an $\mathfrak{m}$-primary ideal. Then $\mathcal{R}_R(I)$ is Cohen–Macaulay if and only if the reduction number of a minimal reduction of I is* 1.

This result has a far-out generalization as follows, as remarked by various authors.

Proposition 7.3.34. *Let $(R, \mathfrak{m})$ be a 2-dimensional regular local ring and let $I \subset R$ be an $\mathfrak{m}$-primary ideal. If $\mathcal{R}_R(I)$ is normal, then it is Cohen–Macaulay.*

If one wishes to bring up the associated graded ring $\operatorname{gr}_I(R)$ as well, then one has in any dimension.

Proposition 7.3.35 ([61], Huneke (unpublished)). *Let $(R, \mathfrak{m})$ be a regular local ring and let $I \subset R$ be an $\mathfrak{m}$-primary ideal. Then $\mathcal{R}_R(I)$ is Cohen–Macaulay if and only if $\operatorname{gr}_I(R)$ is Cohen–Macaulay.*

The original version of this theorem required that, moreover, the reduction number of I be $\leq \dim R - 1$, while Huneke showed that this is automatic if $\operatorname{gr}_I(R)$ is Cohen–Macaulay, arguing by means of the Briançon–Skoda theorem.

In order to retain the reduction number as a main actor, a slightly different version was given by Trung–Ikeda.

Proposition 7.3.36 ([151]). *Let $(R, \mathfrak{m})$ be a regular local ring of dimension d and let $I \subset R$ be an $\mathfrak{m}$-primary ideal. Then $\mathcal{R}_R(I)$ is Cohen–Macaulay if and only if I has a minimal*

reduction J with reduction number $\leq d-1$ and, in addition, $I^n \cap J = JI^{n-1}$ for all $n = 2, \ldots, d-1$.

To conclude, one has the following general criterion for a normal ideal.

Proposition 7.3.37 ([71, Propositions 2.1.2 and 2.1.3]). *Let R be a Noetherian normal domain and let $I \subset R$ be an ideal. The following conditions are equivalent:*
(i) *I is normal.*
(ii) *$I\mathcal{R}_R(I)$ is an integrally closed ideal.*
(iii) *There is a primary decomposition*

$$IR[It] = P_1^{(l_1)} \cap \cdots \cap P_r^{(l_r)},$$

where P_i is a height one prime ideal of $\mathcal{R}_R(I)$.

In the special case of monomial $\mathfrak{m}$-primary ideals in $k[x, y]$, a detailed study has been taken up in [126] and [59].

7.3.5.4 Structured conditions

From the early period, we have the following.

Proposition 7.3.38 ([70, Proposition 9.3]). *Let R be a Cohen–Macaulay ring and let $I \subset R$ be an ideal of positive height. Assume that:*
(1) *R/I and the symmetric algebra $\mathcal{S}_R(I)$ are Cohen–Macaulay.*
(2) *I is generically a complete intersection.*

Then the following conditions are equivalent:
(i) *I is an ideal of linear type (in particular, $\mathcal{R}_R(I)$ is Cohen–Macaulay).*
(ii) *$\mathcal{S}_{R/I}(I/I^2)$ is Cohen–Macaulay.*
(iii) *I satisfies (F_1) (i. e., $\mu(I_P) \leq \operatorname{ht} P$, for every prime $P \supset I$).*

Moreover, the following conditions are equivalent:
(i) *$\mathcal{S}_{R/I}(I/I^2)$ is R/I-torsion-free.*
(ii) *$\mu(I_P) \leq \operatorname{ht} P$, for every prime $P \supset I$ such that $\operatorname{ht} P \geq \operatorname{ht} I + 1$.*
(iii) *$\operatorname{ht} F_s(I) \geq s+1$ in the range $\operatorname{ht} I + 1 \leq s \leq \mu(I)$, where F_s denotes the Fitting ideal of order s.*

As an application, one has the following.

Proposition 7.3.39. *Let R be a Cohen–Macaulay ring and let $I \subset R$ be an ideal of finite homological dimension satisfying the property (F_1). If $\operatorname{ht} I = 2$ or else $\operatorname{ht} I = 3$ and R/I is Gorenstein, then I is of linear type and $\mathcal{R}_R(I)$ is Cohen–Macaulay.*

The following result contains some elements of surprise.

Proposition 7.3.40 ([142], [85]). *Let R be a regular local ring and let $I \subset R$ be an ideal of height ≥ 2. Suppose that:*
(i) *I is a radical generically complete intersection.*
(ii) *$\mathrm{gr}_I(R)$ is reduced.*
Then:
(a) *$\mathrm{gr}_I(R)$ is torsion-free over R/I.*
(b) *$\mathcal{R}_R(I)$ is Cohen–Macaulay.*
If in addition I is a prime ideal then $\mathrm{gr}_I(R)$ is a Gorenstein domain.

The supplementary assertion is essentially due to Hochster ([73]); for another argument see [71].

The Gorenstein property of a Rees algebra is however quite restrictive, in the following sense.

Proposition 7.3.41. *Let R be a Noetherian normal domain quotient of a Gorenstein ring and let $I \subset R$ be an ideal satisfying the following conditions:*
(i) *I is a reduced generically complete intersection of height ≥ 2.*
(ii) *$\mathrm{gr}_I(R)$ is R/I-torsion-free.*

Then the following assertions are equivalent:
(1) *$\mathcal{R}_R(I)$ is quasi-Gorenstein.*
(2) *R is quasi-Gorenstein and $\mathrm{ht}\, I = 2$.*

Here, *quasi-Gorenstein* means that the canonical ideal is principal. In particular, if R is regular then $\mathcal{R}_R(I)$ is (Cohen–Macaulay by the previous proposition and) Gorenstein if and only if $\mathrm{ht}\, I = 2$.

7.3.5.5 Generic ideals

For ideals of minors of generic matrices of various sorts, the situation is reasonably satisfactory.

Proposition 7.3.42 ([28, Theorem 7.7]). *Let $\mathcal{A}$ be an $r \times s$ generic matrix over a field of characteristic zero or sufficient positive characteristic, and let $I = I_t(\mathcal{A})$ be the ideal of t-minors, with $1 \leq t \leq \min\{r, s\}$. Then $\mathcal{R}_R(I)$ is a Cohen–Macaulay normal domain.*

Proposition 7.3.43 ([83], [71], [95], [39]). *Let R be a Noetherian domain and let $\mathcal{A}$ be an $r \times s (r \leq s)$ matrix over R.*
(i) *If $\mathcal{A}$ is generic and $I = I_{r-1}$, then $\mathcal{R}_R(I)$ is a Cohen–Macaulay normal domain.*
(ii) *If $r = s$ and $\mathcal{A}$ is symmetric generic and $I = I_{r-1}$, then $\mathcal{A}$ is a normal domain*
(iii) *If $\mathcal{A}$ is a generic Hankel matrix and $I = I_t$, for any t, then $\mathcal{R}_R(I)$ is a Cohen–Macaulay normal domain.*

Similar results have been proved for the Pfaffians of a skew-symmetric generic matrix ([13], [14]).

For some other kind of determinantal ideals, one has, for example:

Theorem 7.3.44. *Let $\mathcal{A}$ denote the generic $n \times m (n \leq m)$ matrix over a field and let $\mathcal{A}_r$ be an $n \times r$ submatrix of $\mathcal{A}$, where $1 \leq r \leq n-1$. Let J_r stand for the ideal of n-minors of $\mathcal{A}$ fixing $\mathcal{A}_r$. Then:*

(i) *J_r is an ideal of linear type if and only if $r = n-1$ or $m = n+l$.*

(ii) *Moreover, in either of the above cases, one has:*

  (a) *The Rees algebra $\mathcal{R}_R(J_r)$ is a Cohen–Macaulay normal domain.*

  (b) *$\mathrm{gr}_{J_r}(R)$ is Cohen–Macaulay and R/J_r-torsion-free.*

  (c) *J_r is normally torsion-free.*

These ideals have been considered in [76], [27], [81], [2, 3, 4] and [115].

7.3.6 Specialization

A basic specialization result was proved by Eisenbud–Huneke [54, 1.1] to the effect that the Rees algebra $\mathcal{R}(J) = S[Jt]$ of an ideal $J \subset S$ specializes to a Cohen–Macaulay Rees algebra provided both S and $\mathcal{R}(J)$ are Cohen–Macaulay and the local analytic spreads of J are reasonably bounded above. Some of this has been slightly improved by Kennedy–Simis–Ulrich in [94] having in mind applications to the deformation of star algebras.

Previously, in [70, Proposition 10.7] a similar result was obtained for the symmetric algebra $\mathcal{S}(J)$ of J replacing the bounds on the local analytic spreads of J by similar ones for the local numbers of generators of J—the case for the symmetric algebra is less admirable as the Cohen–Macaulayness of $\mathcal{S}(J)$ imposes rather strong restrictions on its dimension (*cf.* [70, Proposition 8.4]).

The next part will focus on some of the aspects of these ideas.

7.3.6.1 Abstract specialization

Let R denote a commutative ring and $J \subset R$ an ideal. The following lemmas are elementary.

Lemma 7.3.45. *Let R and J be as above. Let $\mathfrak{N} \subset R$ be an arbitrary ideal and set $I := (J, \mathfrak{N})/\mathfrak{N}$. Then*

$$\ker(\mathcal{R}(J) \otimes_R R/\mathfrak{N} \xrightarrow{\rho} \mathcal{R}(I)) = \sum_{l \geq 0} (\mathfrak{N} \cap J^l)/\mathfrak{N}J^l.$$

Proof. Since the homogeneous piece of degree l of $\mathcal{R}(J) \otimes_R R/\mathfrak{N}$ (resp., of $\mathcal{R}(I)$) is $J^l/\mathfrak{N}J^l$ (resp., $(J^l, \mathfrak{N})/\mathfrak{N} \simeq J^l/\mathfrak{N} \cap J^l$), the result is obvious. □

Lemma 7.3.46. *Same assumptions as in* Lemma 7.3.45. *If* $\operatorname{Tor}_1^R(\operatorname{gr}_J R, R/\mathfrak{N}) = 0$, *then* $\operatorname{Tor}_1^R(R/J^l, R/\mathfrak{N}) = 0$ *for all* $l \geq 0$.

Proof. Clearly, $\operatorname{Tor}_1^R(\operatorname{gr}_J R, R/\mathfrak{N}) = 0 \Leftrightarrow \operatorname{Tor}_1^R(J^l/J^{l+1}, R/\mathfrak{N}) = 0$ for all $l \geq 0$. Therefore, induction using the long exact sequences of Tor associated to the short exact sequences

$$0 \to J^l/J^{l+1} \to S/J^{l+1} \to S/J^l \to 0$$

will show the contention. □

Theorem 7.3.47 (Specialization of the Rees algebra). *Let* R *be a Noetherian ring, let* $J, \mathfrak{N} \subset R$ *be ideals such that, for every maximal ideal* $\mathfrak{m} \supseteq J + \mathfrak{N}$, *one has:*
(i) $\operatorname{gr}_{J_\mathfrak{m}} R_\mathfrak{m}$ *is Cohen–Macaulay;*
(ii) $\mathfrak{N}_\mathfrak{m}$ *is a perfect ideal.*

Setting $I := (J, \mathfrak{N})/\mathfrak{N}$, *the following conditions are equivalent:*
(a) $\mathcal{R}(J) \otimes_R R/\mathfrak{N} \overset{\rho}{\cong} \mathcal{R}(I)$.
(b) $\operatorname{gr}_J R \otimes_R R/\mathfrak{N} \overset{\bar{\rho}}{\cong} \operatorname{gr}_I R$.
(c) $\ell(J_P) \leq \dim R_\wp$ *for every* $P \in V(J, \mathfrak{N}) \subset \operatorname{Spec} R$, *where* $\wp = P/\mathfrak{N}$.
(d) $\ell(J_P) \leq \dim R_\wp$ *for every* $P \in V(J, \mathfrak{N}) \subset \operatorname{Spec} R$ *which is a contraction of a minimal prime of* $\operatorname{gr}_J R \otimes_R R/\mathfrak{N}$, *where* $\wp = P/\mathfrak{N}$.

If any of these conditions is satisfied, then $\operatorname{gr}_J R \otimes_R R/\mathfrak{N} \simeq \operatorname{gr}_I R$ *is Cohen–Macaulay.*

Proof. Set $S := R/\mathfrak{N}$.
(a) $\Rightarrow$ (b) Clear.
(b) $\Rightarrow$ (c) Since

$$\ell(J_P) = \dim \operatorname{gr}_J R \otimes_R R_P/P_P = \dim \operatorname{gr}_J R \otimes_R S_\wp/\wp_\wp$$

and

$$\ell(I_\wp) = \dim \operatorname{gr}_I S \otimes_S S_\wp/\wp_\wp,$$

the implication is obvious.
(c) $\Rightarrow$ (d) Obvious.
(d) $\Rightarrow$ (a) One may assume that R is a local ring. One first claims that

$$\operatorname{grade} \mathfrak{N} \operatorname{gr}_J R \geq \operatorname{grade} \mathfrak{N}. \tag{7.3.47.1}$$

Since $\operatorname{gr}_J R$ is a positively graded Cohen–Macaulay algebra over a local ring and taking in account the equality $\dim \operatorname{gr}_J R = \dim R$ and the general inequalities,

$$\dim S \leq \dim R - \operatorname{ht} \mathfrak{N} \leq \dim R - \operatorname{grade} \mathfrak{N},$$

inequality (7.3.47.1) is a consequence of the following one:

$$\dim \operatorname{gr}_J R \otimes_R S \leq \dim S. \tag{7.3.47.2}$$

To show the latter, consider a minimal prime Q of $\operatorname{gr}_J R \otimes_R S$ such that

$$\dim \operatorname{gr}_J R \otimes_R S = \dim(\operatorname{gr}_J R \otimes_R S)/Q$$

and let P be its contraction to R and $\wp = P/\mathfrak{N} \in \operatorname{Spec} S$. One has

$$\begin{aligned}
\dim \operatorname{gr}_J R \otimes_R S &= \dim(\operatorname{gr}_J R \otimes_R S)/Q \\
&\leq \dim S/\wp + \operatorname{trdeg}_{S/\wp}(\operatorname{gr}_J R \otimes_R S)/Q, \quad \text{by Corollary 2.5.38} \\
&= \dim S/\wp + \dim((\operatorname{gr}_J R \otimes_R S)/Q) \otimes_{S/\wp} S_\wp/\wp S_\wp \\
&= \dim S/\wp + \dim(\operatorname{gr}_J R \otimes_R S) \otimes_{S/\wp} S_\wp/\wp S_\wp \\
&= \dim S/\wp + \ell(J_P) \\
&\leq \dim S/\wp + \dim S_\wp \leq \dim S, \quad \text{by assumption.}
\end{aligned}$$

Thus, inequality (7.3.47.2) holds, and hence, so does (7.3.47.1). Now, since $\mathfrak{N}$ is perfect, the latter implies, by a well-known result (*cf.*, *e. g.*, [27, 3.5]) that $\operatorname{Tor}_i^R(\operatorname{gr}_J R, S) = 0$ for $i > 0$ and that $\operatorname{gr}_J R \otimes_R S$ is Cohen–Macaulay.

For the conclusion, one uses Lemma 7.3.46 and Lemma 7.3.45 and the fact that

$$\operatorname{Tor}_1^S(S/J^l, R) = \operatorname{Tor}_1^S(S/J^l, S/N) \simeq (N \cap J^l)/NJ^l.$$

This concludes the proof of the theorem. □

Remark 7.3.48. By the very proof of Theorem 7.3.47, any of the equivalent conditions stated there implies that the ideals N and J are *normally transversal*, *i. e.*, that $\operatorname{Tor}_i^S(S/J, S/N) = 0$ for $i > 0$.

In a sense, the next result deals with the other end of the spectrum, namely, that where $\mathfrak{N} \subset J$. It will require that $\mathfrak{N}$ be of the principal class locally everywhere.

Proposition 7.3.49. *Let R be a Noetherian ring and let $\mathfrak{N} \subset J$ be R-ideals. Set $S = R/\mathfrak{N}$, $I = J/\mathfrak{N}$ and $\overline{\mathfrak{N}} = (\mathfrak{N}, J^2)/J^2 \subset [\operatorname{gr}_J R]_1$ and assume that the following conditions hold:*

(i) $\mu(\mathfrak{N}_\mathfrak{m}) = \operatorname{ht} \mathfrak{N}_\mathfrak{m}$ *for every maximal ideal* $\mathfrak{m} \supseteq J$.

(ii) $\operatorname{gr}_{J_\mathfrak{m}} S_\mathfrak{m}$ *is Cohen–Macaulay for every maximal ideal* $\mathfrak{m} \supseteq J$.

(iii) $\mu(I_\wp) \leq \dim S_\wp$ *for every prime ideal* $P \supseteq J$, *where* $\wp = P \cap S$.

Then:

(a) $R[Jt]/(\mathfrak{N}, \mathfrak{N}t) \simeq \mathcal{S}(I)$.

(b) $\operatorname{gr}_J R/(\overline{\mathfrak{N}}) \simeq \operatorname{gr}_I S$.

(c) $\operatorname{gr}_I S$ *is Cohen–Macaulay.*

Proof. (b) clearly follows from (a). As for (a) and (c), one may assume that R is local and that $\mathfrak{N} = (x)$ with $\operatorname{ht}\mathfrak{N} = 1$. One may also assume that $\operatorname{grade} J > 0$. One claims that $\overline{x} \in [\operatorname{gr}_J R]_1$ is actually a nonzero divisor, in which case both assertions are clear.

Now, the surjection $R_{R/J}(J/J^2) \to \operatorname{gr}_J R$ induces a surjection

$$\mathcal{R}_{S/I}(I/I^2) \simeq \mathcal{R}_{R/J}(J/J^2)/(\overline{x}) \to \operatorname{gr}_J R/(\overline{x}).$$

Therefore,

$$\begin{aligned}\dim \operatorname{gr}_J R/(\overline{x}) &\le \dim \mathcal{R}_{S/I}(I/I^2)\\ &\le \dim S, && \text{by condition (iii), } \textit{cf.}\ [82]\\ &= \dim \operatorname{gr}_J R - 1, && \text{since } \operatorname{grade} J > 0 \text{ and } \dim R = \dim S + 1.\end{aligned}$$

Since $\operatorname{gr}_J R$ is Cohen–Macaulay, $\overline{x}$ must be a nonzero divisor. □

Observe that, as in the proof of Theorem 7.3.47, in the last proposition, too, the main point was to show that $\operatorname{ht}\mathfrak{N}\operatorname{gr}_J R \ge \operatorname{ht}\mathfrak{N}$. Condition (iii) is in a sense a cheap way out.

7.3.6.2 Classical specialization

Here, one assumes a more particular case of specialization, following the classical procedure of specializing variables of a ground polynomial ring. Let A denote a Noetherian ring of finite Krull dimension—in the applications it will mostly be the ground ring of variables to be specialized—and let R denote a finitely generated A-algebra. Let $\mathfrak{n} \subset A$ denote a maximal ideal such that the extended ideal $\mathfrak{n}R$ is prime, and $\mathcal{I} \subset R$ any ideal not contained in $\mathfrak{n}R$. Set $I := (\mathcal{I}, \mathfrak{n})/\mathfrak{n}R$ and $k := A/\mathfrak{n}$.

Proposition 7.3.50. *Consider the specialization homomorphism*

$$\mathfrak{s} : \mathcal{R}_R(\mathcal{I}) \otimes_A k \twoheadrightarrow \mathcal{R}_{R/\mathfrak{n}R}(I).$$

Then:

(1) $\ker(\mathfrak{s})$ *is a minimal prime ideal of* $\mathcal{R}_R(\mathcal{I}) \otimes_A k$ *and, for any minimal prime* $\mathfrak{Q}$ *of* $\mathcal{R}_R(\mathcal{I}) \otimes_A k$ *other than* $\ker(\mathfrak{s})$*, one has that* $\mathfrak{Q}$ *corresponds to a minimal prime of* $\operatorname{gr}_{\mathcal{I}}(R) \otimes_A k \simeq (\mathcal{R}_R(\mathcal{I}) \otimes_A k)/\mathcal{I}(\mathcal{R}_R(\mathcal{I}) \otimes_A k)$ *and so*

$$\dim\big((\mathcal{R}_R(\mathcal{I}) \otimes_A k)/\mathfrak{Q}\big) \le \dim\big(\operatorname{gr}_{\mathcal{I}}(R) \otimes_A k\big).$$

In particular,

$$\dim\big(\mathcal{R}_R(\mathcal{I}) \otimes_A k\big) = \max\{\dim(R/\mathfrak{n}R) + 1, \dim\big(\operatorname{gr}_{\mathcal{I}}(R) \otimes_A k\big)\}$$

(2) *Let* $t \ge 0$ *be an integer such that* $\ell(\mathcal{I}_{\mathfrak{P}}) \le \operatorname{ht}(\mathfrak{P}/\mathfrak{n}R) + t$ *for every prime ideal* $\mathfrak{P} \in \operatorname{Spec}(R)$ *containing* $(\mathcal{I}, \mathfrak{n})$*. Then*

$$\dim\big(\operatorname{gr}_{\mathcal{I}}(R) \otimes_A k\big) \le \dim(R/\mathfrak{n}R) + t.$$

(3) $\dim(\ker(\mathfrak{s})) \le \dim\big(\operatorname{gr}_{\mathcal{I}}(R) \otimes_A k\big)$.

Proof. (1) Let $P \in \operatorname{Spec}(R)$ be a prime ideal not containing $\mathcal{I}$. Localizing the surjection $\mathfrak{s} : \mathcal{R}_R(\mathcal{I}) \otimes_A k \twoheadrightarrow \mathcal{R}_{R/\mathfrak{n}R}(I)$ at $R \setminus P$, one easily sees that it becomes an isomorphism. It follows that some power of $\mathcal{I}$ annihilates $\ker(\mathfrak{s})$, *i. e.*,

$$\mathcal{I}^l \cdot \ker(\mathfrak{s}) = 0 \tag{7.3.50.1}$$

for some $l > 0$. Since $I \neq 0$, then $\mathcal{I} \nsubseteq \ker(\mathfrak{s})$. Thus, any minimal prime ideal of $\mathcal{R}_R(\mathcal{I}) \otimes_A k$ contains either the prime ideal $\ker(\mathfrak{s})$ or the ideal $\mathcal{I}$. Thus, $\ker(\mathfrak{s})$ is a minimal prime and any other minimal prime $\mathfrak{Q}$ of $\mathcal{R}_R(\mathcal{I}) \otimes_A k$ contains $\mathcal{I}$. Clearly, then any such $\mathfrak{Q}$ is a minimal prime of $(\mathcal{R}_R(\mathcal{I}) \otimes_A k)/\mathcal{I}(\mathcal{R}_R(\mathcal{I}) \otimes_A k) \simeq \operatorname{gr}_{\mathcal{I}}(R) \otimes_A k$. Since $\dim(\mathcal{R}_{R/\mathfrak{n}R}(I)) = \dim(R/\mathfrak{n}R) + 1$, the claim follows.

(2) For this, let $\mathfrak{M}$ be a minimal prime of $\operatorname{gr}_{\mathcal{I}}(R) \otimes_A k$ of maximal dimension, *i. e.*,

$$\dim(\operatorname{gr}_{\mathcal{I}}(R) \otimes_A k) = \dim((\operatorname{gr}_{\mathcal{I}}(R) \otimes_A k)/\mathfrak{M}),$$

and let $\mathfrak{P} = \mathfrak{M} \cap R$ be its contraction to R. Clearly, $\mathfrak{P} \supseteq (\mathcal{I}, \mathfrak{n})$. By [141, Lemma 1.1.2] and the hypothesis,

$$\begin{aligned}
\dim(\operatorname{gr}_{\mathcal{I}}(R) \otimes_A k) &= \dim((\operatorname{gr}_{\mathcal{I}}(R) \otimes_A k)/\mathfrak{M}) \\
&= \dim(R/\mathfrak{P}) + \operatorname{trdeg}_{R/\mathfrak{P}}((\operatorname{gr}_{\mathcal{I}}(R) \otimes_A k)/\mathfrak{M}) \\
&= \dim(R/\mathfrak{P}) + \dim(((\operatorname{gr}_{\mathcal{I}}(R) \otimes_A k)/\mathfrak{M}) \otimes_{R/\mathfrak{P}} R_{\mathfrak{P}}/\mathfrak{P}R_{\mathfrak{P}}) \\
&\leq \dim(R/\mathfrak{P}) + \dim(\operatorname{gr}_{\mathcal{I}}(R) \otimes_R R_{\mathfrak{P}}/\mathfrak{P}R_{\mathfrak{P}}) \\
&= \dim(R/\mathfrak{P}) + \ell(\mathcal{I}_{\mathfrak{P}}) \\
&\leq \dim(R/\mathfrak{P}) + \operatorname{ht}(\mathfrak{P}/\mathfrak{n}) + t \\
&\leq \dim(R/\mathfrak{n}R) + t,
\end{aligned}$$

as required.

The supplementary assertion on $\dim(\mathcal{R}_R(\mathcal{I}) \otimes_A k)$ is now clear.

(3) From (7.3.50.1), one has $\operatorname{ann}_{\mathcal{R}_R(\mathcal{I}) \otimes_A k}(\ker(\mathfrak{s})) \supseteq \mathcal{I}^l$. Therefore,

$$\dim(\ker(\mathfrak{s})) \leq \dim((\mathcal{R}_R(\mathcal{I}) \otimes_A k)/\mathcal{I}(\mathcal{R}_R(\mathcal{I}) \otimes_A k))$$

and so the result follows. □

The technique developed in this section has applications to the specialization of the so-called tangent star cone ([94]) and the degree of rational maps and fiber cones ([35]). The details are outside the scope of this book.

7.4 Hilbert function of modules

The goal of this chapter is to reproduce the original notion of Hilbert function as given in Section 2.7 within a more encompassing framework. As for many functions in arith-

metic, one can associate to it a generating function. This much could have been developed in the referred section, but in the environment to be assumed here it takes a fully central role. One issue however remains unchanged, and that is the need to have at some point vector spaces of finite dimension or modules with finite length, since after all one wishes to deal with an arithmetic function with nonnegative integer values.

As is routine these days, one considers two situations, one graded, the other local. No matter how general one wishes to assume, these are the two basic cases in use. A good deal of the theory has a combinatorial side to it. Some of the required tools will be reviewed in the first subsection below.

7.4.1 Combinatorial preliminaries

A standing reference for this part is [147].

The interest here lies in the set of functions $\mathbb{Z} \to \mathbb{Z}$, which has a structure of an Abelian group $\mathfrak{Z}$ under the natural addition of functions. Now, a polynomial $p = p(X) \in \mathbb{Q}[X]$ induces a function $\mathbb{Q} \to \mathbb{Q}$ by evaluation and, since $\mathbb{Q}$ is infinite, can be identified with the latter. One is interested in the subset of those p such that $p(n) \in \mathbb{Z}$ for every $n \in \mathbb{Z}$. This set, identified with the corresponding subset of functions from $\mathbb{Z}$ to $\mathbb{Z}$, is a subgroup $\mathfrak{Q} \subset \mathfrak{Z}$. Its elements will be called polynomial functions—always keeping in mind that as polynomials they have rational coefficients.

The focus will be on the nongroup theoretic equivalence relation that identifies two functions $f, g : \mathbb{Z} \to \mathbb{Z}$ provided $f(n) = g(n)$ for all $n \gg 0$. The elements of $\mathfrak{Z}$ that belong to $\mathfrak{Q}$ up to this equivalence relation are very interesting; the Hilbert function will be one such, as one will see.

The (first) *difference operator* is the endomorphism Δ of $\mathfrak{Z}$ such that $\Delta(f)(n) = f(n+1) - f(n)$, for $f \in \mathfrak{Z}$ and $n \in \mathbb{Z}$. For $l \geq 1$, the lth iterated Δ^l of δ is naturally defined by $\Delta^l = \Delta(\Delta^{l-1})$, while Δ^0 is defined by $\Delta^0(f) = f$, for every $f \in \mathfrak{Z}$.

The reason to understand $\mathfrak{Z}$ in terms of its subgroup $\mathfrak{Q}$ is that the latter has a very simple structure.

Proposition 7.4.1. *With the above notation, one has:*

(a) (Polya, Ostrowski) *Let* $\binom{X}{i}$ *denote the polynomial function* $n \mapsto \binom{n}{i}$. *Then* $\mathfrak{Q}$ *is the free Abelian subgroup with basis the set* $\{\binom{X}{i} \mid i = 0, 1, \ldots\}$.

(b) *The following conditions are equivalent for an element* $f \in \mathfrak{Z}$*:*
   (i) f *is a polynomial function of degree* $\leq d$
   (ii) *There exists an integer* $d \geq 1$ *such that* $\Delta^{d+1} f(n) = 0$ *for all* $n \in \mathbb{Z}$.

Proof. (a) It suffices to prove that any element of $\mathfrak{Q}$ associated with a polynomial $p \in \mathbb{Q}[X]$ of degree d is a uniquely determined $\mathbb{Z}$-linear combination of $\{\binom{X}{i} \mid i = 0, \ldots, d\}$. Now, it is well known that $\{\binom{X}{i} \mid i = 0, 1, \ldots\}$ is a basis of the $\mathbb{Q}$-vector space $\mathbb{Q}[X]$.

Therefore, p has a unique representation as a $\mathbb{Q}$-linear combination thereof with rational coefficients. Thus, it suffices to show that these coefficients are integers. Say,

$$p = p(X) = a_0\binom{X}{0} + \cdots a_d\binom{X}{d}, \tag{7.4.1.1}$$

with $a_i \in \mathbb{Q}$.

On the other hand, one has the following relation, which is proved by induction on the order of the iterated difference operator:

$$\Delta^l f(n) = \sum_{i=0}^{l} (-1)^{l-i}\binom{l}{i} f(n+i), \tag{7.4.1.2}$$

for any $l \geq 1$ and any $n \in \mathbb{Z}$. Applying this relation iteratively to the left side of (7.4.1.1), with $n = 0$, yields that $a_i = \Delta^i p(0)$, for every i.

(b) The implication (i) $\Rightarrow$ (ii) is clear since the difference operator decreases the degree of the associated polynomial one unit at the time.

For the reverse implication, one may use relation (7.4.1.2). Since, by assumption, the left side vanishes with $l = d+1$ then $f(n)$ turns out to be a $\mathbb{Z}$-linear combination of the set $\{\binom{n}{i} \mid i = 0, \ldots, d\}$. As n is arbitrary, part (a) implies that $f \in \mathfrak{Q}$ and as such has degree at most d. □

As mentioned above, one considers the equivalence relation in $\mathfrak{Z}$ that identifies two functions if they are asymptotically equal. In this regard, having acquired sufficient familiarity with the above combinatorial steps, the reader can now show that the equivalence of items (i) and (ii) in the above proposition apply as well modulo asymptotically equivalence. Namely, we have the following.

Proposition 7.4.2. *A function $f \in \mathfrak{Z}$ is* asymptotically polynomial, *i. e., its values coincide with the values $p(n)$ of some polynomial $p \in \mathfrak{Q}$ for $n \gg 0$—if and only if there are integers $d \geq 0$ and n_0 such that $\Delta^{d+1} f(n) = 0$ and $\Delta^d f(n) \neq 0$ for every $n \geq n_0$. In this case, d is then exactly the degree of p.*

Note that if $f \in \mathfrak{Z}$ is asymptotically polynomial, there is a uniquely defined polynomial that gives $f(n)$ for all $n \gg 0$. This is because, two polynomial functions are asymptotically equivalent if and only if they coincide.

Next, one briefly discusses the related generating functions. Let $f \in \mathfrak{Z}$ have the property that $f(n) = 0$ for all $n \ll 0$. Recall that the *generating function* of such an f is the Laurent power series $\sum_{n\in\mathbb{Z}} f(n)t^n$, where t is an indeterminate. The question as to when such a series is *rational* is pervasive both in combinatorics as in algebra. Here, by rational one means an element $P(t, t^{-1})/Q(t) \in \mathbb{Z}(t)$, with $P(t, t^{-1}) \in \mathbb{Z}[t, t^{-1}]$ and $Q(t) \in \mathbb{Z}[t]$. Note that $\mathbb{Z}[t, t^{-1}] \simeq \mathbb{Z}[t, u]/(tu - 1)$, hence evaluating $P(t, t^{-1})$ at $1 \in \mathbb{Z}$ makes sense; for this reason, one writes simply $P(1)$ for the result of such evaluation. Also, by the degree of such a Laurent polynomial one means its positive degree.

It is a classical result that the generating function of a polynomial function $f \in \mathfrak{Q}$ is rational. It should not be a surprise that the same is true of an asymptotically polynomial function. The content is pretty much the same as [147, Corollary 4.3.1].

Proposition 7.4.3. *Let $f \in \mathfrak{Z}$ have the property that $f(n) = 0$ for all $n \ll 0$. The following conditions are equivalent:*

(i) *f is asymptotically polynomial of degree $\leq d$.*

(ii) *The generating function of f has the form $P(t, t^{-1})/(1-t)^{d+1}$, where $P(t, t^{-1})$ is a Laurent polynomial.*

Moreover, if any of these conditions holds then:

(a) *The degree of the asymptotic polynomial is d if and only if $P(1) \neq 0$.*

(b) *If $P(1) \neq 0$, the leading term of the asymptotic polynomial in $\mathbb{Q}[X]$ is $P(1)/d!$.*

Proof. (i) $\Rightarrow$ (ii) Let $n_0 \leq 0$ be the least integer such that $f(n_0) \neq 0$. Then

$$\begin{aligned}(1-t)\sum_{n\geq n_0} f(n)t^n &= f(n_0)t^{n_0} - f(n_0)t^{n_0+1} + \cdots + f(n_0+i)t^{n_0+i} - f(n_0+i)t^{n_0+i+1} + \cdots \\ &= f(n_0)t^{n_0} + \cdots + \big(f(n_0+i+1) - f(n_0+i)\big)t^{n_0+i+1} + \cdots \\ &= \Delta f(n_0-1)t^{n_0} + \Delta f(n_0)t^{n_0+1} + \cdots + \Delta f(n_0+i)t^{n_0+i+1} + \cdots \\ &= \sum_{n\geq n_0} \Delta f(n-1)t^n.\end{aligned}$$

By iteration, one gets similarly $(1-t)^l \sum_{n\geq n_0} f(n)t^n = \sum_{n\geq n_0} \Delta^l f(n-l)t^n$, for any $l \geq 1$. Since f is assumed to be asymptotically polynomial of degree $\leq d$, the coefficient $\Delta^{d+1} f(n-d-1)$ on the right-hand side of this equality as applied with $l = d+1$ vanishes for $n \gg 0$. Therefore, the left-hand side vanishes for $n \gg 0$, hence as a function of n it is a Laurent polynomial by Proposition 7.4.2.

(ii) $\Rightarrow$ (i) Conversely, if $\sum_{n\geq n_0} \Delta^{d+1} f(n-d-1)t^n$ is a Laurent polynomial then $\Delta^{d+1} f(n-d-1) = 0$ for $n \gg 0$. Then Proposition 7.4.2 implies that f is asymptotically polynomial of degree at most d.

(a) Suppose that $P(1) = 0$. Then P is a multiple of $1-t$ in $\mathbb{Z}[t, t^{-1}]$. Dividing numerator and denominator by $1-t$ one finds a rational form for the generating function of f where the term $\Delta^d f(n-d)$ on the right hand-side of $(1-t)^d \sum_{n\geq n_0} f(n)t^n$ vanishes for $n \gg 0$. Therefore, Proposition 7.4.2 implies that f is asymptotically polynomial of degree $\leq d_1$.

The converse is similar.

(b) Let $\partial = \partial_t$ denotes the ordinary t-derivative and ∂^i its ith iterated. One observes that Proposition 7.4.1 (a) holds true with $\{\binom{X+i}{i} \mid i = 0, 1, \ldots\}$ instead, since the transition matrices between the two bases have integer entries.

The contention follows from the following more general result.

Proposition 7.4.4. *With $P \in \mathbb{Z}[t, t^{-1}]$ as above, one has*

$$\sum_{n\geq 0} p(n)t^n = \sum_{i=0}^{d} \frac{(-1)^i}{i!} \frac{(\partial^i P)_{|t=1}}{(1-t)^{d-i+1}}.$$

As a consequence, if p is written in the basis $\{\binom{X+i}{i} \mid i = 0, \dots, d\}$, say

$$p = p(X) = \sum_{i=0}^{d} (-1)^{d-i} e_{d-i} \binom{X+i}{i},$$

then $e_i = \frac{1}{i!}(\partial^i P)_{|t=1}$, for $0 \leq i \leq d$.

Proof. Clearly, $\sum_{i=0}^{d} \frac{(-1)^i}{i!}(\partial^i P)_{|t=1}(1-t)^i$ is the Taylor expansion of P about 1 up to degree d. Dividing each coefficient of the latter by $(1-t)^{d+1}$ shows that the coefficients of the generating function of f for $n \gg 0$ coincide with those of the right-hand side of the proposed equality. However, in both sides the coefficients are given by polynomial functions, hence must coincide throughout. Therefore, one can replace the generating function of f by that of p, showing the equality.

Next, expanding the right-hand side as a power series in t gives

$$\sum_{n\geq 0} \left(\sum_{i=0}^{d} \frac{(-1)^i}{i!} (\partial^i P)_{|t=1} \binom{n+d-i}{d-i} \right) t^n.$$

Identifying coefficients on both sides yields finally

$$p(X) = \sum_{i=0}^{d} \frac{(-1)^i}{i!} (\partial^i P)_{|t=1} \binom{X+d-i}{d-i},$$

as required. □

Back to the proof of (b), the leading term of p is $(\partial^0 P)_{|t=1}/d! = P(1)/d!$, as was to be shown. □

7.4.2 The graded Hilbert function

This is the case where one aims at an enlargement of the setup in Section 2.7. Namely, one needs the extended notions of graded structures, as discussed in the beginning of Chapter 7.

The basic sine qua non result is the following elementary observation.

Lemma 7.4.5. *Let A stand for a commutative ring and let R denote an $\mathbb{N}$-graded finitely generated A-algebra, with $R_0 = A$. Let M denote a finitely generated $\mathbb{Z}$-graded R-module. Then every homogeneous part of M is a finitely generated A-module.*

Proof. Since R is graded, one can assume that it is generated by a set $\{f_1, \dots, f_r\}$ of homogeneous elements of degrees, say, $d_1 \leq \cdots \leq d_r$. Consider the $\mathbb{N}$-graded polynomial ring $A[x_1, \dots, x_r]$, where $\deg(x_i) = d_i$. Consider the surjective homomorphism of A-algebras $A[x_1, \dots, x_r] \twoheadrightarrow R$ such that $x_i \mapsto f_i$, for $i = 1, \dots, r$. Since this way the grading of R is induced by that of $A[x_1, \dots, x_r]$, one may assume that $R = A[x_1, \dots, x_r]$. In this case, the result follows by an obvious reasoning from the analogous one for a standard polynomial ring.

This takes care of the case where $M = R$. For the general case, M is the image of a graded R-module homomorphism with source a direct sum of finitely many copies of R or R shifted by some degree. Therefore, the result follows from the previous case. □

In particular, if the ground ring A is Artinian, every homogeneous part of M has finite length. This is the base for the following concept.

Definition 7.4.6. Let $(A, \mathfrak{n})$ be an Artinian local ring and let R denote an $\mathbb{N}$-graded finitely generated A-algebra, with $R_0 = A$. Given a finitely generated $\mathbb{Z}$-graded R-module M, the *Hilbert function* of M is the function

$$H(M, \_) : \mathbb{Z} \to \mathbb{Z}, \quad H(M, n) = \lambda(M_n),$$

where λ denotes length as an A-module.

The *Hilbert series* of M is the generating function of $H(M, \_)$. It will be denoted $H_M(t)$.

Remark 7.4.7. The classical Hilbert function was defined over a ground field. The relevance of upgrading from a field to an Artinian local ring will be clear in the next subsection.

The main basic result is the following.

Theorem 7.4.8 (Hilbert polynomial for modules). *With the notation of* Definition 7.4.6, *assume in addition that the* $\mathbb{N}$*-grading of* R *is standard. Set* $\dim M = d + 1$, *with* $d \geq -1$. *Then*

(a) $H(M, \_)$ *is asymptotically polynomial of degree* d.
(b) $H_M(t) = P(t, t^{-1})/(1-t)^{d+1}$, *where* $P \in \mathbb{Z}[t, t^{-1}]$.
(c) *The leading term of the asymptotic polynomial in* (a) *is* $P(1)/d!$.

Proof. (b) and (c) are immediate consequences of (a) via Proposition 7.4.3.

To prove (a), one first gives an argument in the case where $M = R/\wp$, with $\wp \subset R$ a homogeneous prime ideal, to which the general case will be reduced by taking a well-known filtration method (Proposition 5.2.8 (a)). Note that if A were actually a field, by writing R as a residue ring of a standard polynomial ring over A, the result would follow in this case from Theorem 2.7.17.

Anyway, to argue for this particular case, one inducts on $\dim R/\wp$. If $\dim R/\wp = 0$, then $\wp = (\mathfrak{n}, R_+)$, hence $R/\wp \simeq A/\mathfrak{n}$. Clearly, its graded pieces of positive degree are null.

Let $\dim R/\wp > 0$. Since R is standard, there exists some $a \in R_1 \setminus \wp$. This gives the exact sequence of graded R-modules

$$0 \to R/\wp(-1) \xrightarrow{\cdot a} R/\wp \longrightarrow R/(\wp, a) \to 0.$$

Applying the difference operator of the previous subsection yields

$$\Delta H(R/\wp, n) = H(R/(\wp, a), n+1).$$

(Note the parallel with Proposition 2.7.15.) Since $\dim R/(\wp, a) = \dim(R/\wp) - 1$, the inductive assumption then implies that $\Delta H(R/\wp, n)$ is asymptotically polynomial of degree $\dim(R/\wp) - 2 = d + 1 - 2 = d - 1$.

If $d > 0$, then Proposition 7.4.2 implies that $\Delta^d H(R/\wp, n) = \Delta^{d-1}(\Delta H(R/\wp, n))$ is a nonzero constant for all $n \gg 0$, hence $H(R/\wp, n)$ is asymptotically polynomial of degree d.

If $d = 0$, then $\Delta^0 H(R/\wp, n) = H(R/\wp, n) = H(R/\wp, 0)$ for $n \gg 0$ by the above exact sequence and since $H(R/(\wp, a), R/(\wp, a)i) = 0$ for $i \gg 0$ as $\dim R/(\wp, a) = 0$. But, $H(R/\wp, 0) \neq 0$, hence $\Delta^d H(R/\wp, n)$ is a nonzero constant for $n \gg 0$ in this case, too.

This takes care of the case of a cyclic R-module with a prime annihilator. For the general case, one applies the result of Proposition 5.2.8 (a), with a slight modification. Namely, one can take the submodules of the filtration to be also graded and the successive quotients to be cyclic R-modules with homogeneous prime annihilators, shifted by some degree.

The following easy additional steps are left to the reader:

(1) The dimension of M is the maximum of the dimensions of the cyclic modules obtained in the above graded filtration.

(2) The Hilbert function is additive on exact sequences of graded R-modules (as a consequence of the same property of the length (Section 3.1.2)). □

Remark 7.4.9.

(1) Most proofs of item (a) above are a variation on the original argument of Serre's ([138, Chapitre II (B)]) by induction on the number of a finite set of generators of R over A, or, similarly, on the dimension of a polynomial ring presenting R. The above proof, lifted from [68, Theorem 7.5, Chapter I, Section 7], appeals to an induction on the dimension of the given module and seems more naturally attached to the combinatorial preliminaries developed before. All proofs known to this author appeal in one way or another to the action of the difference operator Δ, through some version of Proposition 7.4.2. Since the typical use of this operator is by taking its iterates, this explains the need of induction in the proofs of (a).

(2) The proof that the Hilbert function is asymptotically polynomial when the ground ring is Artinian local A can be deduced from the same statement over a ground field. For this, one argues by induction of the length of A (see [133, Chapitre II, Section 3]).

The asymptotic polynomial in item (a) of the theorem is called the *Hilbert polynomial* of M. One notes that for $d = -1$ (*i. e.*, $\dim M = 0$), the assertions (a) through (c) of the theorem are not very meaningful since the Hilbert polynomial is the zero polynomial. For $d \geq 0$, one sets $e(M) := P(1)$. If $\dim M = 0$, one sets $e(M) = \lambda(M)$.

Definition 7.4.10. The number $e(M)$ is called the *multiplicity* of M.

By Theorem 7.4.8, $e(M)$ is the numerator of the leading term, with positive denominator, of the corresponding asymptotic polynomial. Since the values of the latter coincide with the respective values of the Hilbert function of M for $n \gg 0$, it follows that $e(M) \geq 0$. This is a déja vu of the multiplicity in the case where the ring R is a standard polynomial ring over a field (Definition 2.7.19).

The multiplicity of M is often called the *degree* of M (not to be confused with any single degree of M in its grading). The reason for doing so is that, in the case where M is the homogeneous coordinate ring of a projectively embedded algebraic variety $V \subset \mathbb{P}^r$, $e(M)$ coincides with the geometric degree of V in this embedding. Another apparent explanation for this terminology option is that the notion of multiplicity is classically assigned to a local situation—as will be seen in the next subsection.

The main way to compute the Hilbert function as devised by Hilbert himself was through the use of graded free resolutions. The idea has both theoretical as computational interest.

Proposition 7.4.11. *Suppose that the finitely generated graded R-module M has finite homological dimension and let*

$$0 \to \bigoplus_s R(-s)^{\beta_{p,s}} \longrightarrow \cdots \longrightarrow \bigoplus_s R(-s)^{\beta_{0,s}} \longrightarrow M \to 0$$

stand for a finite graded resolution of M. Then $H_M(t) = B_M(t)H_R(t)$, where $B_M(t) = \sum_{i,s}(-1)^i\beta_{i,s}t^s$.

Proof. By a previous remark in the proof of Theorem 7.4.8, the Hilbert function is additive on short (homogeneous) exact sequences of graded modules. Therefore, so is the Hilbert series, which as applied to the short exact sequences from the given free resolution yields $H_M(t) = \sum_{i,s}(-1)^i\beta_{i,s}H_{R(-s)}(t)$. □

In general, it is not easy to extract a formula for the multiplicity of M out of the above equality, because one has to deal with the Hilbert function of the graded ring R itself. The case of a polynomial ring is within reach.

Corollary 7.4.12. *Let $R = k[x_0, \dots, x_n]$, a polynomial ring over a field, and let M stand for a finitely generated graded R-module of dimension $d+1$. Then*

$$e(M) = \frac{(-1)^{n-d}}{(n-d)!} \frac{\partial^{n-d} B_M(t)}{\partial t^{n-d}}(1).$$

Proof. The formula follows from the equality $B_M(t) = (1-t)^{n-d}P(t)$, where $P(t)$ denotes the numerator in the reduced rational form of $H_M(t)$. As to this equality, it follows immediately from the one in the above proposition by observing that $H_R(t) = 1/(1-t)^n$. □

7.4.2.1 Selecta

The formula of van der Waerden (Theorem 2.7.25) for the multiplicity of cyclic modules over a polynomial ring now fully extends to the present general situation, where it is called perhaps improperly the (*graded*) *associativity formula*. One goes back to the general setup of Definition 7.4.6.

Proposition 7.4.13. *Let M denote a finitely generated graded R-module. Then*

$$e(M) = \sum_{\wp} \lambda(M_\wp) e(R/\wp),$$

where $\wp$ runs through the minimal primes of M of maximal dimension.

Proof. The basic strategy comes from the following additivity behavior of the multiplicity along an exact sequence.

Claim. Let $0 \to N' \longrightarrow N \longrightarrow N'' \to 0$ stand for a homogeneous exact sequence of finitely generated graded R-modules. Then

$$e(N) = \begin{cases} e(N') + e(N'') & \text{if } \dim N = \dim N' = \dim N'' \\ e(N') & \text{if } \dim N'' < \dim N \\ e(N'') & \text{if } \dim N' < \dim N \end{cases} \tag{7.4.13.1}$$

To see the claim, recall that the Hilbert function is additive on short exact sequences as the one given. Taking $n \gg 0$, one gets an exact sequence of the values of the respective Hilbert polynomials. Since their degrees are the respective dimensions of the terms, the appended leading coefficients are either incomparable or equal. Since, according to Proposition 5.2.6(vii), the only alternatives for the dimensions along the exact sequence are the ones stated in the claim, the alternatives for the respective multiplicities are as stated.

Now, one considers a filtration of the module M as in the proof of Theorem 7.4.8, namely, one can take the submodules of the filtration to be also graded and the successive quotients to be cyclic R-modules with homogeneous prime annihilators, shifted by some degree. Say, $\{0\} \subset M_1 \subset M_2 \subset \cdots \subset M_s = M$, where $M_{i+1}/M_i \simeq R/\wp_i$ (up to a

shift), with $\wp_i$ a homogeneous prime ideal. In particular, as pointed out in the proof of Theorem 7.4.8, one has $\dim M = \max_i\{\dim R/\wp_i\}$. Applying the claim successively, one arrives at the following formula:

$$e(M) = \sum_{\wp} e(R/\wp),$$

where $\wp$ runs through the minimal primes of M of maximal dimension that appear in the above filtration.

Clearly, for every such prime $\wp$, the residue ring $R/\wp$ appears in the short exact sequences $0 \to M_i \longrightarrow M_{i+1} \longrightarrow R/\wp_i \to 0$ a certain number of times. To count this number, one localizes M at $\wp$ and considers a composition series of $M_\wp$ (note that $\dim M_\wp = 0$). Then the composition factors are localizations of global factors of the filtration, hence are all isomorphic to the localization $R_\wp/\wp_\wp$. Therefore, the number of appearances of $\wp$ in the filtration is $\lambda(M_\wp)$. □

In Section 2.7, one saw the interest of having a closer look at the nature of the coefficients of the polynomial P. It has been seen that in the case of a graded cyclic module with prime annihilator, in a standard polynomial ring R, the *sum* of the coefficients of P from the second one is a nonnegative number. The question naturally arises as to the behavior of these individual coefficients. In one important case, one has a much stronger result.

Proposition 7.4.14. *If M is a Cohen–Macaulay module, then the coefficients of the numerator of the Hilbert series of M are nonnegative.*

Proof. One will assume that the residue field of the Artinian ring $A = R_0$ is infinite—this is a minor restriction that can always be lifted by changing all data via the inclusion $A \subset A[Y]_{\mathfrak{n}A[Y]}$, with Y an indeterminate.

One inducts on $\dim M$. For $\dim M = 0$, the Hilbert series is polynomial, hence the result is obvious.

If $\dim M \geq 1$, since M is Cohen–Macaulay and the residue field of A is infinite, one can choose a 1-form $\ell \in R$ which is regular on M. Then $M/\ell M$ is Cohen–Macaulay of dimension $\dim M - 1$. The exact sequence

$$0 \to M(-1) \xrightarrow{\ell} M \longrightarrow M/\ell M \to 0$$

implies the relation $(1-t)H_M(t) = H_{M/\ell M}(t)$ between the respective Hilbert series, hence the equality of the respective numerators. Therefore, the inductive assumption takes care of the result. □

Let $R = k[x_0, \ldots, x_n]$ denote a standard graded polynomial ring over a field. Fixing an integer $s \geq 1$, the k-subalgebra $R^{(s)} := k[R_s] \subset R$ is often called the sth *Veronesean subalgebra* of R. If M is a $\mathbb{Z}$-graded R-module, with $M_n = 0$ for all $n \ll 0$, then $M^{(s)} := \bigoplus_{n\in\mathbb{Z}} M_{ns}$ is naturally a graded module over $R^{(s)}$.

Proposition 7.4.15. *One has* $e(M^{(s)}) = s^d e(M)$, *where* $\dim M = d + 1$.

Proof. Since $R^{(s)}$ is generated in the same degree s, one may rescale its grading so as to have it standard. Then the Hilbert series of $M^{(s)}$ becomes

$$H_{M^{(s)}}(t^s) = P_{M^{(s)}}(t^s)/(1-t^s)^{d+1}.$$

Now use the following basic result about the roots of unit η of order s: for any given integer m

$$\sum_{\eta^s=1} \eta^m = \begin{cases} 1 & \text{if } m|s \\ 0 & \text{otherwise} \end{cases}$$

Then

$$H_{M^{(s)}}(t^s) = \frac{1}{s}\sum_{\eta^s=1} H_M(\eta t) = \frac{1}{s}\sum_{\eta^s=1} \frac{P_M(\eta t)}{(1-\eta t)^{d+1}}.$$

Comparison yields

$$\begin{aligned} P_{M^{(s)}}(t^s) &= \frac{1}{s}\sum_{\eta^s=1} \frac{(1-t^s)^{d+1}}{(1-\eta t)^{d+1}} P_M(\eta t) \\ &= \frac{1}{s}\sum_{\eta^s=1} \frac{(1-t)^{d+1}(1+t+\cdots+t^{s-1})^{d+1}}{(1-\eta t)^{d+1}} P_M(\eta t) \end{aligned}$$

From this,

$$\begin{aligned} e(M^{(s)}) = P_{M^{(s)}}(1) &= \frac{1}{s}\sum_{\eta^s=1} \frac{(1-t)^{d+1}(1+t+\cdots+t^{s-1})^{d+1}}{(1-\eta t)^{d+1}} P_M(\eta t)_{|t=1} \\ &= \frac{s^{d+1}}{s} P_M(1) = s^d e(M), \end{aligned}$$

since all terms on the right side vanish for $t = 1$ except the one with $\eta = 1$. □

Remark 7.4.16. The argument in the beginning of the proof above to the effect of rescaling the degrees of $R^{(s)}$ can only be employed because the latter is generated in a fixed degree. In the general case of an $\mathbb{N}$-graded ring, the Hilbert series of M still has a rational expression, where $1 - t^s$ is replaced by a product $\prod_{i=1}^{d+1}(1 - t^{r_1})$, where r_i is a positive integer independent of M. One will have no use for this generality in this book because there may not exist a Hilbert polynomial in this case, having to be replaced by a function that is piecewise polynomial (often called a *quasi-polynomial*).

7.4.3 Intertwining graded Hilbert functions

It is possible to extend the considerations of Subsection 7.4.2 to a relative concept involving the inclusion of two standard graded algebras. Note that this generalization

has nothing to do with considering the bigraded Hilbert–van der Waerden function. Since this is a fairly recent topic, with continued interest, its general picture will be given.

Let $(A, \mathfrak{n})$ denote a Noetherian local ring and its maximal ideal, and let $R \subset S$ be a homogeneous inclusion of standard A-algebras, with $R_0 = S_0 = A$. Here "homogeneous" means that $R_1 \subset S_1$.

The standing assumption throughout is that the A-module $[S/R]_1 = S_1/R_1$ is Artinian, *i. e.*, $\lambda(S_1/R_1) < \infty$.

Definition 7.4.17. Fix an integer $r \geq 1$. Given $n \in \mathbb{N}$, the A-module

$$S_n/R_{n-r+1}S_{r-1}$$

is the rth *intertwining module of order n* of the inclusion $R \subset S$.

Note that the intertwining module for $r = 1$ gives S_n/R_n. On the other hand, in the particular case in which S is a standard polynomial ring and R is a subalgebra generated in a same degree (renormalized), the length of S_n/R_n retrieves the usual graded Hilbert function of Subsection 7.4.2. This suggests that, for any fixed r, there is an intertwining graded Hilbert function. And indeed this is the case.

For that, it is convenient to introduce an intermediate module as a go-between. Let $G := \mathrm{gr}_I(S)$ stand for the associated graded ring of the ideal $I := R_1S$ in the ring S. Now, $G \simeq S[It]/IS[It]$, where $S[It]$ is the Rees algebra of an ideal generated by forms of the same degree (= 1). Then $S[It]$ is a standard bigraded A-algebra generated in bidegrees $(0, 1)$ and $(1, 0)$. This induces a structure of standard graded A-algebra by taking total degree. Therefore, also G has a structure of standard graded A-algebra.

One can do one step better, by considering the ideal

$$\mathfrak{a} := R_1 :_A S_1 = \mathrm{ann}(S_1/R_1) = [0 :_G S_1G]_0 \subset A.$$

Note that, for any $r \geq 1$, the ideal $\mathfrak{a}$ annihilates S_rG. The latter is then a (finitely generated) graded module over the standard $A/\mathfrak{a}$-algebra $G/0 :_G S_1G$, where $\dim A/\mathfrak{a} = \dim S_1/R_1 = 0$.

Proposition 7.4.18. *With the above notation, one has:*

(a) *The function* $n \mapsto \lambda(S_n/R_{n-r+1}S_{r-1})$ *is asymptotically a polynomial function* $p_r(n)$ *of degree* $\dim S_rG - 1 = \dim(G/0 :_G S_rG) - 1 \leq \dim G - 1 = d - 1$, *with* $d = \dim S$.

(b) *The corresponding polynomial has the form*

$$p_r(X) = \frac{e_r(R,S)}{(d-1)!}X^{d-1} + \text{lower order terms},$$

where

$$e_r(R,S) = \begin{cases} e(S_rG) & \text{if } \dim(G/0 :_G S_rG) = d \\ 0 & \text{if } \dim(G/0 :_G S_rG) < d \end{cases}$$

Proof. It suffices to show that, for every $n \geq r-1$, $\lambda(S_n/R_{n-r+1}S_{r-1}) = \lambda([S_rG]_n)$. Indeed, both (a) and (b) will then follow from Proposition 7.4.13 as applied to the graded module S_rG over the standard $A/\mathfrak{a}$-algebra $G/0 :_G S_1G$.

But this equality follows easily from the fact that

$$[S_rG]_n = \bigoplus_{j=1}^{n-r+1} R_{j-1}S_{n-j+1}/R_jS_{n-j},$$

the latter being evident as soon as one observes that, for any $t \geq 0$, $I^t = (R_1S)^t = R_tS$, hence by writing $G = \bigoplus_{t\geq 0} I^t/I^{t+1}$, the parts of degree n of S_rG in each summand are $S_n/R_1S_{n-1}, R_1S_{n-1}/R_2S_{n-2}, \ldots, R_{n-r}S_r/R_{n-r+1}S_{r-1}$. □

Definition 7.4.19. $e_r(R,S)$ is the *rth intertwining multiplicity* of the inclusion $R \subset S$.

Corollary 7.4.20. *With the above notation and terminology, one has:*

(i) *The intertwining multiplicity $e_r(R,S)$ is nonincreasing with r.*

(ii) *The intertwining multiplicity $e_r(R,S)$ stabilizes for $r \gg 0$; moreover, if the saturation $0 :_G (S_1G)^\infty$ is a minimal prime of G having maximal dimension then the stable value is the multiplicity of the module $G/0 :_G (S_1G)^\infty$.*

Proof. (i) Since $0 :_G S_rG \subset 0 :_G S_{r+1}G$, then $\dim\dim(G/0 :_G S_rG) \geq \dim\dim(G/0 :_G S_{r+1}G)$, and hence, $e(S_rG) \geq e(S_{r+1}G)$. If $e_{r+1}(R,S) = 0$, then trivially $e_r(R,S) \geq e_{r+1}(R,S)$. If $e_{r+1}(R,S) \neq 0$, then $\dim(G/0 :_G S_{r+1}G) = d$ and $e_{r+1}(R,S) = e(S_{r+1}G)$. But then $\dim(G/0 :_G S_rG) = d$ as well, so $e_r(R,S) = e(S_rG) \geq e(S_{r+1}G) = e_{r+1}(R,S)$.

(ii) The stability is obvious due to (i). To get the stable value as claimed, one clearly has $0 :_G (S_1G)^\infty = 0 :_G (S_1G)^{r_0} = 0 :_G S_{r_0}G$ for some $r_0 \gg 0$. By hypothesis, $\dim G/0 :_G (S_1G)^\infty = d$, hence the equalities

$$\dim G/0 :_G S_1G = \dim G/0 :_G (S_1G)^\infty = \dim S_{r_0}G$$

throughout. One claims that, moreover, $e(S_{r_0}G) = e(G/0 :_G (S_1G)^\infty)$. By the additivity formula in Subsection 7.4.2, it suffices to check that both modules have the same length locally at any of their minimal primes of maximal dimension (which are also the minimal primes of maximal dimension of the graded ring $G/0 :_G S_1G$). Letting $\wp \subset G$ being such a prime, since $0 :_G (S_1G)^\infty = 0 :_G S_{r_0}G$, then it follows that $0 :_G S_{r_0}G \notin \wp$ because $\wp$ has height zero. Therefore, $(S_{r_0}G)_\wp \simeq G_\wp$ and $(G/0 :_G S_{r_0}G) \simeq G_\wp$. This shows the stated equality of multiplicities. The result then follows from Proposition 7.4.18(a). □

The two most important multiplicities are $e(R,S) := e_1(R,S)$ and the stable value $e_\infty(R,S) := e(G/0 :_G (S_1G)^\infty)$. To see how meaningful are these multiplicities, one next states a few vanishing criteria.

For this, one needs a lemma.

Note that, by definition, one has

$$G/S_1G = S[(R_1S)t]/(S_1)S[(R_1S)t] \simeq \bigoplus_{i\geq 0} Rt^i \simeq R.$$

Lemma 7.4.21. *Considering* $(S_1G, 0 :_G S_1G)/S_1G$ *as an ideal of* $G/S_1G \simeq R$*, one has the equality* $V((S_1G, 0 :_G S_1G)/S_1G) = \operatorname{supp}_R(S/R)$*. In particular, the ideal* $(S_1G, 0 :_G S_1G)/S_1G$ *has positive height if and only if* $S_p = R_p$ *for every minimal prime* p *of* R*.*

Proof. Since $S_2G = (S_1G)(S_1G)$, the Krull–Nakayama lemma implies that

$$V\big((S_1G, 0 :_G S_1G)/S_1G\big) = \operatorname{supp}_R(S_1G/S_2G).$$

But, from the shape of the graded parts of G, one gets $S_1G/S_2G \simeq R + RS_1/R = S/R$, thus showing the first part of the statement.

The second part of the statement follows immediately from the first. □

Proposition 7.4.22. *One has:*

(a) $\operatorname{ht} 0 :_G S_1G > 0$ *if and only if the extension* $R \subset S$ *is integral and* $S_p = R_p$ *for every minimal prime* p *of* R*.*

(b) $\operatorname{ht} 0 :_G (S_1G)^\infty > 0$ *if and only if the extension* $R \subset S$ *is integral.*

Proof. (a) If $\operatorname{ht} 0 :_G S_1G > 0$, the annihilator is not contained in any minimal prime of G. Therefore, $(S_1G)_\wp = 0$, for every minimal prime of G. In particular, $S_1G \subset \wp$ for all such primes, which means that S_1G is a nilpotent ideal. Translating into ideals of the pair $R \subset S$, it is equivalent to having $S_1 \subset \sqrt{R_1S}$. The latter in turn is equivalent to having $R \subset S$ integral. Indeed, letting $S_1^N \subset (R_1S)_N = R_1^N + R_1S^{N-1}$ for certain $N \geq 1$, then it is clear that S is generated by $\{S_1, S_1^2, \ldots, S_1^{N-1}\}$ as an R-module.

On the other hand, $\operatorname{ht}(S_1G, 0 :_G S_1G)/S_1G \geq \operatorname{ht} 0 :_G S_1G > 0$, hence the previous lemma implies that $S_p = R_p$ for every $p \in \operatorname{Min}(R)$. The converse is also clear since $\operatorname{ht} 0 :_G S_1G = 0$ would imply that $(S_1G, 0 :_G S_1G)/S_1G \simeq 0 :_G S_1G/S_1G \cap 0 :_G S_1G$ has height zero.

(b) The first implication in the proof of (a) is now reversible:

$$\begin{aligned}\operatorname{ht} 0 :_G (S_1G)^\infty > 0 &\Leftrightarrow 0 :_G (S_1G)^\infty \not\subset \wp, \quad \forall \wp \in \operatorname{Min}(G)\\ &\Leftrightarrow \exists l : (S_1G)^l_\wp = 0, \quad \forall \wp \in \operatorname{Min}(G)\\ &\Leftrightarrow S_1G \subset \sqrt{0} \Leftrightarrow S_1 \subset \sqrt{R_1S} \Leftrightarrow R \subset S \quad \text{is integral.}\end{aligned}$$ □

Corollary 7.4.23. *Notation as before. Then:*

(a) *If the extension* $R \subset S$ *is integral and* $S_p = R_p$ *for every minimal prime* p *of* R*, then* $e(R, S) = 0$*.*

(b) *If the extension* $R \subset S$ *is integral, then* $e_\infty(R, S) = 0$*.*

(c) $e(A, B) = e_\infty(A, B)$ *if and only if* $S_p = R_p$ *for every prime* $p \in \operatorname{Spec} R$ *with* $\dim R/p = \dim R$*.*

Proof. (a) and (b) are clear from the respective items of the previous proposition, taking in account Proposition 7.4.18 (b).

As to (c), by the same argument as in the proof of Corollary 7.4.20 (ii), the equality $e(A,B) = e_\infty(A,B)$ is equivalent to having $(S_1G)_{\wp} = G_{\wp}$ for every minimal prime of G of maximal dimension, which in turn is equivalent to having $\dim(S_1G, 0 :_G S_1G)/S_1G < \dim G$. But the latter means that $\operatorname{ht}(S_1G, 0 :_G S_1G)/S_1G > 0$, hence the result follows from Lemma 7.4.21. □

Remark 7.4.24. The converse statement in both (a) and (b) above holds when S is equidimensional (*i. e.*, all minimal primes of S have the same dimension) and *universally catenary* (*i. e.*, the polynomial ring $S[X]$ has the property that height and dimension of any prime ideal add up to $\dim S + 1$). The two conditions are satisfied if, *e. g.*, A is a field and S is a domain (Corollary 2.5.34). For most applications, the conditions are usually verified, so the above give full criteria of vanishing of the extreme intertwining multiplicities.

To close this subsection, one wishes to compare the traditional multiplicities $e(R)$ and $e(S)$ via the intertwining multiplicities. For that, it will be assumed that $R \subset S$ are standard graded A-algebras, with $A = R_0 = S_0$ Artinian local, and $\dim R = \dim S$. So far, the finer structure of S as an R-module has not being essentially touched. Since S may fail to have a well-defined rank over R, one will assume a certain weaker behavior.

Theorem 7.4.25 (Intertwining multiplicities). *Let $R \subset S$ be a homogeneous inclusion of standard graded Noetherian rings of the same dimension with $A = R_0 = S_0$ Artinian local. Let $\mathfrak{P}$ denote the set of minimal primes of R of maximal dimension. Let $r \geq 1$ be an integer such that $S_{\mathfrak{p}}$ contains a free $R_{\mathfrak{p}}$-module of rank r for every prime $p \in \mathfrak{P}$. Then:*

(a) *$re(R) + e_\infty(R,S) \leq e(S)$ and equality holds if and only if S_p is a free R_p-module of rank r for every $p \in \mathfrak{P}$.*

(b) *If S is integral over R and S_p is a free A_p-module of rank r for every $p \in \mathfrak{P}$, then $re(R) = e(S)$. The converse holds if S is equidimensional.*

Proof. (a) Let $t \gg 0$ such that $S_tG = (S_1G)^\infty$ and consider the graded R-submodule $M := \sum_{i=0}^{t-1} RS_i \subset S$. Note that for any n, one has $(S/M)_n = S_n/R_{n-r+1}S_{r-1}$. On the other hand, $\dim M = \dim R$ since M is a finitely generated R-module containing 1. Thus, $\dim M = \dim S$. Finally, $M_p = S_p$ for every $p \in \mathfrak{P}$ since $t \gg 0$. It follows that $\operatorname{ann}(S/M) \subset p$ for every $p \in \mathfrak{P}$, hence has height 0, thus showing that $\dim S/M = \dim R = \dim B$ again.

Summing up, one has a short exact sequence of graded modules with all three terms of the same dimension. Then one can apply the claim in the proof of Proposition 7.4.13 to deduce that $e(S) = e(M) + e_\infty(R,S)$. Here, the three multiplicities are computed over three distinct graded rings: $e(S)$ is over S, $e(M)$ is over R and $e_\infty(R,S)$ is over G/S_1G. However, this should not matter since all one really does is to look at the asymptotic behavior of the three lengths which are given by polynomial functions whose leading terms give the respective multiplicities.

To complete the proof, one has to bring up the multiplicity $e(R)$ into picture.

Claim. $e(M) \geq re(R)$, with equality if and only if S_p is a free R_p-module of rank r for every $p \in \mathfrak{P}$.

To see this, recall that $M_p = S_p$ for every $p \in \mathfrak{P}$ since $t \gg 0$. Therefore, M, too, has the property that M_p contains a free R_p-module of rank r for every $p \in \mathfrak{P}$. By Proposition 7.4.13, one has $e(M) \geq re(R)$ and the equality holds if and only if M_p, hence S_p as well is free of rank r for every $p \in \mathfrak{P}$.

(b) One implication follows from (a) and Corollary 7.4.20 (b); for the reverse implication, one draws on Remark 7.4.24 by observing that $S[X]$ is still finitely generated over A and height and dimension will not change while passing to the residue field of A, in which case height and dimension of any prime ideal add up to $\dim S + 1$ (Corollary 2.5.34). □

Now, for usual applications in algebraic geometry, the Artinian ground ring is a field and S is a domain. The following basic result, a sort of associativity formula, is a nontrivial consequence of the earlier passages. The proof is beyond the objectives of the book: one refers to [145, Proof of Theorem 6.4] for the details.

Proposition 7.4.26. *Letting the notation be that of* Theorem 7.4.25, *suppose for simplicity that S is a domain and $A = k$ is a field. If $R \subset S$ is not integral, then*

$$e_\infty(R, S) = \sum_{\mathfrak{p}} e_{R_1 S_{\mathfrak{p}}}(S_{\mathfrak{p}}) e(S/\mathfrak{p}), \tag{7.4.26.1}$$

where $\mathfrak{p}$ runs through the minimal primes of S/R_1S of maximal dimension and $e_{R_1 S_{\mathfrak{p}}}(S_{\mathfrak{p}})$ is the local Samuel multiplicity.

The following formula has been recognized by several authors (see, *e. g.*, [31, Theorem 2.5]).

Theorem 7.4.27 (Degree formula in dimension one). *Let T denote a standard graded domain of dimension $d \geq 1$ over a field k and let $I \subset T$ denote a homogeneous ideal generated in fixed degree $s \geq 1$. Assume:*
(a) $\dim T/I = 1$.
(b) $\dim k[I_s] = \dim T$.

Then

$$e(k[I_s]) = \frac{1}{r}\left(e(T)s^{d-1} - \sum_{\mathfrak{p}} e_{I_{\mathfrak{p}}}(T_{\mathfrak{p}}) e(T/\mathfrak{p}) \right),$$

where r denotes the degree of the field extension $k(T_s)|k(I_s)$ and $\mathfrak{p}$ runs through the maximal associated primes of T/I in T.

Proof. Using (b), apply Theorem 7.4.25 with $R = k[I_s]$ and $S = k[T_s] = T^{(s)}$, thus getting

$$re(k[I_s]) = e(T^{(s)}) - e_\infty(k[I_s], T^{(s)}).$$

Now, rescale the gradings of both $k[I_s]$ and $T^{(s)}$ so that the inclusion $k[I_s] \subset T^{(s)}$ is a homogeneous inclusion of standard graded algebras over k. By (i), $\dim T^{(s)}/I_s T^{(s)} = 1$, hence $\operatorname{ht} I_s T^{(s)} < \dim T^{(s)}$, thus showing that $T^{(s)}$ is not finitely generated as a $k[I_s]$-module. Now apply (7.4.26.1) to the inclusion $k[I_s] \subset T^{(s)}$ and use Proposition 7.4.15 to get the stated formula. □

There are more involved formulas as the above for $\dim T/I \geq 2$, in terms of the newcomer so-called *j-multiplicity*. These formulas treat the right side of the above formula as a first term of a summation with other terms. The latter depend on certain generic choices and on taking the *j*-multiplicity afterwards. Perhaps they lack the same stability and simplicity statement (see [164] for these generalized formulas).

7.4.4 The local Hilbert–Samuel function

Quite early in the last century the idea of studying the asymptotic behavior of powers of an ideal came up. The intuition that increasing power exponents looked like an alternative to increasing degrees in the graded case took shape in the late 40s of the past century as the remarkable work of Pierre Samuel.

In this part, one covers the main aspects of this theory.

7.4.4.1 Basic definitions

Throughout, $(R, \mathfrak{m})$ denotes a Noetherian local ring and M a finitely generated R-module. The extension of the theory to the case of a Noetherian semilocal ring offers no difficulty and is left to the curious reader.

Fix an $\mathfrak{m}$-primary ideal $\mathfrak{q}$.

Definition 7.4.28. The *Hilbert–Samuel function* $HS_{\mathfrak{q}}(M, \_)$ of M relative to $\mathfrak{q}$ is defined by $HS_{\mathfrak{q}}(M, n) := \lambda(M/\mathfrak{q}^n M)$ for $n \in \mathbb{N}$.

Note that, as $\operatorname{supp} M/\mathfrak{q}^n M \subset \operatorname{supp} R/\mathfrak{q}$ (Corollary 5.1.5), then $\lambda(M/\mathfrak{q}^n M) < \infty$.

Proposition 7.4.29. *$HS_{\mathfrak{q}}(M, n)$ is a polynomial in n for $n \gg 0$.*

Proof. First, note that $\lambda(M/\mathfrak{q}^n M) = \sum_{i=0}^{n} \lambda(\mathfrak{q}^i M/\mathfrak{q}^{i+1} M)$. Therefore, it suffices to show that, $\lambda(\mathfrak{q}^n M/\mathfrak{q}^{n+1} M)$ is a polynomial in n for $n \gg 0$. But $\mathfrak{q}^n M/\mathfrak{q}^{n+1} M$ is the nth graded piece of the standard graded associated module $\operatorname{gr}_{\mathfrak{q}}(M) = \sum_{i \geq 0} \mathfrak{q}^i M/\mathfrak{q}^{i+1} M$, which is finitely generated over the standard graded associated ring $\operatorname{gr}_{\mathfrak{q}}(R)$. Since $R/\mathfrak{q}$ is Artinian, the result follows from Theorem 7.4.8(i). □

The asymptotic polynomial thus obtained is called the *Hilbert–Samuel polynomial* of M relative to the $\mathfrak{m}$-primary ideal $\mathfrak{q}$. One often refers to it, as well as to its source function, simply by the name of Samuel.

Let $d_{\mathfrak{q}}(M)$ denote the degree of the Samuel polynomial of M relative to $\mathfrak{q}$. Although these definitions depend on $\mathfrak{q}$, one has the following independence result.

Lemma 7.4.30. *Let $\mathfrak{q}$ and $\mathfrak{q}'$ denote $\mathfrak{m}$-primary ideals. Then $d_{\mathfrak{q}}(M) = d_{\mathfrak{q}'}(M)$.*

Proof. It follows from having inclusions $\mathfrak{q}^r \subset \mathfrak{q}'$ and $\mathfrak{q}'^{r'} \subset \mathfrak{q}$, for suitable exponents r, r'. □

Thus, one denotes by $d(M)$ the uniquely defined degree of the Samuel polynomial of a finitely generated R-module M. Note that $\lambda(\mathfrak{q}^n M/\mathfrak{q}^{n+1}M)$ is a polynomial of degree $\dim \mathrm{gr}_{\mathfrak{q}}(M)-1$ for $n \gg 0$. By passing to the residue ring $R/\mathrm{ann}(M)$, one may assume that M has zero annihilator, from which one can reduce to the case where $M = R$. Therefore, by Theorem 7.3.6, $\dim \mathrm{gr}_{\mathfrak{q}}(M) = \dim M$. Trailing some further combinatorial steps, it is possible to eventually deduce that $d(M) = \dim M$. A different argument will be given in the proof of the next celebrated theorem.

7.4.4.2 A main theorem

Theorem 7.4.31 (Krull–Chevalley–Samuel). *Let $M \neq \{0\}$ stand for a finitely generated module over the Noetherian local ring $(R, \mathfrak{m})$. Then $d(M) = \dim M = s(M)$, where $s(M)$ denotes the cardinality of a system of parameters of M.*

Proof. The equality $\dim M = s(M)$ has been shown in Theorem 5.1.11. Thus, it suffices to prove that $d(M) \geq \dim M$ and that $s(M) \geq d(M)$. The rest of the proof, at least in the case where $M = R$, is essentially the original argument by Samuel in [133], later transcribed in [169].

– $d(M) \geq \dim M$.
  Suppose this is proved when M is a cyclic R-module. Use a similar strategy to the one in the proofs of Theorem 7.4.8 and of Proposition 7.4.13. Namely, consider a finite filtration of M by cyclic quotients $M_i/M_{i-1} \simeq R/\wp_i$. Then $\dim M = \max_i\{\dim R/\wp_i\}$ by the same argument as in step (1) of the proof of Theorem 7.4.8. Thus, it suffices to show that $d(M) = \max_i\{d(R/\wp_i)\}$ as well. Working up through the filtration of M, using induction, it suffices to argue that in the exact sequence of R-modules

$$0 \to M_{i-1} \to M_i \to R/\wp_i \to 0$$

  for a given i, one has $d(M_i) = \max\{d(M_{i-1}), d(R/\wp_i)\}$. In fact, more generally, the following analogue of 7.4.13.1 holds.

Claim. For any exact sequence $0 \to E' \to E \to E'' \to 0$ of finitely generated R-modules, one has $d(E) = \max\{d(E'), d(E'')\}$.

To see this, recall that the definition of the degree $d(M)$ is independent of the chosen $\mathfrak{m}$-primary ideal. The argument will be through by proving the following assertions:

(a) $HS(E,n) = HS(E'',n) + \lambda(E'/E' \cap \mathfrak{m}^n E)$.
(b) Let $d'(n)$ denote the value of $\lambda(E'/E' \cap \mathfrak{m}^n E)$ for $n \gg 0$. Then $d(M) = \max\{d(E''), d'(n)\}$.
(c) There exists an integer m such that $\mathfrak{m}^{n+1}E' \subset E' \cap \mathfrak{m}^{n+1}E \subset \mathfrak{m}^{n+1-m}E'$, for every $n > m$.

Now, (a) is quite obvious, while (b) follows from the fact that both summands of the right side in (a) take nonnegative values. As to (c), it is a consequence of the Artin–Rees lemma (Proposition 7.3.2.2).

One now considers the case where M is cyclic. Since there is no restriction on the original base ring R (except requiring it be Noetherian local), one may assume that $M = R$.

One inducts on $d := d(R)$. If $d = 0$ then $HS(R,n)$ is constant for all $n \gg 0$, hence $\mathfrak{m}$ is nilpotent, showing that R is Artinian.

Let $d \geq 1$ and suppose that the assertion is true for any Noetherian local ring S with $d(S) < d$. Letting $\wp_0 \subset \wp_1 \subset \cdots \subset \wp_h = \mathfrak{m}$ denote a maximal chain of prime ideals ($h = \dim R$), it will be shown that $d(R) \geq h$. One may assume that $h \geq 1$ as otherwise there is nothing to prove.

Claim 1. For any ideal $I \subset \mathfrak{m}$, $d(R/I) \leq d(R)$.

To see this, first note that $d(R/I)$ is the same regardless as to whether R/I is considered as a ring or as an R-module. Now, $HS(R/I,n) = \lambda(R/(I,\mathfrak{m}^n)) \leq \lambda(R/\mathfrak{m}^n)$ for every $n \geq 0$, whence the contention follows.

Claim 2. For any Noetherian local ring $(S,\mathfrak{n})$ and any element $a \in \mathfrak{n}$, one has $HS(S/(a), n) = HS(S,n) - \lambda(S/\mathfrak{n}^n : (a))$.

This stems from the following equalities:

$$\begin{aligned} HS(S/(a),n) - HS(S,n) &= \lambda(S/\mathfrak{n}^n) - \lambda\big(S/(\mathfrak{n}^n,a)\big) = \lambda\big((\mathfrak{n}^n,a)/\mathfrak{n}^n\big) \\ &= \lambda\big((a)/\mathfrak{n}^n \cap (a)\big) = \lambda\big((a)/(a)(\mathfrak{n}^n : (a))\big) \\ &= \lambda\big(S/\mathfrak{n}^n : (a)\big), \end{aligned}$$

where the last equality is given by multiplication by a.

Next, choose an element $a \in \wp_1 \setminus \wp_0$ (recall that $h \geq 1$). Set $\overline{R} := R/\wp_0$ and $\overline{a}$ for the class of a in $\overline{R}$.

Claim 3. $d(\overline{R}/(\overline{a})) = d(\overline{R}) - 1$.

To prove this claim, set $\overline{\mathfrak{m}} := \mathfrak{m}/\wp_0$. By Proposition 7.3.2.2, there exists an integer m such that $\overline{\mathfrak{m}}^n : (\overline{a}) \subset \overline{\mathfrak{m}}^{n-m}$, for every $n \geq m$. Now, clearly $\overline{\mathfrak{m}}^{n-1} \subset \overline{\mathfrak{m}}^n : (\overline{a})$, hence

$$HS(\overline{R}, n-m) \leq \lambda\big(\overline{\mathfrak{m}}^n : (\overline{a})\big) \leq HS(\overline{R}, n-1).$$

Applying Claim 2, one gets the inequalities

$$HS(\overline{R},n) - HS(\overline{R},n-1) \leq HS\big(\overline{R}/(\overline{a}),n\big) \leq HS(\overline{R},n) - HS(\overline{R},n-m).$$

Since $d(\overline{R}/(\overline{a}))$ is the degree of the polynomial $HS(\overline{R}/(\overline{a}), n)$ for $n \gg 0$, one is through for the claim.

To continue the proof, apply the inductive hypothesis to get $\dim(\overline{R}/(\overline{a})) \leq d(\overline{R}) - 1$. But the assumed chain of prime ideals of R induces the following chain of prime ideals in $\overline{R}/(\overline{a})$:

$$\wp_1/(\wp_0, a) \subset \cdots \subset \wp_h/(\wp_0, a)$$

which, consequently, has at most $d(\overline{R}) - 1$ terms. Therefore, $h \leq d(\overline{R}) \leq d(R)$, by Claim 1 with $I = \wp_0$, as was to be shown.

– $s(M) \geq d(M)$.

  First, for any subset $\{a_1, \ldots, a_r\} \subset \mathfrak{m}$ one has $d(M/\sum_{i=1}^{r} a_i M) \geq d(M) - r$. To see this it suffices, by recurrence, to show that for any $a \in \mathfrak{m}$, one has $d(M/aM) \geq d(M) - 1$. For that, one considers the exact sequence of R-modules induced by multiplication by a:

$$0 \to K \to M/\mathfrak{m}^{n-1}M \xrightarrow{\cdot a} M/\mathfrak{m}^n M \to M/(\mathfrak{m}^n, a)M \to 0.$$

  Since $M/(\mathfrak{m}^n, a)M = (M/aM)/\mathfrak{m}(M/aM)$, one gets $\lambda(M/\mathfrak{m}^{n-1}M) - \lambda(M/\mathfrak{m}^n M) \leq \lambda((M/aM)/\mathfrak{m}(M/aM))$, which shows the contention. Now, in particular, if $\{a_1, \ldots, a_r\}$ is a system of parameters of M then $M/\sum_{i=1}^{r} a_i M$ has finite length, hence its Samuel function is constant, *i. e.*, the Samuel polynomial has degree zero. It follows that $d(M/\sum_{i=1}^{r} a_i M) = 0$, so $d(M) \leq r = s(M)$. □

7.4.4.3 Local multiplicity

By general combinatorics as seen before, the Samuel polynomial of a finitely generated R-module M relative to an $\mathfrak{m}$-primary ideal $\mathfrak{q}$, as a polynomial in $X + 1$, can be written in the form

$$e_0\binom{X + \dim M}{\dim M} - e_1\binom{X - 1 + \dim M}{\dim M} + \cdots + (-1)^{\dim M} e_{\dim M},$$

where each e_i is an integer, often called the ith Hilbert coefficient of $\mathfrak{q}$ on M.

The *multiplicity of* $\mathfrak{q}$ *on* M is defined to $d!$ times the coefficient of degree d of this polynomial, where $d = \dim R$. It is denoted $e(\mathfrak{q}, M)$.

This definition has been introduced by Samuel ([132]) in the case where $M = R$, later extended to arbitrary R-modules by Serre and other authors. Note that, by this extension to R-modules one has $e(\mathfrak{q}, M) = 0$ if $\dim M < d$ and $e(\mathfrak{q}, M) = e_0 > 0$ if $\dim M = d$. If $M = R$, one sets $e(\mathfrak{q}, R) = e(\mathfrak{q})$ and call it the multiplicity of $\mathfrak{q}$. If in addition $\mathfrak{q} = \mathfrak{m}$, then one sets $e(\mathfrak{m}, R) = e(R)$ and call it the multiplicity of R.

One reason to defer $\dim M$ in favor of $\dim R$ in the definition of multiplicity is that one gets the universal formula

$$e(\mathfrak{q}, M) = \lim_{n \to \infty} \frac{d!}{n^d} \lambda(M/\mathfrak{q}^n M),$$

where d is independent of M. In particular, if $d = 0$ then $e(\mathfrak{q}, M) = \lambda(M)$.

7.4.4.4 Parameter ideals

Among $\mathfrak{m}$-primary ideals, the ones generated by a system of parameters have a distinguished role. It is usual to call them *parameter ideals*.

Proposition 7.4.32 (Chevalley–Samuel). *Let $(R, \mathfrak{m})$ stand for a Noetherian local ring of dimension d, let $\mathfrak{q}$ denote a parameter ideal of R and let M be a finitely generated R-module. Then:*

(i) *The fiber cone of $\mathfrak{q}$ is a polynomial ring over $k = R/\mathfrak{m}$; in particular, if R contains a field K, any set of minimal generators of $\mathfrak{q}$ is algebraically independent over K.*
(ii) $\lambda(M/\mathfrak{q}^n M) \leq \lambda(M/\mathfrak{q}M)\binom{n+d-1}{d}$ *for all* $n \geq 0$.
(iii) $e(\mathfrak{q}, M) \leq \lambda(M/\mathfrak{q}M)$.
(iv) *The equality $e(\mathfrak{q}, R) = \lambda(R/\mathfrak{q})$ holds if and only if the associated graded ring of $\mathfrak{q}$ is a polynomial ring over $R/\mathfrak{q}$.*
(v) *If R is Cohen–Macaulay, then $e(\mathfrak{q}, R) = \lambda(R/\mathfrak{q})$.*

Proof. (i) Let $\{a_1, \ldots, a_d\}$ stand for a minimal set of generators of $\mathfrak{q}$ and consider the k-algebra map $k[X_1, \ldots, X_r] \to F(\mathfrak{q}) := \mathcal{R}_R(\mathfrak{q})/\mathfrak{m}\mathcal{R}_R(\mathfrak{q}) = \sum_{t\geq 0} \mathfrak{q}^t/\mathfrak{m}q^{t+1}$ such that X_i maps to the residue of a_i. It suffices to show that $\dim F(\mathfrak{q}) = d$.

Suppose that $\dim F(\mathfrak{q}) \leq d-1$. Let $k[z_1, \ldots, z_{d-1}] \subset F(I)$ be a graded Noether normalization. One may assume for simplicity that $z_1, \ldots, z_{d-1}$ are forms of the same degree $t > 0$, *i. e.*, residues of elements $p_1, \ldots, p_{d-1} \in \mathfrak{q}^t$, respectively. By the integrality of the residue of each a_i over $k[z_1, \ldots, z_{d-1}]$, one deduces that $\mathfrak{q}^n \subset (p_1, \ldots, p_{d-1}, \mathfrak{m}\mathfrak{q}^n)$ for some $n \gg 0$, hence $\mathfrak{q}^n \subset (p_1, \ldots, p_{d-1})$ by Krull–Nakayama for some $n \gg 0$. This is impossible since $\mathfrak{q}^n$ is $\mathfrak{m}$-primary while $(p_1, \ldots, p_{d-1})$ has height $\leq d-1$.

To see the second assertion, recall that as a consequence of the first part a minimal set of generators of $\mathfrak{q}$ is analytically independent in $\mathfrak{q}$ (Section 7.3.3). In particular, a form with coefficients in K that vanish upon evaluation at these generators will have coefficients in $\mathfrak{m}$, hence must itself vanish.

(ii) Using the relation $\lambda(M/\mathfrak{q}^n M) = \sum_{i=0}^n \lambda(\mathfrak{q}^i M/\mathfrak{q}^{i+1}M)$, this follows from the following obvious inequalities:

$$\lambda(\mathfrak{q}^i M/\mathfrak{q}^{i+1}M) \leq \lambda(M/\mathfrak{q}M)\mu(\mathfrak{q}^i)$$

and

$$\mu(\mathfrak{q}^i) \leq \binom{d+i-1}{d-1},$$

for all $i \geq 0$.

(iii) This is an immediate consequence of (i).

(iv) One has $G := \mathrm{gr}_{\mathfrak{q}}(R) = \sum_{t\geq 0} \mathfrak{q}^t/\mathfrak{q}^{t+1}$. Let $G \simeq S/\mathcal{I}$ be a presentation, with $S = R/\mathfrak{q}[X_1, \ldots, X_d]$ a polynomial ring and $\mathcal{I}$ homogeneous. Then

$$\lambda(R/\mathfrak{q}^n) = \lambda(S/(\mathcal{I}, S_+^n)).$$

Note that the right side is a graded Hilbert function. Assuming that $\mathcal{I} \neq 0$, let $f \in \mathcal{I}$ be a nonzero form of degree e. For given $n \geq e$, multiplication by f upon monomials of degrees at most $n-e-1$ gives rise to an $R/\mathfrak{q}$-submodule of $\mathcal{I}$ of length at least $\binom{n-e+d-1}{d-1}$. Therefore, applying length along the exact sequence

$$0 \to \mathcal{I}/\mathcal{I} \cap S_+^n \to S/S_+^n \to S/(\mathcal{I}, S_+^n) \to 0,$$

yields

$$\begin{aligned} HS(R,\mathfrak{q}) &= \lambda(S/(\mathcal{I}, S_+^n)) = \lambda(S/S_+^n) - \lambda(\mathcal{I}/\mathcal{I} \cap S_+^n) \\ &\leq \lambda(R/\mathfrak{q})\binom{n+d-1}{d} - \binom{n-e+d-1}{d-1}. \end{aligned}$$

This inequality implies a strict inequality $e(\mathfrak{q}, R) < \lambda(R/\mathfrak{q})$.

(v) Since R is Cohen–Macaulay, $\mathfrak{q}$ is generated by a regular sequence of length d. Therefore, the minimal number of generators of $\mathfrak{q}^i$ is exactly the above combinatorial expression and $\mathfrak{q}^i/\mathfrak{q}^{i+1}$ is a free $R/\mathfrak{q}$-module of rank equal that same number. Thus, both inequalities above become equalities for $M = R$. □

Remark 7.4.33. Note that item (iv) above says that every higher conormal module $\mathfrak{q}^t/\mathfrak{q}^{t+1}$ is a free $R/\mathfrak{q}$-module of rank $\binom{d+t-1}{d-1}$. However, for $\mathfrak{q}$ to be moreover generated by a regular sequence one needs that $R/\mathfrak{q}$ have finite homological dimension over R—in this case R is necessarily Cohen–Macaulay. An easy example of a parameter ideal in a ring of dimension 2, satisfying the inequality $e(\mathfrak{q}, R) < \lambda(R/\mathfrak{q})$, is shown in Exercise 7.6.6.

7.4.4.5 Associativity formulas

The purpose of this short part is to state two useful results, both called associativity formulas. The first is the analogue of the associativity formula for the graded Hilbert function. It is stated as follows.

Theorem 7.4.34 (Associativity of local multiplicities). *Let $(R, \mathfrak{m})$ be a Noetherian local ring, let $\mathfrak{q} \subset R$ be an $\mathfrak{m}$-primary ideal and let M be a finitely generated R-module. Then*

$$e(\mathfrak{q}, M) = \sum_{\wp} \lambda(M_\wp) e\big((\mathfrak{q}, \wp)/\wp, R/\wp\big),$$

where $\wp$ runs through the set of prime ideals of R such that $\dim R/\wp = \dim R$ and $(\mathfrak{q}, \wp) \neq R$.

One of the known proofs follows pretty much the same scheme as that of the associativity formula for the Hilbert function in the graded case (Proposition 7.4.13). The only point that needs to be established is the additivity of the local multiplicity along an exact sequence as an analogue of 7.4.13.1.

Lemma 7.4.35. *Let $(R, \mathfrak{m})$ be a Noetherian local ring, let $\mathfrak{q} \subset R$ be an $\mathfrak{m}$-primary ideal and let $N \subset M$ be finitely generated R-modules. Then*

$$e(\mathfrak{q}, M) = e(\mathfrak{q}, N) + e(\mathfrak{q}, M/N).$$

Proof. The proof follows pretty much the same scheme as in the proof of the claim in Theorem 7.4.31. Namely, one has

$$\lambda\big(M/\mathfrak{q}^n M\big) - \lambda\big((M/N)/\mathfrak{q}^n(M/N)\big) = \lambda\big(N/N \cap \mathfrak{q}^n M\big).$$

Thus, one only has to care about the right-hand side, which one does by applying the Artin–Rees result: let $r \geq 0$ be an integer such that $N \cap \mathfrak{q}^n M \subset \mathfrak{q}^{n-r} N$ for $n > r$. From this, get $\lambda(N/\mathfrak{q}^{n-r}N) \leq \lambda(N/N \cap \mathfrak{q}^n M) \leq \lambda(N/\mathfrak{q}^n N)$ for $n > r$. Therefore,

$$e(\mathfrak{q}, M) - e(\mathfrak{q}, M/N) = \lim_{n\to\infty} \frac{d!}{n^d} \lambda\big(N/N \cap \mathfrak{q}^n M\big) = \lim_{n\to\infty} \frac{d!}{n^d} \lambda\big(N/\mathfrak{q}^n N\big) = e(\mathfrak{q}, N). \qquad \square$$

Alternatively, transcribing the argument established by Nagata ([112, Theorem 23.5]), still drawing upon the above additivity claim, but with a different inductive procedure.

Nagata inducts on the integer $m_M := \sum_{\wp} \lambda(M_\wp)$.

If $m_M = 0$, then each $\lambda(M_\wp) = 0$, hence $M_\wp = 0$ for every such prime ideal. Thus, one can pick a single $a \in \mathfrak{m} \setminus \cup_\wp \wp$. Since a thus taken is a parameter of R, one has $\dim M = \dim R/0 : M \leq \dim R - 1$. Therefore, $e(\mathfrak{q}, M) = 0$.

Now, assume that $m \geq 1$. Then $M_\wp \neq 0$ for some $\wp$, hence $\wp \in \operatorname{supp} M$, so $\wp$ must be an associated prime of M. Let $N \subset M$ denote a submodule such that $R/\wp \simeq N$. Clearly, $N_\mathfrak{p} = 0$ for every prime $\mathfrak{p} \neq \wp$, while $\lambda(N_\wp) = 1$ Therefore, $m_{M/N} < m_M$. Applying the inductive hypothesis to M/N and noting that $e(\mathfrak{q}, N) = e(\mathfrak{q}, R/\wp) = e((\mathfrak{q}, \wp)/\wp, R/\wp)$, one is through. $\square$

The second associativity result is actually a generalization of the one above but only for the case where $\mathfrak{q}$ is a parameter ideal. It gives a kind of recursive formula on multiplicities.

Theorem 7.4.36 (Chevalley associativity formula for parameter ideals). *Let $(R, \mathfrak{m})$ be a Noetherian local ring of dimension d and M a finitely generated R-module. Let $\{a_1, \ldots, a_d\} \subset \mathfrak{m}$ be a system of parameters and $\{a_1, \ldots, a_r\}$ a subsystem thereof $(r \leq d)$. Setting $\mathfrak{a} = (a_1, \ldots, a_r) \subset \mathfrak{q} = (a_1, \ldots, a_d)$, one has*

$$e(\mathfrak{q}, M) = \sum_{\wp} e(\mathfrak{a}_\wp, M_\wp) e\big((\mathfrak{q}, \wp)/\wp, R/\wp\big),$$

where $\wp$ runs through the set of minimal prime ideals of $R/\mathfrak{a}$ such that $\operatorname{ht}\wp = r$ and $\dim R/\wp = d - r$.

In comparison with the previous result, besides the requirement that $\mathfrak{q}$ be a parameter ideal, the lengths have been replaced by local multiplicities along minimal primes of the subsystem of parameters. The two versions are visibly intermingled, but it is the version for parameter ideals that has been originally named *associativity formula*.

The proof of this theorem will be omitted, but see the historic note below for comments on both the inception and the proofs of this celebrated result.

7.5 Historic note

7.5.1 The Rees algebra

Rees used the algebra that bears his name for the purpose of studying analytic properties of a set of generators of an ideal in a local ring. Actually, Rees used the now called "extended" Rees algebra (sometimes called the Rees ring), namely, $R[It, t^{-1}]$. The reason was that this algebra is a deformation of the associated graded ring of the ideal (originally introduced by Krull).

Nearly at the same time, the French school (enhanced by the Grothendieck program) was using the "ordinary" Rees algebra as the corresponding object of the geometric blow-up process used in resolution of singularities. It is possible that even earlier versions were made available. It would be interesting to find out who was the first to clearly pinpoint these algebras.

The definition of the Rees algebra of a module in one of its current uses was first given by Micali ([109], [110]). From a review by P. Samuel, one reads: "*Etant donnés un anneau commutatif A et un A-module M, soit S l'ensemble des nondiviseurs de zéro de A; le noyau $t(M)$ de $M \to S^{-1}M$ s'appelle le sous-module de torsion de M. On appelle algèbre de Rees $R(M)$ de M la solution du problème universel relatif aux applications A-linéaires de M dans les A-algèbres (commutatives) E telles que $t(E) = 0$. On construit cette algèbre comme quotient de l'algèbre symétrique $S(M)$; elle est munie d'une structure graduée.*"

7.5.2 The symmetric algebra

As to the terminology "symmetric algebra," which is now widely accepted by commutative algebraists, there was some slight early controversy as to its current use since it means something else in the realm of non-commutative algebra. From the review by M. Nagata of one of the first results on symmetric algebras by A. Micali: "*Let A be a commutative ring having 1, and let M be an A-module. The author considers $S_A(M)$, the symmetric algebra of M* (*algèbre symétrique de M*) (*No definition of this is given, but it appears to be the most general commutative ring generated by M over A. The reviewer takes exception to the use of the term, because $S_A(M)$ has no special relationship with the usual notion of a symmetric algebra, which is a generalization of a group algebra of a finite group.*)."

Of course, there is no discussion about the firm use of this terminology, as it is one of the most basic constructions in ring theory, being defined by means of a universal property. Besides, historically it is responsible for most variations of symmetrization of chain complexes out of the de Rham-like or Koszul-like complexes. It is still a bit of a surprise that, being such a ground gadget, it has as far out a role as the "naive blowup" in geometry.

7.5.3 Artin–Rees lemma

The history of this celebrated result is reasonably short. What has subsequently taken up the work of many algebraists is various ways of generalizing the lemma, searching for some universal Artin–Rees exponent.

As to its origins, says a well-known researcher:

> (R. Sharp) "David Rees explained the name of the lemma as follows: he had his proof of the lemma in 1954, but did not submit it for publication until May 1955; the resulting paper appeared in 1956, in the very month in which Emil Artin lectured, at a conference in Japan, about his discovery of the same argument and result; M. Nagata was asked to adjudicate as to who should receive the credit, and responded that it is obviously the Artin–Rees lemma."

7.5.4 Associativity formulas

The history of the associativity formulas goes back to van der Waerden, as discussed in this book (Subsection 2.7.4). It has three more or less distinct phases, starting with the seminal paper of van der Waerden, going through the case of graded modules (Hilbert–Serre) and reaching the local case (Samuel). The terminology is already entrenched in the literature, although some people believe that it is misleading. In fact, the result itself looks more like an additivity formula or, more precisely, a decomposition expression. Here is the opinion on the importance of the formula by an undeniable expert:

> (C. Chevalley, 1945) "Another intersection theory of algebraic varieties will be published shortly by A. Weil. I have been in constant communication with A. Weil during the writing of this paper; many of the ideas involved can be traced back to discussions of the subject between him and myself. It is therefore impossible for me to acknowledge with precision the extent of my indebtedness to him. Nevertheless, it can be said definitely that the statement of the "projection formula" and the knowledge of the fact that all properties of intersections can be derived from three basic theorems (namely, the theorem on intersection of product varieties, the projection formula and the formula of associativity) are both due specifically to A. Weil."

7.6 Exercises

Exercise 7.6.1. Let $(R.\mathfrak{m})$ denote a Noetherian local domain admitting a nonzero principal ideal that is $\mathfrak{m}$-primary.

(a) Prove that $\mathfrak{m}$ is the only prime ideal of R other than zero.
Hint: (Rees) Show that for any nonzero $b \in \mathfrak{m}$, there is some integer $r \geq 0$ such that $a^r \in (b)$ (hence (b) is $\mathfrak{m}$-primary). To see this, first use the Artin–Rees lemma to get r such that $(a)^{r+1} \cap (b) = a((a)^r \cap (b))$. Then, using various elementary modulo isomorphisms and multiplication by the nonzero divisor b, argue that the two modules $(a^{r+1}, b)/(a)^{r+1}$ and $(a^r, b)/(a)^{r+1}$ have the same length, hence $a^r \in (a^{r+1}, b)$. From this, we finally arrive at $a^r \in (b)$.
(b) Deduce the principal ideal theorem from (a).

Exercise 7.6.2. Let R be a ring and $I \subset R$ an ideal.
(i) Show that if I is generated by an R-sequence then $\mathrm{gr}_I(R)$ is a polynomial ring over R/I.
(Hint: do not assume known the fact that I is an ideal of linear type: use the Koszul complex instead.)
(ii) Show that if R is Noetherian and $\mathrm{gr}_I(R)$ is a polynomial ring over R/I then I^r/I^{r+1} is a free R/I-module, for every $r \geq 1$.
(iii) (Rees) If $(R, \mathfrak{m})$ is a Noetherian local ring and $I \subset \mathfrak{m}$ is such that $\mathrm{gr}_I(R)$ is a polynomial ring over R/I then I is generated by an R-sequence.
(Hint: induct on the number of generators of I—this is trickier, as just knowing that the modules I^r/I^{r+1} are free R/I-modules will not do it (see [128]).)

Exercise 7.6.3. Let $(R, \mathfrak{m})$ be a Noetherian local domain of dimension and let M be a finitely generated R-module that is free on $\operatorname{Spec} R \setminus \{\mathfrak{m}\}$. Then $\dim \mathcal{S}_R(M) = \sup\{\mu(M), \dim R + \operatorname{rank}(M)\}$.

Exercise 7.6.4. Show that the Huneke–Rossi formula for the dimension of the symmetric algebra implies the formula stated in Proposition 7.2.19 for ideals contained in the Jacobson radical.

Exercise 7.6.5. (This is an exercise about the Rees algebra of simplest possible ideals.) Let $R = k[X, Y]$ be a polynomial ring in two variables over a field k.
– Given polynomials $f, g \in R \setminus k$ having no proper common factor, show that the Rees algebra of the complete intersection (f, g) is normal if and only if either $f \notin (X, Y)^2$ or $g \notin (X, Y)^2$.
– Let $I = (X^a, X^c Y^d, Y^b)$, with $a > c \geq 1$ and $b > d \geq 1$. Show that the Rees algebra of I is Cohen–Macaulay if and only if either $a \geq 2c$, $b \geq 2d$ or else $a \leq 2c$, $b \leq 2d$.
(Hint: if, say, $a \geq 2c$, $b \geq 2d$, construct the explicit 3×2 Hilbert–Burch defining matrix; for the converse, argue that there exists a minimal relation with some coefficient $\notin (X, Y)$, thus contradicting the fact that the analytic spread of an (X, Y)-primary ideal has maximum value 2.)
– For I as in the previous item, show that the Rees algebra $\mathcal{R}(I)$ of I is normal if and only if either $a = 2$, $c = 1$, $b \geq 2d$ or else $b = 2$, $d = 1$, $a \geq 2c$.

(Hint: use the fact that Cohen–Macaulayness implies the property (S_2) and that for normal semigroup rings are Cohen–Macaulay; the rest is taken care by considering the codimension of the Jacobian ideal of a defining ideal of $\mathcal{R}(I)$.)

– Let $I = (X, Y)^n$, for $n \geq 1$. Prove that a defining ideal of $\mathcal{R}(I)$ is generated by the 2-minors of the scroll (double catalecticant) matrix

$$\begin{bmatrix} X & T_1 & T_2 & \cdots & T_n \\ Y & T_2 & T_3 & \cdots & T_{n+1} \end{bmatrix}$$

where the T's are indeterminates over R. Prove that $\mathcal{R}(I)$ is normal.
(Hint: argue first that $\mathcal{R}(I)$ is a Cohen–Macaulay prime ideal by the Eagon–Northcott criterion. Then argue that it is actually locally regular on the punctured spectrum.)

Exercise 7.6.6. Consider the local ring $R = k[X, Y, Z]_{X,Y,Z}/(XY, XZ)_{X,Y,Z}$, where k is a field. Letting x, y, z denote the residues of X, Y, Z, respectively, show:
(i) $\mathfrak{q} = \{x + z, y\}$ is a system of parameters of R;
(ii) $e(\mathfrak{q}, R) = 1$, $\lambda(R/\mathfrak{q}) = 2$.
(iii) Apply the associativity formula to confirm the value $e(\mathfrak{q}, R) = 1$.

Exercise 7.6.7. Let $R = k[x, y, z]$ be a polynomial ring over a field k and let $I \subset R$ be the ideal of maximal minors of the matrix

$$\begin{pmatrix} x & 0 & 0 \\ y & x & 0 \\ z & y & x \\ 0 & z & y \end{pmatrix}.$$

Show that I is not of linear type, but all the associated algebras to I (symmetric algebra, Rees algebra, associated graded ring and fiber cone) are Cohen–Macaulay.

Exercise 7.6.8. Let $R = k[x_0, x_1, x_2, x_3]$ and consider the respective homogeneous defining ideals I and J in R of the rational *normal* cubic curve and the rational *non-normal* quartic curve in $\mathbb{P}^3$. Prove the and elaborate on the following phenomena:
(i) $\mathcal{S}_{R/I}(I/I^2)$ is not Cohen–Macaulay.
(ii) $\mathcal{S}_{R/J}(J/J^2)$ is not Cohen–Macaulay.

Exercise 7.6.9 (Trung–Ikeda). Let $A = k[u^3, u^2v, uv^2, v^3]$ (k a field) and set $R = A[t]$. Consider the ideal $I := (u^3, u^2v, v^3, t) \subset R$.
(i) Show that I has maximal analytic spread and compute a minimal reduction J of I.
(ii) Show that the reduction number of J in (i) is ≤ 2.
(iii) Prove that the fiber cone $\mathcal{F}(I)$ is Cohen–Macaulay (actually, a hypersurface ring), but the Rees algebra $\mathcal{R}_R(I)$ is not Cohen–Macaulay.

(iv) Prove that $\mathrm{gr}_I(R)$ is equidimensional and normal, but not R/I-torsion-free.
(Hint: show that one of its associated primes contracts to an associated prime of R/I^2.)

Exercise 7.6.10. Let $I \subset k[x,y,z,w]$ denote a presentation ideal of the k-subalgebra $k[u^4, u^3v, uv^3, v^4] \subset k[u,v]$.
(i) Prove that I can be generated by one quadric and three cubics.
(Hint: consider the matrix

$$\begin{pmatrix} x & z & y^2 & yw \\ y & w & xz & z^2 \end{pmatrix}.)$$

(ii) Write a minimal reduction of I with reduction number one.
(iii) Compute a defining ideal of the fiber cone $\mathcal{F}(I)$.

Exercise 7.6.11. Repeat the previous exercise for $k[u^5, u^4v, uv^4, v^5] \subset k[u,v]$. Can one see a pattern for the generation of I as for a defining ideal of the corresponding fiber cone?

Exercise 7.6.12. Consider the ring $R = k[X,Y,Z]/(Y^2 - XZ)$ and its prime ideal $\wp = (x,y) = (X,Y)/(Y^2 - XZ)$.
(1) Show that the symbolic Rees algebra $\mathfrak{R} := \sum_i \wp^{(i)} t^i \subset R[t]$ of $\wp$ is generated by $\{xt, yt, xt^2\}$ as a graded R-algebra.
(2) Prove that there is a presentation $\mathfrak{R} \simeq S/I_2(\mathcal{S})$, where $S = k[X,Y,Z,T,U,V]$ and $\mathcal{S}$ is a 3×3 generic symmetric matrix. Conclude that $\mathfrak{R}$ is Cohen–Macaulay.

Exercise 7.6.13. Let $R = k[x,y,z]$ (k a field) and let $I \subset R$ be a perfect ideal of codimension 2, generated by three forms of equal degree $d \geq 2$. Then the Hilbert polynomial of R/I is

$$\binom{d + d_0 - 1}{2} + \binom{2d - d_0 - 1}{2} - 3\binom{d-1}{2} + 1,$$

for some $1 \leq d_0 \leq \lfloor \frac{d}{2} \rfloor$.

Exercise 7.6.14. Let $f \in R = k[x,y,z]$ be a square-free homogeneous polynomial of degree $d + 1 \geq 3$ and let $J \subset R$ denote its gradient ideal. If $\mathrm{depth}(R/J) > 0$ then

$$\deg(R/J) = \binom{d + d_0 - 1}{2} + \binom{2d - d_0 - 1}{2} - 3\binom{d-1}{2} + 1,$$

for some $1 \leq d_0 \leq \lfloor \frac{d}{2} \rfloor$.

Bibliography

[1] Y. Akizuki, Teilerkettensatz und Vielfachenkettensatz, Proc. of the Physico–Mathematical Society of Japan (3) **17** (1935), 337–345. 86

[2] J. Andrade and A. Simis, A complex that resolves the ideal of minors having $n - 1$ columns in common, Proc. Amer. Math. Soc. **8:1** (1981), 217–219. 246, 251, 289

[3] J. Andrade and A. Simis, Ideals of minors fixing a submatrix, J. Algebra **102** (1986), 249–259. 246, 289

[4] J. Andrade and A. Simis, Free resolutions of certain codimension three perfect radical ideals, Arch. Math. **53** (1989), 448–460. 246, 289

[5] J. Andrade and A. Simis and W. Vasconcelos, On the grade of some ideals, Manuscripta math. **34** (1981), 241–254. 77

[6] M. Artin and M. Nagata, Residual intersections in Cohen–Macaulay rings, J. Math. Kyoto Univ. **12** (1972), 307–323. 111

[7] M. Auslander and D. Buchsbaum, Homological dimension in Noetherian rings, Proc. Nat. Acad. Sci. **42** (1956), 36–38. 249

[8] M. Auslander and D. Buchsbaum, Homological dimension in local rings, Trans. Amer. Math. Soc. **85** (1957), 390–405. 249

[9] M. Auslander and D. Buchsbaum, Homological dimension in Noetherian rings II, Trans. Amer. Math. Soc. **88** (1958), 194–206. 249

[10] M. Auslander and D. Buchsbaum, Codimension and multiplicity, Ann. of Math. **68** (1958), 625–657. 129, 134, 137, 249

[11] R. Baer, Erweiterung von Gruppen und ihren Isomorphismen, Math. Z. **38** (1934), 375–416. 221

[12] R. Baer, Abelian groups that are direct summands of every containing abelian group, Bull. Amer. Math. Soc., **46** (1940), 800–806. 250

[13] C. Baetica, Rees algebras of ideals generated by Pfaffians, Comm. in Algebra **26** (1998), 1769–1778. 289

[14] C. Baetica, Pfaffian ideals of linear type, Comm. in Algebra **27** (2007), 3909–3920. 282, 289

[15] H. Bass, Torsion free and projective modules, Transactions of the American Mathematical Society **102** (1962), 319–327. 184

[16] H. Bass, On the ubiquity of Gorenstein rings, Math. Z. **82** (1963), 8–28. 171, 172

[17] R. Berger, Über verschiedene Differentenbegriffe. vol. 1, Springer, Berlin, 1960. 137

[18] I. Bermejo and P. Gimenez and A. Simis, Polar syzygies in characteristic zero: the monomial case, J. Pure Appl. Algebra **213** (2009), 1–21. 124

[19] I. Bermejo and P. Gimenez and A. Simis, Syzygies of differential of forms, J. Algebra **375** (2013), 41–58. 124

[20] E. Bézout, *Théorie Générale des Équations algébriques*, Paris, 1779. 80

[21] N. Bourbaki, *Algèbre Commutative*, Chapitres 1–4, Masson, Paris, 1985/Springer, Berlin, 2006. 155

[22] H.-B. Brinkmann, Equivalence of n-extensions, Arch. Math. (Basel) **19** (1968), 624–626. 221

[23] P. Brumatti and A. Simis, The module of derivations of a Stanley–Reisner ring, Proceedings of the Amer. Math. Society **123** (1995), 1309–1318. 129

[24] P. Brumatti and P. Gimenez and A. Simis, On the Gauss algebra associated to a rational map $\mathbb{P}^d \dashrightarrow \mathbb{P}^n$, J. Algebra **207** (1998), 557–571. 124

[25] W. Bruns and J. Herzog, *Cohen–Macaulay Rings*, Cambridge University Press, Cambridge, 1993. 172, 220, 221, 226

[26] W. Bruns and A. Simis, Symmetric algebras of modules arising from a fixed submatrix of a generic matrix, J. of Pure Applied Algebra **49** (1987), 227–245. 247, 248

[27] W. Bruns and U. Vetter, *Determinantal Rings*, Lecture Notes in Mathematics **1327**, Springer,

https://doi.org/10.1515/9783110616989-008

Berlin, 1988. 111, 246, 248, 281, 289, 291
[28] W. Bruns and A. Conca, Gröbner bases and determinantal ideals, *in* Commutative algebra, singularities and computer algebra (Sinaia, 2002), 9–66, NATO Sci. Ser. II Math. Phys. Chem., 115, Kluwer, Dordrecht, 2003. 288
[29] D. Buchsbaum and D. Eisenbud, Remarks on ideals and resolutions, Sympos. Math. **11** (1973), 191–204. 247
[30] D. Buchsbaum and D. Eisenbud, Algebraic structures for finite free resolutions, and some structure theorems for ideals of codimension 3, American J. Math. **99** (1977), 447–485. 171
[31] L. Busé and J.-P. Jouanolou, On the closed image of a rational map and the implicitization problem, J. Algebra **265** (2003), 312–357. 308
[32] H. Cartan and S. Eilenberg, *Homological Algebra*, Princeton University Press, Princeton, 1999. PMS-19. 192, 206, 210, 248, 249
[33] H. Cartan and C. Chevalley, Geométrie Algébrique. Seminaire Cartan–Chevalley, Paris, 1955/56. 130, 138
[34] C. Chevalley, On the theory of local rings, Ann. of Math. **44** (1943), 690–708. 175, 277
[35] Y. Cid-Ruiz and A. Simis, Degree of rational maps via specialization, arXiv:1901.06599v2 [math.AG], 2019. 293
[36] I. S. Cohen and A. Seidenberg, Prime Ideals and Integral Dependence, Bull. Amer. Math. Soc. **52** (1946), 252–261. 30
[37] I. S. Cohen, Commutative rings with restricted minimum condition, Duke Math. J. **17** (1950), 27–42. 43, 47, 87
[38] I. S. Cohen, Lengths of chains of prime ideal chains, American Journal of Mathematics **76** (1954), 654–668. 58
[39] A. Conca, Straightening law and powers of determinantal ideals of Hankel matrices, Adv. Math. **138** (1998), 263–292. 174, 288
[40] R. Cowsik and M. V. Nori, On the fibers of blowing up, J. Indian Math. Soc. **40** (1976), 217–222. 281
[41] E. D. Davis, Ideals of the principal class, R-sequences and a certain monoidal transformation, Pacific J. Math. **20** (1967), 197–205. 180, 279
[42] P. del Pezzo, Sulle superficie di ordine n immerse nello spazio di $n + 1$ dimensioni, Rend. R. Acc. delle Scienze Fisiche e Mat. di Napoli **24** (1885), 212–216. 82
[43] F. DeMeyer and E. Ingraham, *Separable Algebras over Commutative Rings*, LNM **181**, Springer, Berlin, 1971. 136
[44] J. Dieudonné, Remarks on quasi-Frobenius rings, Ill. J. Math. **12** (1958), 346–354. 172
[45] J. A. Eagon, Ideals generated by the subdeterminants of a matrix, PhD Thesis, University of Chicago, 1961. 239, 241
[46] J. A. Eagon and D. G. Northcott, Ideals defined by matrices and a certain complex associated with them, Proc. Royal Soc. **269** (1962), 188–204. 237, 239
[47] J. A. Eagon and D. G. Northcott, Generically acyclic complexes and generically perfect ideals, Proc. R. Soc. Lond. A **299** (1967), 147–172. 174, 215, 216, 246
[48] P. M. Eakin, The converse to a well known theorem on Noetherian rings, Math. Ann. **177** (1968), 278–282. 44
[49] B. Eckmann and A. Schopf, Über injektive Moduln, Arch. Math. **4** (1953), 75–78. 220
[50] S. Eilenberg, Homological dimension and syzygies, Ann. of Math. **64** (1956), 328–336. 249
[51] S. Eilenberg and T. Nakayama, On the dimension of modules and algebras. V. Dimension of residue rings, Nagoya Math. J. **11** (1957), 9–12. 249
[52] D. Eisenbud and J. Harris, On varieties of minimal degree (A centennial account), Proceedings of Symposia in Pure Mathematics **46** (1987), 3–13. 82
[53] D. Eisenbud and M. Hochster, A Nullstellensatz with Nilpotents and Zariski's Main Lemma on

Holomorphic Functions, J. Algebra **58** (1979), 157–161. 42, 83
[54] D. Eisenbud and C. Huneke, Cohen–Macaulay Rees algebras and their specializations, J. Algebra **81** (1983), 202–224. 289
[55] D. Eisenbud, Linear sections of determinantal varieties, Amer. J. Math. **110** (1988), 541–575. 174
[56] S. Endo, On flat modules over commutative rings, J. Math. Soc. Japan **14** (1962), 284–291. 213
[57] M. Fiorentini, On relative regular sequences, J. Algebra **18** (1971), 384–389. 283
[58] H. Fitting, Die Determinantenideale Moduls, Jahresbericht DMV **46** (1936), 192–228. 106, 115, 186
[59] P. Gimenez and A. Simis and W. Vasconcelos and R. Villarreal, On complete monomial ideals, J. Comm. Algebra **8** (2016), 207–226. 287
[60] S. Goto and S. Tachibana, A complex associated with a symmetric matrix, J. Math. Kyoto Univ. **17** (1977), 51–54. 244
[61] S. Goto and Y. Shimoda, Rees algebras of Cohen–Macaulay local rings, *in* Commutative algebra, Lect. Notes Pure Appl. Math. 68, Marcel Dekker, New York, 1982. 286
[62] C. Gottlieb, A proof that commutative artinian rings are noetherian, Comm. in Algebra **23** (1995), 4687–4691. 87
[63] H. Grell, Beziehungen zwischen den Idealen verschiedener Ringe, Math. Ann. **97** (1927), 490–523. 23, 83
[64] W. Gröbner, *Moderne Algebraische Geometrie*, Springer, Wien–Innsbruck, 1949. 90
[65] T. Gulliksen and G. Levin, *Homology of Local Rings*, Papers in Pure and Applied Mathematics, vol. 20, Queen's University, Canada, 1969. 253
[66] T. Gulliksen and O. Négard, Un complexe résolvant pour certains idéaux déterminantiels, C. R. Acad. Sci. **274** (1972), 16–18. 171, 242, 243
[67] J. Harris, Algebraic Geometry, Graduate Texts in Mathematics, vol. 133, Springer, Berlin, 1992. 81, 90
[68] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, vol. 52, Springer, Berlin, 1975. 79, 299
[69] M. Herrmann, S. Ikeda and U. Orbanz, *Equimultiplicity and Blowing up*, Springer, Berlin Heidelberg, 1988. 284
[70] J. Herzog and A. Simis and W. Vasconcelos, Koszul homology and blowing-up rings, *in* Commutative Algebra, Proceedings: (Trento 1981) (S. Greco and G. Valla, Eds.), Lecture Notes in Pure and Applied Mathematics **84**, Marcel Dekker, New York, 1983. pp. 79–169. 110, 263, 265, 283, 284, 287, 289
[71] J. Herzog and A. Simis and W. Vasconcelos, Arithmetic of normal Rees algebras, J. Algebra **143** (1991), 269–294. 287, 288
[72] D. Hilbert, Über die Theorie der algebraischen Formen, Math. Ann. **36** (1890), 473–534. 43, 68, 89, 181
[73] M. Hochster, Criteria for equality of ordinary and symbolic powers of an ideal, Math. Z. **133** (1973), 53–65. 288
[74] M. Hochster, Grade-sensitivity modules and perfect modules, Proc. London Math. Soc. **29** (1974), 55–76. 216, 248
[75] M. Hochster and J. Eagon, A class of perfect determinantal ideals, Bull. Amer. Math. Soc. 1970;76:1026–1029 (short). 174, 248
[76] M. Hochster and J. A. Eagon, Cohen–Macaulay rings, invariant theory, and the generic perfection of determinantal loci, Amer. J. Math. **93** (1971), 1020–1058. 174, 246, 248, 289
[77] O. Hölder, Zurückführung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen, Math. Ann. **34** (1889), 26–56. 114
[78] C. Hopkins, Rings with minimal condition for left ideals, Annals of Math. **40** (1939),

712–730. 87
[79] C. Huneke, On the symmetric and Rees algebra of an ideal generated by a d-sequence, J. Algebra **62** (1980), 268–275. 283
[80] C. Huneke, The theory of d-sequences and powers of ideals, Advances in Math. **46** (1982), 249–279. 284
[81] C. Huneke, Strongly Cohen–Macaulay schemes and residual intersections, Trans. Amer. Math. Soc. **277** (1983), 739–763. 289
[82] C. Huneke and M. E. Rossi, The dimension and components of symmetric algebras, J. Algebra **98** (1986), 200–210. 264, 265, 292
[83] C. Huneke, Determinantal ideals of linear type, Arch. Math. **47** (1986), 324–329. 280, 281, 288
[84] C. Huneke and J. Sally, Birational extensions in dimension two and integrally closed ideals, J. Algebra **115** (1988), 48–500. 286
[85] C. Huneke and A. Simis and W. Vasconcelos, Reduced normal cones are domains, *in* Invariant Theory, Proceedings (Eds: R. Fossum, W. Haboush, M. Hochster and V. Lakshmibai), Contemp Math. Vol. **88** (1989), 95–101. 288
[86] C. Jordan, *Traité des Substitutions et des Équations Algébriques*, Gauthier–Villars, Paris, 1870. 48, 101, 114
[87] D. Jorgensen, A generalization of the Auslander–Buchsbaum formula, J. Pure Appl. Algebra **144** (1999), 145–155. 216
[88] T. Jósefiak, Ideals generated by minors of a symmetric matrix, Comment. Math. Helvetici **53** (1978), 595–607. 242, 244
[89] J. Jothilingam, Cohen's theorem and Eakin–Nagata theorem revisited, Comm. in Algebra **28:10** (2000), 4861–4866. 44
[90] E. Kähler, Geometria aritmetica, Ann. Mat. Pura Appl. Ser. IV **45** (1958), 1–399. 130, 138
[91] Mathematische Werke/Mathematical works/Erich Kähler; edited by Rolf Berndt and Oswald Riemenschneider, de Gruyter, Berlin, 2003. 138
[92] I. Kaplansky, Projective modules, Ann. Math. **68** (1958), 372–377. 183
[93] I. Kaplansky, *Commutative Rings*, The University of Chicago Press, Chicago and London, 1970 (Revised 1974). 31, 175
[94] G. Kennedy and A. Simis and B. Ulrich, Specialization of Rees algebras with a view to tangent star algebras, in *Commutative Algebra, Proceedings*, ICTP, Trieste, September 1992, World Scientific, Singapore 1994, 130–139. 289, 293
[95] B. Kotsev, Determinantal Ideals of Linear Type of a Generic Symmetric Matrix, J. of Algebra **139** (1991), 484–504. 282, 288
[96] K. Konrad, Tensor Products, I and II, available at: https://kconrad.math.uconn.edu/. 104
[97] K. Konrad, Exterior powers, available at: https://kconrad.math.uconn.edu/. 105
[98] W. Krull, *Idealtheorie*, Ergebnisse d. Math. **46**, Zweite, ergänze Auflage. Springer, Berlin, 1968. VII, 4, 19, 49, 175
[99] W. Krull, Gesammelte Abh. (P. Ribenboim, Ed.), Vol 1, de Gruyter, Berlin, 1999. 19
[100] R. E. Kutz, Cohen–Macaulay rings and ideal theory in rings of invariants of algebraic groups, Trans. Amer. Math. Soc. **194** (1974), 115–129. 174, 242, 268
[101] E. Lasker, Zur Theorie der Moduln und Ideale, Math. Ann. **60** (1905), 20–116. 69, 89
[102] J. Levitzki, On rings which satisfy the minimum condition for right handed ideals, Compositio Math. **7** (1939), 214–222. 87
[103] J. Lipman, Free derivation modules on algebraic varieties, Amer. J. Math. **87** (1965), 874–898. 134
[104] J. Lipman and B. Teissier, Pseudo-rational local rings and a theorem of Briançon–Skoda about integral closures of ideals, Michigan Math. J. **28** (1981), 97–116. 285

[105] F. S. Macaulay, On the resolution of a given modular system into primary systems including some properties of Hilbert numbers, Math. Ann. **74** (1913), 66–121. 90
[106] F. S. Macaulay, *The Algebraic Theory of Modular Systems*, Cambridge Tracts in Mathematics and Mathematical Physics, **19**, Cambridge University Press, New York–London, 1916. (Reprinted: Hafner Service Agency; 1964). 167
[107] E. Matlis, Injective modules over Noetherian rings, Pacific J. Math. **8** (1958), 511–528. 220
[108] H. Matsumura, *Commutative ring theory*, Cambridge University Press, Cambridge, 1990. 58, 213, 221
[109] A. Micali, Sur les algèbres universelles, Ann. Inst. Fourier (Grenoble) **14:2** (1964), 33–87. 316
[110] A. Micali, Sur les algèbres de Rees, Bull. Soc. Math. Belg. **20** (1968), 215–235. 316
[111] M. Nagata, On the purity of branch locus in regular local rings, Illinois J. Math. **3** (1959), 328–333. 137
[112] M. Nagata, *Local Rings*, Interscience, New York, 1962. 46, 48, 65, 85, 200, 234, 315
[113] M. Nagata, A type of subring of a noetherian ring, J. Math. Kyoto Univ. **8** (1968), 465–467. 44
[114] M. Nagata, A proof of the theorem of Eakin–Nagata, Proc. Japan Acad. **67** (1991), 238–239. 44
[115] K. M. Neuerburg and Z. Teitler, Decompositions of ideals of minors meeting a submatrix, Comm. in Algebra **44:4** (2016), 1809–1820. 246, 289
[116] E. Noether, Idealtheorie in Ringebereiche, Math. Ann. **83** (1921), 24–66. 19, 85
[117] E. Noether, Eliminationstheorie und algemeine Idealtheorie, Math. Ann. **90** (1923), 229–261. 19, 84
[118] E. Noether, Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern, Math. Ann. **96** (1927), 26–61. 19, 48, 86
[119] E. Noether, Idealdifferentiation und Differente, J. reine angew. Math. **188** (1950), 1–21. 134
[120] E. Noether, *Gesammelte Abhandlugen (Collected Papers)*, (N. Jacobson, Ed.) Springer, Berlin, 1983. 17, 19
[121] D. Northcott and D. Rees, Reductions of ideals in local rings, Proc. Cambridge Phil. Soc. **50** (1954), 145–158. 276, 277
[122] D. Northcott and D. Rees, Extensions and simplifications of the theory of regular local rings, J. London Math. Soc. **32** (1957), 367–374. 175
[123] L. O'Carroll and G. Valla, On the smoothness of blowups, Comm. in Algebra **25** (1997), 1861–1872. 284
[124] A. Ornstein, Rings with restricted minimum condition, Proc. Amer. Math. Soc. **19** (1968), 1145–1150. 87
[125] H. Prüfer, Untersuchungen über die Teilbarkeitseigenschaften in Körpern, J. Reine Angew. Math. **168** (1932), 1–36. 29, 83, 84
[126] V. C. Quiñonez, Integral closure and other operations on monomial ideals, J. Comm. Alg. **2** (2010), 359–386. 287
[127] D. Rees, Two classical theorems of ideal theory, Mathematical Proceedings of the Cambridge Philosophical Society **52** (1956), 155–157. 275
[128] D. Rees, A theorem of homological algebra, Proc. Cambridge Phil. Soc. **52** (1956), 605–610. 175, 249, 318
[129] D. Rees, The grade of an ideal or module, Proc. Cambridge Phil. Soc. **53** (1957), 28–42. 175, 249
[130] K. Saito, Theory of logarithmic differential forms and logarithmic vector fields, J. Fac. Sci. Univ. Tokyo Sect. 1A Math. **27** (1980), 265–291. 134
[131] P. Salmon, Sulle algebre graduate relative ad un ideale, Symposia Mathematica **8** (1972), 269–293. 265
[132] P. Samuel, Une généralisation des polynomes de Hilbert, C. R. Acad. Sci. Paris **225** (1947), 1111–1113. 312

[133] P. Samuel, Algèbre Locale, Mémorial des sciences mathématiques **123** (1953), 1–76. 175, 300, 310
[134] A. Seidenberg, The hyperplane sections of normal varieties, Trans. Amer. Math. Soc **69** (1950), 357–386. 81
[135] J.-P. Serre, Sur la dimension homologique des anneaux et des modules noethériens, In *Proc Int Symp Tokyo–Nikko 1955*, Science Council of Japan, Tokyo, (1956), 175–189. 249
[136] J.-P. Serre, Faisceaux algébriques cohérents, Ann. Math. **61** (1955), 197–278. 249
[137] J.-P. Serre, Géométrie algébrique et géometrie analytique, Annales de l'institut Fourier **6** (1956), 1–42. 212
[138] J.-P. Serre, *Algèbre Locale–Multiplicités*, Lecture Notes in Mathematics **11**, Springer, Berlin, 1965. 56, 79, 155, 249, 299
[139] A. Simis, *When are projective modules free?* Queen's papers in pure and applied mathematics, no. 21, Kingston, Ont., 1969. 249
[140] A. Simis and W. Vasconcelos, On the dimension and integrality of symmetric algebras, Math. Z. **177** (1981), 341–358. 254
[141] A. Simis and W. Vasconcelos, Krull dimension and integrality of symmetric algebras, Manuscripta Math. **61** (1988), 63–78. 59, 110, 293
[142] A. Simis and N. V. Trung, The divisor class group of ordinary and symbolic blow-ups, Math. Z. **198** (1988), 479–491. 288
[143] A. Simis, Effective computation of symbolic powers by Jacobian matrices, Comm. in Algebra **24** (1996), 3561–3565. 42
[144] A. Simis, On the Jacobian module associated to a graph, Proc. Amer. Math. Soc. **126** (1998), 989–997. 124
[145] A. Simis and B. Ulrich and W. Vasconcelos, Codimension, multiplicity and integral extensions, Math. Proc. Camb. Phil. Soc. **130** (2001), 237–257. 308
[146] A. Simis and B. Ulrich and W. Vasconcelos, Tangent algebras, Trans. Amer. Math. Soc. **364** (2012), 571–594. 137
[147] R. Stanley, *Enumerative Combinatorics, Vol. 1*, Cambridge Studies in Advanced Mathematics, vol. 49, 2nd edition, 2012. 294, 296
[148] E. Steinitz, Algebraische Theorie der Körper, Journal f. reine angew. Mathematik (Crelle's Journal) **137** (1910), 167–309. 12, 14, 18
[149] E. Strickland, On the conormal bundle of the determinantal variety, J. Algebra **75** (1982), 523–537. 282
[150] I. Swanson and C. Huneke, *Integral Closure of Ideals, Rings, and Modules*, LMN vol. 336. Cambridge University Press, Cambridge, 2006. 32, 286
[151] N. V. Trung and S. Ikeda, When is the Rees algebra Cohen–Macaulay? Com. in Algebra **17:12** (1989), 2893–2922. 286
[152] G. Valla, Certain Graded Algebras are Always Cohen–Macaulay, J. Algebra **42** (1976), 537–548. 267, 285
[153] G. Valla, On the Symmetric and Rees algebras of an ideal, Manuscripta Math. **30** (1979), 239–255. 265, 283
[154] B. L. van der Waerden, On Hilbert's function, series of composition of ideals and a generalization of the theorem ot Bézout, Proc. K. Akad. Wet. Amsterdam **31** (1928), 749–770. 69, 255
[155] B. L. van der Waerden, Verallgemeneirung des Bézoutschen Theorems, Math. Ann. **99** (1928), 497–541. 69, 78
[156] B. L. van der Waerden, Zur Algebraischen Geometrie, XII. Ein Satz über Korrespondenzen und die Dimension einer Schnittmannifaltigkeit, Math. Ann. **115** (1938), 330–332. 79
[157] W. V. Vasconcelos, On the homology of $I//I^2$, Comm. in Algebra **6** (1978), 1801–1809. 199

[158] W. V. Vasconcelos, On finitely generated flat modules, Trans. Amer. Math. Soc. **138** (1969), 505–512. 213
[159] W. V. Vasconcelos, *Arithmetic of Blowup Algebras*, London Math. Soc., Lecture Note Series 195, Cambridge University Press, Cambridge, 1994. 258, 280
[160] W. V. Vasconcelos, *Computational Methods in Commutative Algebra and Algebraic Geometry*. Springer, Heidelberg, 2004. 212
[161] J. Watanabe, $\mathfrak{m}$-full ideals, Nagoya Math. J. **106** (1987), 101–111. 286
[162] J. Watanabe, Hankel matrices and Hankel ideals, Proc. Schl. Sci., Tokai Univ. **32** (1997), 11–21. 174
[163] C. Weibel, History of homological algebra. In: *History of topology*, 797–836, North-Holland, Amsterdam, 1999. 249, 250
[164] Y. Xie, Formulas for the multiplicity of graded algebras, Trans. Amer. Math. Soc. **364** (2012), 4085–4106. 309
[165] N. Yoneda, On the homology theory of modules, J. Fac. Sci. Tokyo **7** (1954), 193–227. 221
[166] O. Zarisky, A fundamental lemma from the theory of holomorphic functions on an algebraic variety, Ann. Mat. Pura Appl. **29** (1949), 187–198. Reprinted in "Oscar Zariski, Collected Papers," Vol. II, pp. 55–66, MIT Press, Cambridge, 1973. 83
[167] O. Zariski, On the purity of the branch locus of algebraic functions, Proc. Nat. Acad. Sci. USA **44** (1958), 791–796. 137
[168] O. Zarisky and P. Samuel, *Commutative Algebra*, Volume I, Van Nostrand, Princeton, 1958. (Reprinted: Graduate Texts in Mathematics, vol. 28, Springer, Berlin). 37, 38, 85
[169] O. Zarisky and P. Samuel, *Commutative algebra*, Volume II, Van Nostrand, Princeton, 1958. (Reprinted: Graduate Texts in Mathematics, vol. 29, Springer, Berlin). 32, 79, 175, 285, 310

Index